UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

Departamento de Ciência da Computação–UFRJ

21 de julho de 2016

Números inteiros e criptografia

S. C. Coutinho

Provas e gabaritos

Até a página 25 você encontrará as provas do curso de *Álgebra para a informática*–que era basicamente uma versão anterior do mesmo curso.

Lembre-se: Nas provas não são aceitas respostas sem justificativa. Você deve saber explicar tudo o que fizer.

Prova 1: segundo semestre de 1995

1^a Questão. Determine:

1. o máximo divisor comum d de $a = 272828282$ e $b = 3242$ e inteiros α e β tais que $\alpha a + \beta b = d$.

2. um fator de 6883901 pelo algoritmo de Fermat.

3. um fator primo de $2^{3965157} - 1$.

4. as soluções de $x^2 \equiv 7 \pmod{43}$.

5. o resto da divisão de $39^{50!}$ por 2251.

6. uma seqüência de 5646345 inteiros consecutivos que sejam *todos compostos*.

2^a Questão. Chamamos de *hexagonais* os números definidos pela fórmula $h_n = 1 + 3n(n-1)$ para $n = 1, 2, \ldots$. O nome vem do fato de que estes números podem ser dispostos em hexágonos regulares concêntricos.

1. Calcule a soma dos n primeiros números hexagonais quando $n = 1$, 2, 3 , 5, 6 e 7. Use estes dados numéricos para advinhar a fórmula da soma dos n primeiros números hexagonais.

2. Prove a fórmula obtida no item anterior usando o *método de indução finita*.

Prova 2: segundo semestre de 1995

1^a Questão. Determine:

1. Um fator primo de $M(37)$.
2. Dois inteiros positivos que sejam solução de $\phi(n) = 136$.

2^a Questão. Verifique se 703 é:

1. um número de Carmichael;
2. um pseudoprimo forte para a base 7.
3. um pseudoprimo para a base 7;

3^a Questão. Três satélites passarão sobre o Rio esta noite. O primeiro passará à 1 hora da madrugada, o segundo às 4 horas e o terceiro às 8 horas da manhã. Cada satélite tem um período diferente. O primeiro leva 13 horas para completar uma volta em torno da Terra, o segundo leva 15 horas e o terceiro 19 horas. Determine quantas horas terão que se passar, a partir da meia-noite, até que os três satélites passem ao mesmo tempo sobre o Rio.

4^a Questão. Seja G um grupo finito provido de uma operação $\star$. Suponha que um primo p divide a ordem de G e considere o subconjunto H_p de G formado pelo elemento neutro e pelos elementos de ordem p contidos em G.

1. Mostre que se G é *abeliano* então H_p é um subgrupo de G.
2. Determine H_3 quando $G = U(28)$.
3. Dê um exemplo de um grupo *não abeliano* G para o qual H_2 *não* é um subgrupo de G.

Prova Final: segundo semestre de 1995

1^a Questão. Determine:

1. O resto da divisão de 2^{78654} por 137.

2. O menor inteiro positivo que deixa resto 2 na divisão por 5, resto 4 na divisão por 7 e resto 5 na divisão por 11.

3. As soluções da equação $\phi(n) = 22$.

4. O inverso de 137 módulo 2887.

5. Todas as soluções da equação $8^x \equiv 9 \pmod{37}$.

6. Se 825265 é um número de Carmichael.

2^a Questão. O objetivo desta questão é mostrar que os grupos $U(3^n)$ são sempre cíclicos.

1. Mostre que $\overline{2}$ é um gerador de $U(9)$.

2. Prove por indução em n que se $n \geq 2$, então $2^{3^{n-2}} \equiv 3^{n-1} - 1 \pmod{3^n}$.

3. Mostre, usando (2), que $U(3^n)$ é gerado por $\overline{2}$.

Prova 1: primeiro semestre de 1996

1. Determine:

   1. Um múltiplo de 330 e um múltiplo de 240 cuja soma seja 210.

   2. Um fator *primo* de $2^{1067} - 1$.

   3. Um fator de 13886959 pelo método de Fermat.

   4. todos os possíveis algarismos x e y de modo que o número cuja representação na base 10 é $yx5y$ seja divisível por 7.

   5. o resto da divisão de 3^{1034^2} por 1033.

   6. O maior número possível de fatores primos de um inteiro n que não tem nenhum fator $\leq n^{1/3}$.

2. O objetivo desta questão é obter e provar uma fórmula para a soma dos cubos dos n primeiros inteiros positivos. Seja, então,

$$S_n = 1^3 + 2^3 + 3^3 + \cdots + n^3.$$

   1. Tabele os valores de S_n para n de 1 a 6 e compare-os com os valores cor-respondentes para a soma dos n primeiros inteiros positivos. Use isto para advinhar qual deve ser a fórmula para S_n.

   2. Prove a fórmula obtida em (1) por indução finita.

Prova 2: primeiro semestre de 1996

1. Seja $n = 15841$.

   1. Verifique se n é um número de Carmichael.

   2. Calcule o resto da divisão de 2^{495} por n pelo teorema chinês do resto.

   3. Determine se n é um pseudoprimo forte para a base 2.

2. Em seu primeiro contato com um planeta com que a Federação deseja estabelecer relações diplomáticas, os oficiais da *Enterprise* foram convidados para um banquete. Infelizmente há um grupo dissidente no planeta que deseja apoiar os Klingons e não a Federação. Um espião desta facção é instruído a envenenar um dos oficiais da Enterprise. O traidor é descoberto, mas foge a tempo. Em seu alojamento é encontrada a mensagem codificada $2451 - 1830$ que contém o nome do oficial envenado e um pedaço de papel com os números 5893 e 3827, usados na codificação. Como o veneno é seu próprio antídoto é preciso saber exatamente quem foi envenenado. Trabalhando contra o tempo, Spock verificou que se tratava de um código primitivo, utilizado na terra no século XX, quando era conhecido por RSA. Quem foi o oficial envenenado?
Lembretes: no RSA $n > \phi(n) > e$. A correspondência entre letras e números é

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

3. Determine os subgrupos de ordem 4 de $U(21)$. Indique quais são cíclicos e quais não são.

4. Seja $p \neq 2$ um número *primo* e $n = 10^p - 1$. Seja $q > 3$ um fator *primo* de n.

   1. Calcule a ordem de $\overline{10}$ em $U(q)$.

   2. Mostre que q tem que ser da forma $q = 2pk + 1$ onde $k \geq 1$ é um inteiro.

   3. Use a fórmula de (2) para achar todos os fatores primos de

$$11111 = (10^5 - 1)/9.$$

Prova Final: primeiro semestre de 1996

1. Determine:.

   1. se 41041 é número de Carmichael;

   2. o resto da divisão de 2^{41045} por 41041;

   3. um fator primo de $2^{22121} - 1$;

   4. um fator de 2234047 pelo algoritmo de Fermat;

   5. o máximo divisor comum entre 200! e $2^{83} - 1$.

   6. duas soluções da equação $\phi(n) = 30$.

2. Verifique se cada uma das afirmações abaixo é verdadeira ou falsa. Justifique cuidadosamente suas respostas.

   1. Se $p > 31$ é primo ímpar e $n = 2p + 1$ satisfaz $5^p \equiv -1 \pmod{n}$ então n é primo.

   2. Existem inteiros x e y tais que $x^2 - 7y^2 = 3$.

   3. Se juntarmos aos elementos de ordem 2 de D_4 o elemento neutro temos um subgrupo de D_4.

   4. Qualquer que seja $n \geq 1$ inteiro, o número $4^{24n+1} + 3^{2(18n^2+1)}$ é divisível por 13.

Prova 1: segundo semestre de 1996

1. Determine:

   1. Inteiros x e y que satisfaçam a equação $12435x + 798y = 3$.

   2. A maior potência de 2 que divide $3^p - 1$, onde p é um número primo. De que maneira o resultado depende do primo p?

   3. Um fator de 1341671 pelo método de Fermat.

   4. Infinitos inteiros positivos $n_1, n_2, \ldots$ tais que $8n_i^2 + 1$ é um número composto.

   5. O resto da divisão de $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1}$ por p, sabendo-se apenas que $p > 2$ é *primo*. Verifique que o resultado que você obteve se aplica a *qualquer* primo $p > 2$.

2. Considere o produto

$$A_n = \left(1 + \frac{1}{1}\right)\left(1 + \frac{1}{2}\right)\left(1 + \frac{1}{3}\right)\cdots\left(1 + \frac{1}{n}\right).$$

Tabele os valores de A_n para $n = 1, \ldots, 5$. Use estes valores para advinhar uma fórmula simples para o produto. Prove que a sua fórmula é verdadeira para qualquer n usando *indução finita*.

Prova 2: segundo semestre de 1996

1^a Questão. Determine:

1. se 2465 é um número de Carmichael;

2. o resto da divisão de 2^{77} por 2465, usando o teorema chinês do resto;

3. se 2465 é um pseudoprimo forte para a base 2;

4. duas soluções de $\phi(n) = 2^{16}$;

5. um fator primo de $M(179)$;

6. a fatoração de 13281841, sabendo-se que tem apenas dois fatores primos distintos, cada um dos quais tem multiplicidade 1, e que $\phi(13281841) = 13274212$.

3. O objetivo desta questão é mostrar que se $n = pq$, onde p e q são primos ímpares distintos, então $U(n)$ *não* é um grupo cíclico.

1. Mostre que se a é um inteiro e $\text{mdc}(a, n) = 1$, então

$$a^{\phi(n)/2} \equiv 1 \pmod{p},$$

   e que a mesma congruência vale módulo q.

2. Mostre, usando (1), que se $\text{mdc}(a, n) = 1$, então

$$a^{\phi(n)/2} \equiv 1 \pmod{n}.$$

3. Qual a maior ordem possível de um elemento de $U(n)$?

4. Use (3) para mostrar que $U(n)$ *não* pode ser cíclico.

Prova Final: segundo semestre de 1996

1^a Questão. Determine:

1. múltiplos de 3736489 e 393307 cuja soma seja 3.

2. o resto da divisão de $3^{2^{67!}}$ por $F(4) = 2^{2^4} + 1$.

3. a solução geral do sistema $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod{11}$ e $x \equiv 3 \pmod{13}$.

4. a maior potência de 2 que divide $3^n + 1$, onde n é um inteiro positivo. Explique como a resposta vai depender de n, justificando cuidadosamente seu argumento.

5. um fator primo de $2^{83} - 1$.

6. um fator de 970171 pelo método de Fermat.

2^a Questão. Seja $p > 11$ um número primo. Determine se cada uma das afirmações abaixo é verdadeira ou falsa, justificando cuidadosamente suas respostas.

1. Se $2p + 1$ é composto, então existe apenas um inteiro positivo tal que $\phi(n) = 2p$.

2. Se $\overline{a} \in U(2p)$ tem ordem $(p-1)/2$, então $\overline{-a}$ é um gerador de $U(2p)$.

3. O menor divisor primo de $p! + 1$ é maior que p.

4. Se $p > 11$ e $3^{2p} \equiv 1 \pmod{2p+1}$ então $2p + 1$ é primo.

Prova 1: primeiro semestre de 1997

1. Determine:

   1. Inteiros x e y que satisfaçam a equação $54317x + 1145y = 2$.

   2. O resto da divisão de $2^{p!} - 1$ por $2^{p+1} - 1$, sabendo-se que p é um número primo. De que maneira o resto depende de p?

   3. Um fator de 1382963 pelo método de Fermat.

   4. O resto da divisão de 2^{130} por 263.

   5. Todos os primos positivos p para os quais a equação

      $$2x + x^p + x^{p!} \equiv 1 \pmod{p}$$

      tem solução $x \not\equiv 0 \pmod{p}$.

2. Seja $F(k) = 2^{2^k} + 1$ e chame de p_k o menor fator primo de $F(k)$.

   1. Mostre *por indução em* $k \geq 1$ que $F(k) - 1$ é igual ao produto dos números de Fermat $F(0), \ldots, F(k-1)$.

   2. use 1. para mostrar, por absurdo, que se $k < m$, então $p_k \neq p_m$.

Prova 2: primeiro semestre de 1997

1. Determine:

   1. se 1541 é um número de Carmichael;

   2. o resto da divisão de 3^{385} por 1541, usando o teorema chinês do resto;

   3. se 1541 é um pseudoprimo forte para a base 3;

   4. se 1541 é um pseudoprimo para a base 3;

   5. um fator primo de $M(1541)$.

2. Agentes de vários países vinham sendo assassinados por um fanático cujo esconderijo foi finalmente descoberto pela polícia. Infelizmente o fanático já havia partido em mais uma missão, de modo que se tornava essencial descobrir quem seria a próxima vítima. Apesar de ser um calculista mental prodigioso, o fanático habitava um local ermo, sem luz elétrica. Por isso, embora houvesse codificado sua lista de vítimas usando um código identificado como sendo o RSA, havia sido obrigado a usar senhas pequenas, tornando o código vulnerável. O código utilizado tinha senha pública $n = 20413$ e $e = 13419$, e o nome do agente a ser assassinado havia sido codificado como

$$5282 \quad - \quad 8435.$$

Decodifique a mensagem e descubra quem seria a próxima vítima.

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

3. O objetivo desta questão é mostrar que o grupo $U(2^k 3)$ *não* é cíclico se $k \geq 2$.

   1. Mostre por indução em k, que se b não é divisível por 2, nem por 3, e se $k \geq 2$, então $b^{2^{k-1}} \equiv 1 \pmod{2^k 3}$.

   2. Determine a ordem de $U(2^k 3)$ e mostre, usando (1), que este grupo não pode ser cíclico se $k \geq 2$.

   3. Mostre que o grupo $U(2^k 3)$ é cíclico se $k = 0$ ou $k = 1$.

Prova Final: primeiro semestre de 1997

1. Determine:
   1. uma solução para a equação $3452x + 125y = 6$;
   2. os dois fatores primos de 999367 pelo algoritmo de Fermat;
   3. o resto da divisão de 5^{150154} por 999367 pelo algoritmo chinês do resto;
   4. se 46657 é um número de Carmichael;
   5. dois inteiros positivos que satisfaçam $\phi(n) = 20$;
   6. os subgrupos de ordem 6 de $U(28)$ indicando quais são cíclicos e quais não são;
   7. o máximo divisor comum entre $2^p - 1$ e $(p + 1)!$ sabendo-se que p é um número primo.

2. Mostre *por indução* em n que

$$(1 + t)(1 + t^2)(1 + t^4) \ldots (1 + t^{2^{n-1}}) = \frac{t^{2^n} - 1}{t - 1}.$$

Explicite cada etapa da indução claramente.

Prova 1: segundo semestre de 1997

1. Determine:

   1. Múltiplos de 749 e 418 cuja diferença é 13.

   2. Um fator de 1333037 pelo método de Fermat.

   3. O resto da divisão de 3^{104} por 257

   4. O máximo divisor comum entre $p^2 - p + 1$ e $(p^2)! + 1$, sabendo-se que p é um primo positivo. De que modo a resposta depende de p ?

   5. O resto da divisão por 7 de

$$1 + 2^{2!} + 3^{3!} + 4^{4!} + 5^{5!} + 6^{6!} + 7^{7!} + 8^{8!} + 9^{9!} + 10^{10!}.$$

2. Seja S_n a soma

$$S_n = \frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \frac{1}{5 \cdot 7} + \frac{1}{7 \cdot 9} + \cdots + \frac{1}{(2n-1)(2n+1)}.$$

   1. Tabele S_n para $n = 1, 2, 3, 4$ e 5, simplifique as frações obtidas, e use isto para advinhar uma fórmula simples para S_n.

   2. Prove sua fórmula por indução em n. Indique claramente cada etapa da demonstração por indução.

Prova 2: segundo semestre de 1997

1. Determine:

   1. se 4371 é um número de Carmichael;

   2. o resto da divisão de 2^{2185} por 4371, usando o teorema chinês do resto;

   3. se 4371 é um pseudoprimo forte para a base 2;

   4. se 4371 é um pseudoprimo para a base 2;

   5. um fator primo de $M(131)$.

   6. as soluções da equação $\phi(n) = 1365$.

2. Um dos maiores gênios

No século XXIII, todas as informações conhecidas sobre a história da humanidade foram armazenadas em um enorme computador. Segundo seus idealizadores, este computador deveria ser capaz de fornecer respostas exatas sobre quem foram os maiores personagens da história em cada época: o maior filósofo, o maior matemático, e assim por diante. Curiosamente, por causa de algum 'bug' em seu software extremamente complexo, o computador desenvolveu um estranho senso de humor. Perguntado sobre quem havia sido o mais esperto personagem do final do século XX, respondeu:

$$n = 11413, \quad e = 7467, \quad 6775 \quad - \quad 9696.$$

Como o computador se recusava a dar maiores explicações, foi necessário consultar as empoeiradas bibliotecas, abandonadas muitos séculos antes. Lá os historiadores descobriram que a resposta havia sido criptografada usando um método da época a que se referia a pergunta, e conhecido como RSA. Quebre a mensagem e descubra qual a resposta dada pelo computador.

3. O objetivo desta questão é mostrar que o grupo $U(3^k)$ é cíclico se $k \geq 3$.

   1. Mostre por indução em k, que se $k \geq 3$ então $2^{3^{k-2}} = -1 + 3^{k-1}q$, onde q é um inteiro que não é divisível por 3. Explicite cada etapa da indução.

   2. Conclua de (1) que $2^{3^{k-1}}$ e $2^{2 \cdot 3^{k-2}}$ *não* são congruentes a 1 módulo 3^k quando $k \geq 3$. Use então o teorema de Euler para mostrar que $\overline{2}$ tem ordem exatamente $2 \cdot 3^{k-1}$ em $U(3^k)$, quando $k \geq 3$.

   3. Explique porque (2) implica que o grupo $U(3^k)$ é cíclico, quando $k \geq 3$.

Prova Final: segundo semestre de 1997

1. Determine:

   1. múltiplos de 3189 e 233 cuja diferença seja 5.

   2. os dois fatores primos de 504467 pelo algoritmo de Fermat.

   3. um fator primo de $2^{609931} - 1$.

   4. se 935 é um número de Carmichael.

   5. o resto da divisão de 2^{111871} por 935 pelo algoritmo chinês do resto.

   6. se a equação $\phi(n) = 2q$ tem solução, sabendo-se que $q > 3$ é um primo ímpar e que $2^{2q} \equiv 5 \pmod{2q+1}$.

   7. um gerador do grupo $U(22)$.

   8. se a equação $x^3 + 7y^8 = 5$ tem soluções inteiras.

2. Seja F_n o n-ésimo número de Fibonacci. Isto é: $F_1 = F_2 = 1$ e $F_{n+1} = F_n + F_{n-1}$. Mostre, *por indução em n* que

$$F_1^2 + F_2^2 + \cdots + F_n^2 = F_n F_{n+1}.$$

Explicite cada etapa da indução claramente.

Prova 1: primeiro semestre de 1998

1. Determine:

   1. inteiros x e y que sejam solução da equação $2633x + 418y = 3$.

   2. um fator de 15693001 pelo método de Fermat.

   3. o resto da divisão de 7^{4205^3} por 4201.

   4. um fator primo ímpar de $5^{25} - 1$.

   5. o resto da divisão de d por 3 sabendo-se que $p > 3$ e $d > 0$ são inteiros e que p, $p + d$ e $p + 2d$ são todos três primos.

2. Mostre, por indução em n, que 24 divide $5^{2n} - 1$ para todo $n \geq 1$. Indique claramente cada etapa da demonstração por indução.

Prova 2: primeiro semestre de 1998

1. Seja $n = 109 \cdot 163 \cdot 379$.

   1. Verifique se n é um número de Carmichael.

   2. Qual a menor base $b > 1$ para a qual n *não* é um pseudoprimo para a base b? Justifique sua resposta cuidadosamente.

2. Este é um problema do *Aryabhatiya*, um tratado indiano do século 6 d.C.. Use o algoritmo chinês do resto para achar o menor número que, se dividido por 8 deixa resto 5, se dividido por 9 deixa resto 4, e se dividido por 7 deixa resto 1.

3. Determine todas as possíveis soluções da equação $\phi(n) = 38$.

4. Você sabe quem é o maior jovem gênio científico do final do século XX? Descubra, decodificando a mensagem

$$5666 \quad - \quad 1680 \quad - \quad 8559$$

que foi codificada usando o RSA, com chave pública $n = 14017$ e $e = 9187$.

5. Seja $p > 5$ um número primo, e suponha que $q > 2$ é um fator *primo* de $n = 5^p - 1$.

   1. Calcule a ordem de $\overline{5}$ em $U(q)$.

   2. Mostre que $q = 2kp + 1$, para algum inteiro $k \geq 1$.

   3. Use 2. para calcular $\text{mdc}(5^{41} - 1, 200!)$—mas cuidado com as potências de 2.

Para decodificar a mensagem da questão 2. use a tabela abaixo:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Prova Final: primeiro semestre de 1998

1. Ache o inverso de 12453 módulo 331.

2. Ache dois fatores de 74483 pelo algoritmo de Fermat.

3. Calcule o resto da divisão de $3^{19!}$ por 307.

4. Determine os dois primos distintos positivos p e q para os quais $pq = 351251$ e $\phi(pq) = 349272$.

5. Determine todos os subgrupos de ordem 4 de $U(28)$, indicando quais são cíclicos e quais não são.

6. Determine o menor primo p para o qual $31 \cdot 61 \cdot p$ é um número de Carmichael.

7. Lembre-se que o n-ésimo termo f_n da seqüência de Fibonacci é definido por $f_1 = f_2 = 1$ e $f_n = f_{n-1} + f_{n-2}$. Mostre, por indução finita em n, que

$$f_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$$

onde α e β são as raízes da equação quadrática $x^2 - x - 1 = 0$. Indique claramente cada etapa da demonstração por indução.
Sugestão: Não esqueça que, como α é raiz de $x^2 - x - 1 = 0$, então $\alpha^2 = \alpha + 1$, e que o mesmo vale para β.

Prova 1: segundo semestre de 1998

1. Ache o inverso de 125 módulo 5441.

2. Ache um fator de 95839 pelo algoritmo de Fermat.

3. Ache um fator *primo* de $2^{625} - 1$.

4. Ache o resto da divisão de 24^{16807} por 233.

5. Sabe-se que a e b são inteiros positivos que satisfazem $a^3 - b^2 = 2$. Determine os possíveis restos da divisão de a por 3. De que modo estes restos dependem de b?

6. Considere a recorrência $a_n = a_{n-1} + (n+1)2^n$, onde $a_1 = 4$.

   (a) Calcule a_n/n para alguns valores pequenos de n, compare o resultado com os valores de n e advinhe uma fórmula para a_n.

   (b) Prove que sua fórmula é verdadeira para todo $n \geq 1$ usando indução em n. Indique claramente cada etapa do método de indução.

Prova 2: segundo semestre de 1998

1. Seja $n = 1905$.
   (a) Verifique se n é um número de Carmichael.
   (b) Use o algoritmo chinês do resto para calcular o resto da divisão de 7^{1904} por n.
   (c) Verifique se n é um pseudoprimo para a base 7.

2. Determine, se existir, o primo p para o qual 223 é um fator primo de $2^p - 1$.

3. Que famoso matemático francês do século XVII inventou uma máquina mecânica de calcular para ajudar o pai na contabilidade de seus negócios? A resposta está contida na mensagem
   $$6531 \quad - \quad 4695 \quad - \quad 113$$
   que foi codificada usando o RSA, com chave pública $n = 8383$ e $e = 5467$.

4. Seja G um grupo finito e seja n um número inteiro positivo. Considere o conjunto $S_n = \{x^n : x \in G\}$. Isto é, os elementos de S_n são as potências n-ésimas de elementos de G.
   (a) Mostre que se G é *abeliano* então S_n é um subgrupo de G.
   (b) Calcule S_2 no caso em que $G = U(14)$.
   (c) Dê exemplo de um grupo finito não abeliano G para o qual S_3 *não* é um subrgupo.

5. Determine, se existirem, todas as soluções da equação $\phi(n) = 26$.

Prova Final: segundo semestre de 1998

1. Determine múltiplos de 3850 e 1773 cuja diferença seja 5.

2. Fatore 64777 usando o algoritmo de Fermat.

3. Calcule o resto da divisão de 2^{324179} por 41.

4. Determine um fator primo de $2^{22823} - 1$.

5. Determine, se existir, um primo $p > 5$ tal que $p + 2$ também é primo e $3 \cdot p \cdot (p + 2)$ é número de Carmichael.

6. Determine os subgrupos não-cíclicos de ordem 4 de $U(36)$.

7. Calcule p e q sabendo-se que são primos distintos, que $pq = 6011003$ e que $\phi(pq) = 6006000$.

8. Considere a afirmação: se $n \geq 1$, então 6 divide $n^3 - n$.
   (a) Prove a afirmação por indução em n. Identifique, claramente, cada etapa do processo de indução.
   (b) Prove a afirmação usando o algoritmo chinês do resto.

Prova 1: primeiro semestre de 1999

1. Ache múltiplos de 625 e 7947 cuja diferença é 4.

2. Ache dois fatores de 95677 pelo algoritmo de Fermat.

3. Ache o resto da divisão de 2^{5^6} por 257.

4. Sejam a e n inteiros positivos. Determine a e n sabendo-se que a e $a^n - 1$ são primos, e que $60 \leq n \leq 66$.

5. Determine se $(2^{30} + 1)!$ tem inverso módulo $(10^{10})! + 1$.

6. Determine qual é a maior potência de 2 que divide $3^{227} + 1$.

7. Considere a recorrência

$$s_n = 2 + s_{n-1}(s_{n-1} - 2) \quad \text{onde} \quad s_0 = 3.$$

   (a) Calcule $s_n - 1$ para $n = 0, 1, 2, 3$ e 4 e compare-os com as potências de 2. De que forma $s_n - 1$ depende de n? Use isto para advinhar uma fórmula fechada para s_n.

   (b) Mostre, por indução finita em n, a fórmula que você obteve em (a). Indique cuidadosamente cada passo da demonstração por indução.

Prova 2: primeiro semestre de 1999

1. Seja $n = 1387$.
   (a) Verifique se n é um número de Carmichael.
   (b) Use o algoritmo chinês do resto para calcular o resto da divisão de 2^{693} por n.
   (c) Determine se n é um pseudoprimo forte para a base 2.
   (d) Determine se n é um pseudoprimo para a base 2.

2. Ache todos os inteiros n para os quais $\phi(n) = 182$.

3. A primeira pessoa a escrever de maneira detalhada sobre a programação de computadores foi uma dama da sociedade inglesa do século passado. Para descobrir como ela se chamava, decifre a mensagem

   $$7790 \quad - \quad 6301$$

   que foi codificada usando o sistema RSA com chave pública $n = 8509$ e $e = 6653$.

4. Considere o primo $p = 10^9 + 21$ e seja $n = 16p + 1$. Sabe-se que $3^{8p} \equiv -1 \pmod{n}$ e que $2^{2p} \equiv -1 \pmod{n}$.
   (a) Mostre que n é primo.
   (b) Ache um gerador para $U(n)$.
   (c) Qual a ordem de $\overline{2^8}$ em $U(n)$?

Prova Final: primeiro semestre de 1999

1. Calcule, se existir, o inverso de 55 por 514229.

2. Seja n um inteiro positivo. Calcule o resto da divisão do número $4^{11236n} - 2^{4n}$ por 53. De que maneira o resto depende de n?

3. Prove, por indução em n, que $n! \geq 4^n$ para todo $n \geq 9$.

4. Determine o menor inteiro positivo que deixa resto 2 na divisão por 9, resto 3 na divisão por 8 e resto 8 na divisão por 11.

5. Ache um fator primo de $2^{88711} - 1$.

6. Seja $n = 821707$.
   (a) Calcule $\phi(n)$.
   (b) Qual o menor valor de $d > 0$ para o qual o par (n, d) pode servir como chave secreta para uma implementação do RSA?

7. Ache todos os subgrupos *não cíclicos* de ordem 4 do grupo $U(33)$.

Turma MAI–2002/1

Gabarito do teste 1

1. Ache múltiplos de 40320 e 29687 cuja diferença é 21.
   Aplicando o algoritmo euclidiano estendido, temos

Restos	Quocientes	x
40320	*	1
29687	*	0
10633	1	1
8421	2	-2
2212	2	3
1785	3	-11
427	1	14
77	4	-67
42	5	349
35	1	-416
7	1	765
0	*	*

   Como $40320\alpha + 29687\beta = 7$ e $\alpha = 765$, então

$$\beta = \frac{7 - 40320 \cdot 765}{29687} = -1039.$$

Logo

$$40320 \cdot 765 - 29687 \cdot 1039 = 7,$$

e multiplicando tudo por 3 obtemos

$$40320 \cdot 765 \cdot 3 - 29687 \cdot 1039 \cdot 3 = 21.$$

Portanto, os múltiplos de 40320 e 29687 cuja diferença é 21 são

$$40320 \cdot 765 \cdot 3 \text{ e } 29687 \cdot 1039 \cdot 3.$$

2. Explique porque você tem confiança de que sua resposta esteja correta.
   Porque, ao calcular β obtive um número inteiro. Se eu houvesse cometido um erro, é praticamente certo que o cálculo de β teria me dado um número não inteiro.
3. A solução encontrada em 1. é a única possível? Justifique sua resposta.
   Não. Há infinitas soluções, descritas pela fórmula

$$40320(765 \cdot 3 + 29687k) - 29687(\cdot 1039 \cdot 3 + 40320k) = 21,$$

onde k é um número inteiro qualquer.

Gabarito do teste 2

Ache dois fatores de 1297097 pelo algoritmo de fatoração de Fermat.

Calculando a raiz quadrada de $n = 1297097$, obtemos $1138,90$, que não é um inteiro. Portanto o número dado não é um quadrado perfeito e precisamos calcular a tabela do algoritmo:

x	$\sqrt{x^2 - n}$	Inteiro?
1139	$14,96$	não
1140	$50,02$	não
1141	$69,16$	não
1142	$84,06$	não
1143	$96,70$	não
1144	$107,88$	não
1145	$118,01$	não
1146	$127,35$	não
1147	$136,05$	não
1148	$144,24$	não
1149	$152,00$	sim

De modo que $x = 1149$ e $y = 152$. Logo os fatores são

$$x + y = 1149 + 152 = 1301 \text{ e}$$
$$x - y = 1149 - 152 = 997.$$

Para saber se estes números são mesmo fatores de n basta multiplicá-los; de fato

$$1301 \cdot 997 = 1297097,$$

portanto o resultado está correto.

Gabarito do teste 3

Considere os números primos $p_1 < \cdots < p_r$. Seja $N = p_1 \cdot p_2 \cdots p_r$ o produto destes primos e

$$S = \frac{N}{p_1} + \frac{N}{p_2} + \cdots + \frac{N}{p_r}.$$

1. Mostre, por contradição, que S é um número inteiro que não é divisível por nenhum dos primos $p_1, p_2, \cdots, p_r$.

2. Use (1) para dar uma demonstração (por contradição) de que existem infinitos números primos.

(1) Em primeiro lugar, cada p_i divide N, então S é inteiro. Por outro lado, se $i \neq j$ então p_i divide N/p_j. Portanto, se supusermos, por contradição, que p_i divide S, então p_i também divide

$$S - (\frac{N}{p_1} + \frac{N}{p_2} + \frac{N}{p_{i-1}} + \cdots + \frac{N}{p_{i+1}} + \cdots + \frac{N}{p_r} = \frac{N}{p_i}.$$

Mas N/p_i é um produto de primos diferentes de p_i, de modo que obtivemos uma contradição pelo teorema da fatoração única. Portanto, p_i não pode dividir S.

(2) Suponhamos, por contradição, que haja apenas uma quantidade finita de primos, digamos $p_1 < \cdots < p_r$. Tome $N = p_1 p_2 \cdots p_r$ e seja

$$S = \frac{N}{p_1} + \cdots + \frac{N}{p_r}.$$

Então S tem que ter um fator primo pelo teorema da fatoração única. Mas por (1) este fator tem que ser diferente de todos os primos $p_1, \ldots, p_r$. Como estamos supondo que estes são todos os primos que existem, temos uma contradição.

Esta demonstração da infinidade dos primos foi dada originalmente por Métrod em 1917.

Gabarito do teste 4

1. Calcule todas as potências distintas de $\overline{97}$ em $\mathbb{Z}_{233}$.
2. Use (1) calcular o resto da divisão de 97^{234111} por 233

(1) As potências distintas de $\overline{97}$ em $\mathbb{Z}_{233}$ são:

$$\begin{array}{cccc} \overline{97}^0 = \overline{1} & \overline{97}^1 = \overline{97} & \overline{97}^2 = \overline{89} & \overline{97}^3 = \overline{12} \\ \overline{97}^4 = \overline{232} & \overline{97}^5 = \overline{136} & \overline{97}^6 = \overline{144} & \overline{97}^7 = \overline{221} \end{array}$$

já que $\overline{97}^8 = \overline{1}$.
(2) Como $\overline{97}^8 = \overline{1}$, precisamos calcular o resto da divisão de 234111 por 8, que dá 7 (e quociente 29263). Logo

$$\overline{97}^{234111} = (\overline{97}^8)^{29263} \cdot \overline{97}^7 = \overline{1}^{29263} \cdot \overline{97}^7 = \overline{221}.$$

Portanto, o resto da divisão de 97^{234111} por 233 é 221.

Gabarito do teste 5

Determine todas as soluções da equação $2758x \equiv 7 \pmod{4167}$.

Aplicando o algoritmo euclidiano estendido a 4167 e 2758 descobrimos que o máximo divisor comum é 1 e que o valor correspondente a x é -1333. Portanto, $4167 \cdot (-1333) + 2758y = 1$, isto é, $y = 2014$. Assim, $4167 \cdot (-1333) + 2758 \cdot 2014 = 1$, que dá $\overline{2014} \cdot \overline{2758} = \overline{1}$ em $\mathbb{Z}_{4167}$. Logo $\overline{2758}$ tem inverso $\overline{2014}$ em $\mathbb{Z}_{4167}$. Multiplicando $2758x \equiv 7 \pmod{4167}$ por 2014, obtemos que $x \equiv 2014 \cdot 7 \equiv 1597 \pmod{4167}$. Concluímos que a solução é $x \equiv 1597 \pmod{4167}$, ou $x = 1597 + 4167k$, onde k é um número inteiro.

Gabarito do teste 6

Prove, por indução em n, que a soma das medidas dos ângulos internos de um polígono convexo de n lados é igual a $(n-2)\pi$. Indique claramente os diversos passos da indução: a base, a hipótese de indução e a demonstração do passo indutivo.

A afirmação a ser provada por indução é a seguinte:
$A(n)$: a soma das medidas dos ângulos internos de um polígono convexo de n lados é igual a $(n-2)\pi$.

Como o menor polígono tem 3 lados, a base da indução será $A(3)$. Mas neste caso o polígono é um triângulo, que tem soma dos ângulos internos igual a $\pi = (3-2)\pi$. Portanto, o resultado vale neste caso.

Hipótese de indução: Suponhamos que soma das medidas dos ângulos internos de qualquer polígono convexo de n lados é igual a $(n-2)\pi$.

Passamos a provar o passo de indução. Para isso suponha que temos um polígono convexo $P = ABC\cdots$ com n lados. Ligando os vétices A a C e apagando os lados AB e CB, obtemos um polígono P' de $n-1$ lados.

Portanto, pela hipótese de indução a soma dos ângulos internos de P' é $((n-1)-2)\pi = (n-3)\pi$. Para voltar ao polígono original de n lados P precisamos repor o triângulo ABC que tem soma dos ângulos internos π. Observe que o ângulo interno de P em A é igual à soma do ângulo interno de P' em A com o ângulo do triângulo ABC em A; e o mesmo ocorre em C. Logo, a soma dos ângulos internos de P é

$$\text{soma dos ângulos internos de } \ P' + \ \text{soma dos ângulos internos de } \ ABC$$

que, por sua vez, é igual a

$$(n-3)\pi + \pi = (n-2)\pi.$$

Assim, $A(n)$ é verdadeira para todo $n \geq 3$, pelo princípio de indução finita.

Gabarito do teste 7

1. Verifique se 2665 é um pseudoprimo para a base 3.
2. Determine um inteiro positivo b de modo que $10 < b < 2664$ e 2665 não é um pseudoprimo para a base b.

(1) Fatorando 2665 temos que $2665 = 5 \cdot 13 \cdot 41$. Vamos calcular 3^{2664} módulo cada um dos fatores primos de 2665. Usando o teorema de Fermat, temos

$$\begin{aligned} 3^{2664} \equiv (3^4)^{666} \equiv 1 \pmod 5 \\ 3^{2664} \equiv (3^{12})^{222} \equiv 1 \pmod{13} \\ 3^{2664} \equiv (3^{40})^{66} \cdot 3^{24} \equiv (3^{12})^2 \equiv 40^2 \equiv (-1)^2 \equiv 1 \pmod{41}. \end{aligned}$$

Portanto, $3^{2664} - 1$ é divisível por 5, e por 13 e por 41. Como estes números são primos distintos, segue que eles são dois a dois co-primos. Logo, $3^{2664} - 1$ é divisível pelo produto $5 \cdot 13 \cdot 41 = 2665$. Em outras palavras,

$$3^{2664} \equiv 1 \pmod{2665}.$$

(2) Um número n não pode ser pseudoprimo para uma base que seja um fator de n. Portanto, 2665 não é um pseudoprimo para a base 13, nem para a base 41.

Gabarito do teste 8

1. Determine o resto da divisão de 3^{279} por 2233, pelo teorema chinês do resto.
2. Verifique se 2233 é ou não um pseudoprimo forte para a base 3.

(1) Fatorando 2233 temos que $2233 = 7 \cdot 11 \cdot 29$. Vamos calcular 3^{279} módulo cada um dos fatores primos de 2233. Usando o teorema de Fermat, temos

$$\begin{aligned} 3^{279} \equiv 3^3 \equiv 6 \pmod 7 \\ 3^{279} \equiv 3^9 \equiv 4 \pmod{11} \\ 3^{279} \equiv 3^{27} \equiv 10 \pmod{29}. \end{aligned}$$

Portanto, se r é o resto da divisão de 3^{279} por 2233, então

$$\begin{aligned} r \equiv 6 \pmod 7 \\ r \equiv 4 \pmod{11} \\ r \equiv 10 \pmod{29}. \end{aligned}$$

Resolvendo o sistema pelo teorema chinês do resto, tiramos o valor de r na terceira equação, obtendo $r = 10 + 29y$ e substituindo na segunda equação, obtemos $10 + 29y \equiv 4 \pmod{11}$. Portanto, $7y \equiv 5 \pmod{11}$. Multiplicando esta congruência por 3, obtemos

$$21y \equiv 15 \pmod{11} \text{ que é equivalente a } y \equiv 7 mod 11.$$

Logo $y = 7 + 11z$ e assim

$$r = 10 + 29y = 10 + 29(7 + 11z) = 213 + 319z.$$

substituindo este último valor de r na primeira equação, obtemos $4z \equiv 3 \pmod 7$, que uma vez resolvida dá $z \equiv 6 \pmod 7$. Assim $z = 6 + 7w$, donde $r = 2127 + 2233w$. Logo o resto da divisão procurado é 2127.

(2) Para aplicar o teste de Miller a 2233 na base 3 precimos começar fatorando a maior potência de 2 de $2233 - 1 = 2232$. Mas $2232 = 2^3 \cdot 279$. Em seguida precisamos calcular a seguinte seqüência módulo 2233:

$$3^{279}, \quad 3^{279\cdot 2} \text{ e } \quad 3^{279\cdot 2^2}.$$

Mas já sabemos que $3^{279} \equiv 2127 \pmod{2233}$. Por outro lado,

$$\begin{aligned} 3^{279\cdot 2} &\equiv 2127^2 \equiv 71 \pmod{2233} \\ 3^{279\cdot 2^2} &\equiv 71^2 \equiv 575 \pmod{2233}. \end{aligned}$$

Como o primeiro elemento da seqüência não é congruente a 1, e nenhum elemento da da seqüência é congruente a 2232, então a saída do teste de Miller é composto. Portanto, 2233 não é pseudoprimo forte para a base 3.

Gabarito do teste 9

1. Seja G um grupo munido de uma operação $\star$ e a e b elementos de G. Mostre que se $a^3 = b^2 = a^2 \star b = e$, então $a = b = e$, onde e é o elemento neutro de G.

2. Determine todos os inteiros positivos $n > 1$ tais que $\phi(n) = 76$.

(1) Multiplicando $a^2 \star b = e$ á esquerda por a temos $a^3 \star b = a$. Como $a^3 = e$, então $a = b$. Mas $a^3 = b^2$, donde $a^3 = a^2$. Cancelando a^2, obtemos $a = e$. Mas já vimos que $a = b$, logo $a = b = e$.

(2) Temos que $76 = 2^2 \cdot 19$. Mas se p é um fator primo de n então $p - 1$ é divisor de $\phi(n)$. Tabelando os divisores de 76 temos

Como 39 e 77 são compostos, podemos descartá-los. Logo $n = 2^i \cdot 3^j \cdot 5^k$. Contudo, se n tem esta decomposição então os únicos fatores primos possíveis para $\phi(n)$ são 2, 3 e 5. Como 19 divide 76, não há valores de i, j e k tais que $\phi(n) = \phi(2^i \cdot 3^j \cdot 5^k) = 76$. Assim, a resposta é que a equação não tem solução.

Gabarito do teste 11

Possíveis fatores primos de n	Divisores de 76
2	1
3	2
5	$4 = 2^2$
39	$38 = 2 \cdot 19$
77	$76 = 2^2 \cdot 19$

1. Determine, se existir, um fator primo comum a $2^{41} - 1$ e 300!.

2. Seja $p > 11$ um número primo e $n = 4p + 1$. Tendo aplicado o teste de Miller a n na base 2, obtivemos a saída inconclusivo. Além disso, sabe-se que $2^{2p} \equiv n - 1 \pmod{n}$. Use esta informação e o teste de Lucas, para mostrar que n é primo.

(1) Vamos procurar por fatores primos comuns a 300! e $2^{41} - 1$. Os fatores primos de $2^{41} - 1$ são da forma $2 \cdot 41 \cdot k + 1$. Os fatores que forem comuns com 300! satisfarão $2 \cdot 41 \cdot k + 1 \leq 300$, o que dá $k \leq 3,6$. Portanto, $k = 1$, 2 ou 3. O fator correspondente a $k = 1$ é 83, que é primo. Entretanto,

$$2^{41} \equiv (2^{20}) \cdot 2 \equiv 37^2 \cdot 2 \equiv 41 \cdot 2 \equiv 82 \pmod{83}.$$

Logo 83 não é fator de $M(41)$. Por outro lado, se $k = 2$ então $2 \cdot 41 \cdot 2 + 1 = 165$ e se $k = 3$ então $2 \cdot 41 \cdot 3 + 1 = 247$, ambos compostos (247 é múltiplo de 13).

(2) Para aplicar o teste de Lucas a n precisamos calcular 2^{n-1}, $2^{(n-1)/2} = 2^{2p}$ e $2^{(n-1)/q} = 2^4$ módulo n. Mas o primeiro destes números é congruente a 1 porque n deu inconclusivo para o teste de Miller na base 2. Por outro lado

$$2^{(n-1)/2} \equiv 2^{2p} \equiv n - 1 \not\equiv 1 \pmod{n}.$$

Finalmente,

$$2^{(n-1)/q} \equiv 2^4 \equiv 16 \pmod{n},$$

que é menor que $n = 4p + 1 > 45$ e, portanto, não é congruente a 1 módulo n. Portanto, pelo teste de Lucas, este número é primo.

Na verdade, $n = 149$.

Universidade Federal do Rio de Janeiro
Departamento de Ciência da Computação

Números inteiros e criptografia—2002

Atenção

Neste semestre houve duas turmas de **Números inteiros e criptografia**, e os critérios de avaliação destas turmas foram diferentes. Na turma MAI foi realizado um teste por semana, na turma MAJ foram realizadas duas provas parciais e uma prova final. Este arquivo contém os testes e as provas das duas turmas e respectivos gabaritos.

Gabarito do teste 1

1. Use a fórmula da soma de uma progressão geométrica para provar a seguinte fórmula: se $a \neq b$ são números reais e n é um inteiro positivo, então

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + a^2b^{n-3} + ab^{n-2} + b^{n-1}).$$

2. Determine o inteiro n tal que $(3^{2^8})^{2^5} \cdot (3^{2^6})^{2^7}$ é igual a 3^{2^n}.

1. Como $a \neq b$, então um dos dois números é diferente de zero. Digamos que $a \neq 0$. Então

$$S = a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + a^2b^{n-3} + ab^{n-2} + b^{n-1}$$

é a soma de uma PG de primeiro termo $a_1 = a^{n-1}$, razão $q = b/a$ e último termo $a_n = b^{n-1}$. Pela fórmula da soma de uma PG temos que

$$S = \frac{a_1 - a_n q}{1-q} = \frac{a^{n-1} - b^{n-1} \cdot (b/a)}{1 - (b/a)} = \frac{a^n - b^n}{a-b}.$$

Isto é, $(a-b)S = a^n - b^n$, que é a fórmula desejada.

2. Como $(a^n)^m = a^{nm}$ temos que

$$(3^{2^8})^{2^5} = 3^{2^8 \cdot 2^5} \quad \text{e} \quad (3^{2^6})^{2^7} = 3^{2^6 \cdot 2^7}.$$

Mas $a^m \cdot a^n = a^{n+m}$, logo

$$3^{2^8 \cdot 2^5} = 3^{2^8+5} = 3^{13} \quad \text{e} \quad 3^{2^6 \cdot 2^7} = 3^{2^6+7} = 3^{13}.$$

Portanto,

$$(3^{2^8})^{2^5} \cdot (3^{2^6})^{2^7} = 3^{2^{13}} \cdot 3^{2^{13}} = 3^{2^{13}+2^{13}} = 3^{2 \cdot 2^{13}} = 3^{2^{14}}.$$

Assim, $n = 14$.

Gabarito do teste 2

1. Determine números inteiros x e y que sejam soluções da equação $7001x + 503y = 2$.

2. Mostre que esta equação tem infinitas soluções inteiras.

Aplicando o algoritmo euclidiano estendido, temos
Como $7001\alpha + 503\beta = 1$ e $\alpha = 184$, então

$$\beta = \frac{1 - 7001 \cdot 184}{503} = -2561.$$

Restos	Quocientes	x
7001	*	1
503	*	0
462	13	1
41	1	-1
11	11	12
8	3	-37
3	1	49
2	2	-135
1	1	184
0	*	*

Logo

$$7001 \cdot 184 - 503 \cdot 2561 = 1,$$

e multiplicando tudo por 2 obtemos

$$7001 \cdot 368 + 503 \cdot (-5122) = 2.$$

Portanto, $x = 368$ e $y = -5122$ são soluções da equação dada.
3. Uma família infinita de soluções é dada por:

$$7001(368 + 503k) + 503(-5122 - 7001k) = 2,$$

onde k é um número inteiro qualquer.

Gabarito do teste 3

Ache dois fatores de 4819589 pelo algoritmo de fatoração de Fermat.

Calculando a raiz quadrada de $n = 4819589$, obtemos $2195,35$, que não é um inteiro. Portanto o número dado não é um quadrado perfeito e precisamos calcular a tabela do algoritmo:

x	$\sqrt{x^2 - n}$	Inteiro?
2196	$53,169$	não
2197	$84,970$	não
2198	$107,772$	não
2199	$126,538$	não
2200	$142,867$	não
2201	$157,518$	não
2202	$170,923$	não
2203	$183,357$	não
2204	$195,005$	não
2205	206	sim

De modo que $x = 2205$ e $y = 206$. Logo os fatores são

$$x + y = 2135 + 206 = 2411 \text{ e}$$
$$x - y = 2135 - 206 = 1999.$$

Para saber se estes números são mesmo fatores de n basta multiplicá-los; de fato

Gabarito do teste 4

Seja $n \geq 2$ um inteiro positivo ímpar.

1. Mostre que se $(n-1)! + n$ é primo então n é primo.
2. Mostre se n for primo então o menor fator primo de $(n-1)! + n$ será maior que n.

(1) Se n for composto então terá um fator $k < n-1$, já que $\text{mdc}(n, n-1) = 1$. Logo k também será um fator de $(n-1)!$. Assim, k será um fator de $(n-1)! + n$.

(2) Seja q for o menor fator primo de $(n-1)!+n$. Se $q \leq n$ então temos duas possibilidades. A primeira é que $q < n$. Neste caso q divide $(n-1)!f$. Portanto, q divide $(n-1)! + n - (n-1)! = n$, o que contradiz o fato de q e n serem primos distintos. A outra possibilidade é que $n = q$. Neste caso q dividiria $(n-1)! + n - n = (n-1)!$. Mas isto também não é possível porque n é primo.

Gabarito do teste 5

1. Determine todas as potências distintas de $\overline{5}$ em $\mathbb{Z}_{71}$.
2. Use (1) para calcular o resto da divisão de $5^{213466876452}$ por 71.

(1) As potências distintas de $\overline{5}$ em $\mathbb{Z}_{71}$ são:

$$\overline{5}^0 = \overline{1} \quad \overline{5}^1 = \overline{5} \quad \overline{5}^2 = \overline{25} \quad \overline{5}^3 = \overline{125} = \overline{54} \text{ e } \overline{5}^4 = \overline{54} \cdot \overline{5} = \overline{57}.$$

Note que $\overline{5}^5 = \overline{1}$.
(2) Como $\overline{5}^5 = \overline{1}$, então

$$\overline{5}^{213466876458} = \overline{5}^{213466876455} \cdot \overline{5}^3 = \overline{1} \cdot \overline{54}.$$

Logo o resto que foi pedido é 54.

Gabarito do teste 6

Ache todas as soluções do seguinte sistema de congruências:

$$\begin{aligned} 5x + 2y &\equiv 1 \pmod{18} \\ 3x + 15y &\equiv 3 \pmod{18}. \end{aligned}$$

O inverso de $\overline{5}$ em $\mathbb{Z}_{18}$ é $\overline{11}$. Multiplicando a primeira congruência por 11, obtemos

$$55x + 22y \equiv 11 \pmod{18},$$

k	$y \pmod{18}$	$x \equiv 11 - 4y \pmod{18}$
0	2	3
1	8	15
2	14	9

ou seja $x+4y \equiv 11 \pmod{18}$. Portanto, $x \equiv 11-4y \pmod{18}$. Substituindo na segunda equação, obtemos

$$(33 - 12y) + 15y \equiv 3 \pmod{18}.$$

Isto é, $3y \equiv 6 \pmod{18}$. Convertendo para a equação de inteiros $3y-6 = 18k$. Dividindo tudo por 3, obtemos $y = 2 + 6k$. Obtemos, assim, as seguintes soluções distintas módulo 18:

Portanto, as soluções do sistema em $\mathbb{Z}_{18}$ são $x = \overline{3}$ e $y = \overline{2}$ ou $x = \overline{15}$ e $y = \overline{8}$.

Gabarito do teste 7

Considere a soma $S_n = 1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n!$.

1. Tabele S_n e $(n+1)!$ para $n = 1, 2, 3$ e 4, e advinhe uma fórmula fechada para S_n.
2. Prove sua fórmula por indução finita. Identifique claramente as várias etapas da sua demonstração: a base, o passo de indução e a hipótese de indução. Explicite também qual a condição de recorrência que está sendo utilizada.

(1) Tabelando, temos

n	S_n	$(n+1)!$
1	1	2
2	5	6
3	23	24
4	119	120

Portanto, $S_n = (n+1)! - 1$.

(2) Queremos provar a seguinte afirmação por indução finita:
$\mathbf{A}(n): \quad S_n = (n+1)! - 1$.

Lembre-se que S_n foi definida como sendo a soma $1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n!$.
Base da indução: a base é o caso $n = 1$. Temos que $S_1 = 1 \cdot 1! = 1$, ao passo que $(n+1)!- = 2 - 1 = 1$. Logo a fórmula vale neste caso.

Passamos ao *passo de indução*. A *hipótese de indução* nos diz que, para algum $k \geq 1$, $S_k = (k+1)! - 1$. A condição de recorrência nos diz que

$$S_{k+1} = S_k + (k+1) \cdot (k+1)!.$$

Logo, utilizando a hipótese de indução, obtemos

$$S_{k+1} = S_k + (k+1) \cdot (k+1)! = (k+1)! - 1 + (k+1) \cdot (k+1)!$$

Pondo $(k+1)!$ em evidência, obtemos,

$$S_{k+1} = (k+1)!(k+2) - 1 = (k+2)! - 1,$$

como queríamos mostrar. Portanto, pelo *princípio de indução finita* $S_n = (n+1)! - 1$ para todo $n \geq 1$.

Gabarito do teste 8

Sejam p e q dois primos positivos distintos maiores que 10^{2300}, e seja $n = pq$. Sabendo-se que n é um pseudoprimo para a base 2, calcule o resto da divisão 2^{q-1} por p. Justifique cada passo dos seus cálculos!
Sugestão: Divida n por $p-1$ e aplique o teorema de Fermat.

Como n é um pseudoprimo para a base 2, temos que $2^{n-1} \equiv 1 \pmod{n}$. Mas $n = pq$, de modo que $2^{n-1} \equiv 1 \pmod{p}$. Porém

$$n - 1 = p(q-1) + p - 1,$$

de modo que

$$1 \equiv 2^{n-1} \equiv 2^{p(q-1)} \cdot 2^{p-1} \pmod{p}.$$

Mas, pelo teorema de Fermat $2^{p-1} \equiv 1 \pmod{p}$ e $2^p \equiv 2 \pmod{p}$, donde

$$1 \equiv 2^{p(q-1)} \cdot 2^{p-1} \equiv 2^{q-1} \cdot 1 \pmod{p}.$$

Logo $2^{q-1} \equiv 1 \pmod{p}$ e o resto desejado é 1.

Gabarito do teste 9

1. Determine o resto da divisão de 2^{251} por 4017, pelo algoritmo chinês do resto.
2. Verifique se 4017 é ou não um pseudoprimo forte para a base 2.

(1) Fatorando 4017 temos que $4017 = 3 \cdot 13 \cdot 103$. Vamos calcular 2^{251} módulo cada um dos fatores primos de 4017. Usando o teorema de Fermat, temos

$$\begin{aligned} 2^{251} &\equiv 2 \pmod{3} \\ 2^{251} \equiv 2^{11} &\equiv 7 \pmod{13} \\ 2^{251} \equiv 2^{47} &\equiv 58 \pmod{103}. \end{aligned}$$

Portanto, se r é o resto da divisão de 2^{251} por 4017, então

$$\begin{aligned} r &\equiv 2 \pmod{3} \\ r &\equiv 7 \pmod{13} \\ r &\equiv 58 \pmod{103}. \end{aligned}$$

Resolvendo o sistema pelo teorema chinês do resto, tiramos o valor de r na terceira equação, obtendo $r = 58+103y$ e substituindo na segunda equação, obtemos $58+103y \equiv 7 \pmod{13}$. Portanto, $12y \equiv 1 \pmod{13}$. Multiplicando esta congruência por -1, obtemos

$$y \equiv 12 \pmod{13}.$$

Logo $y = 12 + 13z$ e assim

$$r = 58 + 103y = 58 + 103(12 + 13z) = 1294 + 1339z,$$

substituindo este último valor de r na primeira equação, obtemos $z + 1 \equiv 2 \pmod 3$, que uma vez resolvida dá $z \equiv 1 \pmod 3$. Assim $z = 1 + 3w$, donde $r = 2633 + 4017w$. Logo o resto da divisão procurado é 2633.

(2) Para aplicar o teste de Miller a 4017 na base 2 precimos começar fatorando a maior potência de 2 de $4017 - 1 = 4016$. Mas $4016 = 2^4 \cdot 251$. Em seguida precisamos calcular a seguinte seqüência módulo 4017:

$$2^{251}, \quad 2^{251\cdot 2}, \quad 2^{251\cdot 2^2} \text{ e } \quad 2^{251\cdot 2^3}.$$

Mas já sabemos que $2^{251} \equiv 2633 \pmod{4017}$. Por outro lado,

$$\begin{aligned} 2^{251\cdot 2} &\equiv 2633^2 \equiv 3364 \pmod{4017} \\ 2^{251\cdot 2^2} &\equiv 3364^2 \equiv 607 \pmod{4017} \\ 2^{251\cdot 2^3} &\equiv 607^2 \equiv 2902 \pmod{4017}. \end{aligned}$$

Como o primeiro elemento da seqüência não é congruente a 1, e nenhum elemento da da seqüência é congruente a 4016, então a saída do teste de Miller é composto. Portanto, 4017 não é pseudoprimo forte para a base 2.

Gabarito do teste 10

1. Mostre que, se existe um número ímpar n_0 tal que $\phi(n_0) = 2^r$ e n_0 não é múltiplo de 3, então existe um número ímpar m tal que $\phi(m) = 2^{r+1}$.
2. Use isto para achar um número ímpar m tal que $\phi(m) = 2^5$.

(1) Como 3 não divide n_0 e 3 é primo, temos que $\text{mdc}(n_0, 3) = 1$. Portanto, pelo teorema sobre a função ϕ,

$$\phi(3n_0) = \phi(3)\phi(n_0) = 2 \cdot 2^r = 2^{r+1}.$$

Assim, $3n_0$ é solução ímpar de $\phi(m) = 2^{r+1}$.

(2) Para usar (1) precisamos determinar uma solução ímpar para $\phi(n) = 2^4 = 16$. Mas 17 é primo, logo $\phi(17) = 17 - 1 = 16$. Portanto, por (1), $\phi(3 \cdot 17) = 2^5$. Logo a solução desejada é 51.

Gabarito do teste 11

A Enterpise NX-01 está visitando um planeta que enfrenta uma brutal guerra civil, quando intercepta uma mensagem criptografada. Há indícios de que as forças rebeldes pretendem seqüestrar um dos membros da tripulação, e a subcomandante T'Pol é encarregada de decifrar a mensagem. Ela descobre que se trata de um código semelhante ao usada na Terra do século XX, e conhecido como RSA. Sabendo que a mensagem interceptada foi

$$(9047, 7085) \quad 8655 - 1969 - 1563$$

decodifique-a e descubra qual o membro da tripulação que os rebeldes pretendem seqüestrar.

Fatorando $n = 9047$ pelo algoritmo de Fermat descobrimos que $p = 109$ e $q = 83$. Portanto, $\phi(n) = (p-1)(q-1) = 8856$. Calculando o inverso de $e = 7085$ pelo algoritmo euclidiano estendido, obtemos

Restos	Quocientes	x
8856	*	1
7085	*	0
1771	1	1
1	4	-4

Logo $1 = 8856 \cdot (-4) + 7085 \cdot d$, donde $d = 5$. Finalmente, podemos decodificar a mensagem:

$$8655^5 \equiv 2930 \pmod{n}, \quad 1969^5 \equiv 1220 \pmod{n} \text{ e } 1563^5 \equiv 1427 \pmod{n}$$

Portanto, a mensagem decodificada é $2930-1220-1427$. Trocando os números pelas letras correspondentes, temos TUCKER. Isto é, os rebeldes pretendem seqüestrar o comandante Tucker, oficial-chefe da engenharia. Para mais detalhes sobre a série ENTERPRISE visite `www.startrek.com`.

Gabarito do teste 12

1. Determine o menor fator primo do número de Mersenne $M(29) = 2^{29} - 1$ pelo método de Fermat.

2. Determine os subgrupos não cíclicos de ordem 4 de $U(44)$.

(1) Como 29 é primo, segue pelo método de Fermat, que os fatores primos de $2^{29} - 1$ são da forma $2 \cdot 29 \cdot k + 1 = 58k + 1$. Vamos tabelar estes fatores para valores de $k \geq 1$ e calcular o resto da divisão de 2^{29} por $q = 58k + 1$, quando q é primo. Obtemos

k	$q = 58k + 1$	composto?	resto de $2^p - 1$ por q
1	59	primo	58
2	117	múltiplo de 3	*
3	175	múltiplo de 5	*
4	233	primo	1

Logo $2^{29} \equiv 1 \pmod{59}$ e, portanto, 59 é o menor fator primo de $M(29)$.

(2) Para isso precisamos encontrar 3 elementos de ordem 2 em $U(44)$. Um destes elementos é $\overline{43} = \overline{-1}$. Podemos achar os outros por tentativa. Em primeiro lugar $\phi(44) = 20$, de modo que $U(44)$ tem 20 elementos, que são os números entre 1 e 43 que são ímpares e não são primos com 11. Vamos listar estes números até encontrar um cujo quadrado seja congruente a 1 módulo 44. Além disso, nenhum número menor que 7 pode satisfazer esta condição (porque o seu quadrado é menor que 44 e portanto não pode se reduzir a 1 módulo 44). Começamos a lista com 7:

$$\overline{7}^2 = \overline{5}, \quad \overline{9}^2 = \overline{37}, \quad \overline{13}^2 = \overline{37}, \quad \overline{15}^2 = \overline{5}, \quad \overline{17}^2 = \overline{25}, \quad \overline{19}^2 = \overline{9}, \quad \overline{21}^2 = \overline{1}.$$

Como

$$\overline{2143} = \overline{21-1} = \overline{-21} = \overline{23}$$

então $\overline{23}$ também tem ordem 2, e o subgrupo desejado é $\{\overline{1}, \overline{21}, \overline{23}, \overline{43}\}$.

Números inteiros e criptografia—2002/1 –Primeira Prova–Turma MAJ

Não serão aceitas respostas sem justificativa. Explique tudo o que você fizer.

1. Determine:
   (a) o inverso de 71 em $\mathbb{Z}_{8635}$;
   (b) dois fatores de 10217593 pelo algoritmo de fatoração de Fermat;
   (c) o resto da divisão de $2^{2^{21}}$ por 71;
   (d) o resto da divisão de 2^{705} por 2821 pelo algoritmo chinês do resto;
   (e) se 2821 é um pseudoprimo forte para a base 2;
   (f) se 2821 é um pseudoprimo para a base 2.

2. Sejam n e c inteiros positivos e r o resto da divisão de $2^{c!}$ por n. Considere $d = \text{mdc}(r-1, n)$. Lembre-se que $\text{mdc}(0, a) = a$, qualquer que seja a.
   (a) Mostre que se n tem um fator primo p tal que $p-1$ divide $c!$ então $r = 1$ ou p divide d.
   (b) Explique como isto poderia ser usado para achar um fator de um inteiro n. Que problemas você espera encontrar na aplicação deste método?

Gabarito da Prova

(1)

(a) Aplicando o algoritmo euclidiano estendido a 8635 e 71, obtemos

Restos	Quocientes	x
8635	$*$	1
71	$*$	0
44	121	1
27	1	-1
10	1	-3
7	1	5
3	1	-8
1	2	21

Portanto, $21 \cdot 8635 + 71y = 1$, donde

$$y = \frac{1 - 21 \cdot 8635}{71} = -2554.$$

Assim, $21 \cdot 8635 + 71 \cdot (-2554) = 1$, e passando a $\mathbb{Z}_{8635}$, obtemos

$$\overline{71} \cdot \overline{-2554} = \overline{1}.$$

Portanto o inverso de $\overline{71}$ em $\mathbb{Z}_{8635}$ é $\overline{-2554} = \overline{6081}$.

(b) Como $\sqrt{10217593} = 3196,497...$ não é inteiro, precisamos calcular a tabela

x	$\sqrt{x^2 - 10217593}$
3197	56,70...
3198	98,03...
3199	126,52...
3200	149,68...
3201	169,72...
3202	187,64...
3203	204

Donde concluímos que os fatores são

$$x - y = 3203 - 204 = 2999 \text{ e } \quad x + y = 3203 + 204 = 3407$$

(c) Como 71 é primo, podemos usar o teorema de Fermat para calcular o resto da divisão de $2^{2^{21}}$ por 71. Mas, segundo o teorema de Fermat, $2^{70} \equiv 1 \pmod{71}$. Portanto, precisamos determinar o resto da divisão de 2^{21} por 70. Usando a calculadora para fazer esta conta descobrimos que o resto é 22. Assim, pelo teorema de Fermat,

$$2^{2^{21}} \equiv 2^{22} \pmod{71}.$$

Usando a calculadora mais uma vez, verificamos que o resto da divisão de 2^{22} por 71 é 50. Logo o resto da divisão de $2^{2^{21}}$ por 71 é 50.
(d) Como $2821 = 7 \cdot 13 \cdot 31$, vamos calcular 2^{705} módulo cada um destes números. Assim, usando o teorema de Fermat para cada um destes fatores primos temos:

$$\begin{aligned} 2^{705} &\equiv 2^{702} \cdot 2^3 \equiv 2^3 \equiv 1 \pmod 7 \\ 2^{705} &\equiv 2^{696} \cdot 2^9 \equiv 2^9 \equiv 5 \pmod{13} \\ 2^{705} &\equiv 2^{690} \cdot 2^15 \equiv 2^15 \equiv 1 \pmod{31} \end{aligned}$$

Note que, da primeira e da última congruência concluímos que $2^{705} \equiv 1 \pmod{217}$, onde $217 = 7 \cdot 31$. Assim, se r é o resto da divisão de 2^{705} por 2821, então

$$\begin{aligned} r &\equiv 5 \pmod{13} \\ r &\equiv 1 \pmod{217}. \end{aligned}$$

Tirando o valor de r da segunda congruência, obtemos $r = 1 + 217k$, que substituído na segunda dá: $1 + 217k \equiv 5 \pmod{13}$. Isto é, $9k \equiv 4 \pmod{13}$. Mas $9 \equiv -4 \pmod{13}$, de modo que cancelando 4 na congruência obtemos

$$k \equiv -1 \equiv 12 \pmod{13}.$$

Assim, $k = 12 + 13t$, donde

$$r = 1 + 217(12 + 13t) = 2605 + 2821t.$$

Portanto, o resto da divisão de 2^{705} por 2821 é 2605.

(e) Para determinar se 2821 é pseudoprimo forte para a base 2 precisamos aplicar o teste de Miller para 2821 na base 2. Para começar temos que

$$2821 - 1 = 2820 = 2^2 \cdot 705.$$

Calculando agora a seqüência de potências de 2 módulo 2821, obtemos:

$$\begin{aligned} r_1 &\equiv 2^{705} \equiv 2605 \pmod{2821} \\ r_2 &\equiv 2^{2 \cdot 705} \equiv 2605^2 \equiv 1520 \pmod{2821} \end{aligned}$$

Como $r_1 \neq 1, 2820$ e $r_2 \neq 2820$ então o teste de Miller tem como saída composto. Logo 2821 não é um pseudoprimo forte para a base 2.

(f) Para verificar se 2821 é pseudoprimo para a base 2 calcular 2^{2820} módulo 2821. Mas, $2820 = 2^2 \cdot 705$. Como já sabemos que

$$2^{2 \cdot 705} \equiv 1520 \pmod{2821},$$

concluímos que

$$2^{4 \cdot 705} \equiv 1520^2 \equiv 1 \pmod{2821}.$$

Logo 2821 é um pseudoprimo para a base 2.

(2)

(a) Como $p-1$ divide $b!$, então $b! = (p-1)k$, para algum inteiro k, donde

$$r \equiv 2^{b!} \equiv (b^{p-1})^k \equiv 1 \pmod{p}.$$

Logo $r-1$ é divisível por p. Assim, se $r \neq 1$ então p é um divisor comum entre $r-1$ e n.

(b) O algoritmo é o seguinte:

Entrada: inteiros positivos n e b.
Saída: um fator de n ou inconclusivo.
Etapa 1: Calcule o resíduo r de $2^{b!}$ módulo n.
Etapa 2: Calcule $d = \text{mdc}(r-1, d)$. Se $d = 1$ ou $d = 0$ a saída é inconclusivo. Senão, a saída é d.

O algoritmo só funciona se b puder ser escolhido pequeno, do contrário fica impossível calcular $2^{b!}$. Portanto, para que o algoritmo tenha sucesso em determinar um fator de n é preciso que n tenha um fator primo p tal que $p-1$ possa ser fatorado completamente em termos de primos pequenos. Note que se isto não acontece então esperamos que o cálculo do máximo divisor comum retorne 1.

Números inteiros e criptografia—2002/2 –Segunda Prova–Turma MAJ

Não serão aceitas respostas sem justificativa. Explique tudo o que você fizer.

1. Determine:
   (a) o resto da divisão de 3^{385} por 342, pelo teorema chinês do resto;
   (b) todas as soluções de $\phi(n) = 92$;
   (c) um subgrupo não cíclico de ordem 11 do grupo $U(92)$.

2. Use o algoritmo do cálculo indicial para calcular $\log_{10} 17$ módulo 23.
   SUGESTÃO: Tome $S = \{2, 5\}$.

3. A mensagem abaixo foi codificada com o RSA usando como chave pública $n = 6077$ e $e = 4733$, decodifique-a.

   $$5441 - 4676.$$

   A relação entre letras e números neste caso é dada por

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

4. Seja $p > 0$ um primo e c um inteiro positivo. Mostre que se $2^{c!} \equiv 1 \pmod{p}$ e se $\overline{2}$ é um gerador do grupo $U(p)$ então todos os fatores primos de $p - 1$ são menores que c.

Gabarito da Prova

(1)
(a) Como $342 = 2 \cdot 3^2 \cdot 19$, então podemos quebrar a conta nas potências de primos. Aplicando o teorema de Fermat, teremos

$$3^{385} \equiv 1 \pmod 2$$
$$3^{385} \equiv 3^7 \equiv 2 \pmod{19},$$

ao passo que $3^{385} \equiv 0 \pmod 9$. Isto nos dá o sistema:

$$x \equiv 1 \pmod 2$$
$$x \equiv 0 \pmod 9$$
$$x \equiv 2 \pmod{19}.$$

Da última equação tiramos $x = 2 + 19y$. Substituindo na segunda equação chegamos a $y \equiv 7 \pmod 9$. Portanto, $y = 7 + 9t$, donde $x = 135 + 171t$. Substituindo na primeira equação chegamos a $t \equiv 0 \pmod 2$. Logo $t = 2u$ e $x = 135 + 342u$. Assim, o resto desejado é 135.

(b) Temos que $92 = 2^2 \cdot 23$. Mas se p é um fator primo de n então $p-1$ é divisor de $\phi(n)$. Tabelando os divisores pares de 92 (e o 1) temos

Possíveis fatores primos de n	Divisores de 92
2	1
3	2
5	$4 = 2^2$
47	$46 = 2 \cdot 23$
93	$92 = 2^2 \cdot 23$

Como 93 é composto, podemos descartá-lo. Logo $n = 2^i \cdot 3^j \cdot 5^k \cdot 47^m$. Passamos a nalisar os vários casos possíveis. Se $m \neq 0$, então

$$\phi(n) = \phi(2^i \cdot 3^j \cdot 5^k) \cdot 47^{m-1} \cdot 46.$$

Para que isto dê 92 precisamos ter que $m = 1$ e que $\phi(2^i \cdot 3^j \cdot 5^k) = 2$. Mas esta última igualdade só pode acontecer se $2^i \cdot 3^j \cdot 5^k$ é 3, 4 ou 6; como vimos em sala de aula. Portanto, devemos ter que $n = 3 \cdot 47$ ou $n = 4 \cdot 47$ ou $n = 6 \cdot 47$.

Por outro lado, se $m = 0$ então

$$\phi(n) = \phi(2^i \cdot 3^j \cdot 5^k),$$

cujos fatores primos são 2, 3 e 5; já que $2-1$, $3-1$ e $5-1$ não produzem novos fatores. Entretanto, 23 é primo e não podemos escrevê-lo a partir de 2, 3 e 5. Logo a equação $\phi(2^i \cdot 3^j \cdot 5^k) = 92$ não tem solução.

Portanto as únicas soluções do problema são 141, 188 e 282.

(c) Como $92 = 2^2 \cdot 23$, temos que

$$\phi(92) = \phi(2^2)\phi(23) = 2 \cdot 22 = 44.$$

Logo 11 divide 44 e é possível que o grupo $U(92)$ tenha um subgrupo de ordem 11. Entretanto, 11 é primo, e todo grupo cuja ordem é um número primo tem que ser cíclico. Portanto, não há subgrupos não cíclicos de ordem 11 em $U(92)$.

(2) Queremos achar a tal que $\overline{10}^a = \overline{17}$ em $U(23)$. Para isso vamos usar o algoritmo do cálculo indicial. Começamos escolhendo $S = \{2, 5\}$ e fatorando potências de $\overline{10}$ em termos de 2 e 5. Assim, temos em $U(23)$, que

$$\overline{10} = \overline{25}$$
$$\overline{10}^2 = \overline{2}^3.$$

Portanto,

$$1 \equiv \log 2 + \log 5 \pmod{22}$$
$$2 \equiv 3 \log 2 \pmod{22}.$$

Tirando o valor de $\log 2$ da segunda equação, obtemos

$$\log 2 \equiv 15 \cdot 2 \equiv 8 \pmod{22}.$$

Donde

$$\log 5 \equiv 1 - \log 2 \equiv 1 - 8 \equiv 15 \pmod{22}.$$

Finalmente,

$$\overline{17}^4 \cdot \overline{10} = \overline{2} \text{ em } U(23).$$

Logo,

$$\log 17 + 6 \equiv \log 2 + \log 5 \equiv 15 + 8 \equiv 1 \pmod{22}.$$

Donde, $\log 17 \equiv 17 \pmod{22}$.

(3) Aplicando o algoritmo de fatoração de Fermat descobrimos em dois passos que $n = 6077 = 59 \cdot 103$. Portanto,

$$\phi(6077) = (59 - 1)(103 - 1) = 5916.$$

Aplicando o algoritmo euclidiano estendido a 5916 e $e = 4733$, obtemos o inverso de e módulo $\phi(n)$, que é 5. Decodificando a mensagem, temos as seguintes congruências módulo 6077:

$$5441^5 \equiv 2130$$
$$4676^3 \equiv 2110.$$

Assim, a mensagem decodificada é $2130 - 2110$ que transliterada dá LULA.

(4) Suponhamos que $\overline{2}$ é um gerador do grupo $U(p)$, onde p é um primo positivo. Como $U(p)$ tem ordem $\phi(p) = p - 1$, e $\overline{2}$ é um gerador de $U(p)$, então $\overline{2}$ tem ordem $p - 1$. Como $2^{c!} \equiv 1 \pmod{p}$, segue pelo lema chave, que a ordem de $\overline{2}$ deve dividir $c!$. Portanto, $p - 1$ divide $c!$. Em particular cada fator primo de $p - 1$ divide $c!$. Mas todos os fatores de $c!$ são menores que c, donde concluímos que todos os fatores primos de $p - 1$ são menores que c.

Números inteiros e criptografia—2002/2 –Prova Final–Turma MAJ

Não serão aceitas respostas sem justificativa. Explique tudo o que você fizer.

1. Determine:

   (a) $\mathrm{mdc}(a, c)$ sabendo-se que a, b e c são inteiros maiores que $2^{200!}$ e que c divide $a + b$ e $\mathrm{mdc}(a, b) = 1$;

   (b) dois fatores de 53897891 pelo algoritmo de Fermat;

   (c) o resto da divisão de 2^{185} por 741;

   (d) se 741 é um pseudoprimo forte para a base 2;

   (e) o menor fator primo, maior que 11200, de $2^{97} - 1$.

2. A mensagem abaixo foi codificada com o RSA usando como chave pública $n = 7597$ e $e = 4947$, decodifique-a.

   $$7272 - 7295 - 5789.$$

   A relação entre letras e números neste caso é dada por

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

3. Seja G um grupo cíclico finito gerado por um elemento a.

   (a) Mostre que se S é um subgrupo de G e se m é o menor inteiro positivo tal que $a^m \in S$, então a^m gera S.

   (b) Dê um exemplo de um grupo G que não é cíclico, mas cujos subgrupos próprios são todos cíclicos.

Gabarito da Prova

(1)
(a) Como $a + b = ck$, temos que $a = ck - b$ e pelo resultado auxiliar usado para provar o algoritmo euclidiano, segue que $\text{mdc}(a, c) = \text{mdc}(a, b)$. Mas $\text{mdc}(a, b) = 1$ por hipótese. Logo $\text{mdc}(a, c) = 1$.

(b) Como a raiz quadrada de 53897891 é $7341,51...$, que não é inteira, devemos montar a tabela

x	$\sqrt{x^2 - 10217593}$
7342	84,10...
7343	147,50...
7344	190,90...
7345	226,12...
7346	256,56...
7347	283,75...
7348	308,56...
7349	331,52...
7350	353

Donde concluímos que os fatores são

$$x - y = 7350 - 353 = 6997 \text{ e } x + y = 7350 + 353 = 7703.$$

(c) Como $741 = 3 \cdot 13 \cdot 19$, então vamos calcular 2^{185} módulo 3, módulo 13 e módulo 19 e colar o resultado usando o teorema chinês do resto. Mas, pelo teorema de Fermat:

$$\begin{aligned} 2^{185} &\equiv 2 \pmod 3 \\ 2^{185} &\equiv 2^5 \equiv 6 \pmod{13} \\ 2^{185} &\equiv 2^5 \equiv 13 \pmod{19} \end{aligned}$$

Portanto, precisamos resolver o sistema:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 6 \pmod{13} \\ x &\equiv 13 \pmod{19} \end{aligned}$$

pelo teorema chinês do resto. Mas da última equação $x = 13 + 19t$. Substituindo na segunda equação, obtemos $13 + 19t \equiv 6 \pmod{13}$, ou seja $6t \equiv 6 \pmod{13}$. Como 6 é inversível módulo 13, podemos cancelá-lo, obtendo $t \equiv 1 \pmod{13}$. Portanto, $x = 32 + 247v$. Substituindo na primeira equação $32 + 247v \equiv 2 \pmod 3$, donde $v \equiv 0 \pmod 3$. Logo $x \equiv 32 \pmod{741}$.

(d) Para verificar se 741 é pseudoprimo forte, aplicamos o teste de Miller a $n = 741$. Mas $n - 1 = 740 = 2^2 \cdot 185$. Logo precisamos calcular 2^{185} e $2^{185 \cdot 2}$ módulo 741. Mas temos que $2^{185} \equiv 32 \pmod{741}$ e

$$2^{2 \cdot 185} \equiv (2^{185})^2 \equiv 283 \pmod{741}$$

Como $32 \neq 1, 740$ e $283 \neq 740$ então este número não é um pseudoprimo forte para a base 2.

(e) Pelo método de Fermat, como 97 é primo, os fatores primos de $2^{97} - 1$ são da forma $2 \cdot 97 \cdot k + 1 = 194k + 1$. Como queremos um fator maior que 11200, devemos tomar $194k + 1 > 11200$, donde $k > (11200 - 1)/194 = 57, 72....$ Mas se $k = 58$, obtemos $194 \cdot 58 + 1 = 11253$ que é múltiplo de 3. Por outro lado, se $k = 59$, então $194 \cdot 59 + 1 = 11447$ que é primo. De fato,

$$2^{97} \equiv (2^{20})^4 \cdot 2^{17} \equiv 6899^4 \cdot 5155 \equiv 8920 \cdot 5155 \equiv 1 \pmod{11447}.$$

(2) Fatorando $n = 7597$ pelo algoritmo de Fermat, obtemos $p = 107$ e $q = 71$. Donde $\phi(n) = 7420$. Como $e = 4947$, devemos calcular o inverso de e módulo $\phi(n)$ pelo algoritmo euclidiano estendido, o que dá $d = 3$. Decodificando a mensagem, obtemos:

$$\begin{aligned} 7272^3 &\equiv 2718 \pmod{7597} \\ 7295^3 &\equiv 3114 \pmod{7597} \\ 5789^3 &\equiv 2829 \pmod{7597}. \end{aligned}$$

Substituindo as letras por números de acordo com a tabela, obtemos RIVEST.

(3)
(a) Seja $S \neq \{e\}$ um subgrupo do grupo cíclico G gerado pelo elemento a. Escolha o elemento a^m de S para o qual $m > 0$ é o menor possível. Vamos mostrar que a^m gera S. Seja a^n outro elemento de S. Dividindo n por m obtemos $n = mq + r$ onde $0 \leq r \leq m - 1$. Mas

$$a^n = (a^m)^q \star a^r \text{ donde } a^r = a^n \star ((a^m)^q)'.$$

Como a^n e a^m pertencem a S, que é um subgrupo, temos que $a^r \in S$. Mas isto só é possível se $r = 0$, porque se $r > 0$ então teríamos uma contradição com a escolha de m. Portanto $r =$ e $a^n = (a^m)^q$, de modo que a^m gera S.
(b) Um exemplo é D_6, já que os subgrupos próprios têm ordens 1, 2 ou 3. Como 2 e 3 são primos estes subgrupos têm que ser todos cíclicos.

2003/1–Testes e Gabaritos

Teste 1

Seja $n > 2^{100!}$ um número inteiro. Determine $\text{mdc}(6n+1, 6n! + (n-1)! + 6n - 3)$.

Solução

Como $6n! + (n-1)! + 6n - 3 > 6n + 1$, vamos dividir o primeiro pelo segundo, como no algoritmo euclidiano estendido. Obtemos $6n! + (n-1)! + 6n - 3 = (6n+1)(n-1)! + 6n - 3$. Portanto, pelo resultado auxiliar,

$$\text{mdc}(6n+1, 6n! + (n-1)! + 6n - 3) = \text{mdc}(6n+1, 6n-3).$$

Como $6n + 1 = 6n - 3 + 4$, segue pelo resultado auxiliar mais uma vez que $\text{mdc}(6n + 1, 6n - 3) = \text{mdc}(6n - 3, 4)$. Mas $6n - 3 = 3(2n - 1)$, que é um número ímpar. Como 4 é uma potência de 2, não pode haver nenhum fator maior que 1 comum a $6n - 3$ e 4. Logo $\text{mdc}(6n + 1, 6n - 3) = 1$.

Outra maneira de calcular $\text{mdc}(6n-3, 4)$ (baseada na solução de Moyses Afonso Assad Cohen). Podemos considerar dois casos. No primeiro caso n é par e podemos escrevê-lo na forma $n = 2k$. Neste caso, precisamos calcular $\text{mdc}(12k-3, 4)$. Mas, dividindo $12k-3$ por 4, obtemos

$$12k - 3 = 4 \cdot 4k - 3$$

de modo que, pelo resultado auxiliar visto em aula,

$$\text{mdc}(12k - 3, 4) = \text{mdc}(-3, 4) = \text{mdc}(3, 4) = 1.$$

No segundo caso n é ímpar, de modo que $n = 2k + 1$. Então, precisamos calcular $\text{mdc}(12k + 3, 4)$. Mas repetindo um argumento semelhante ao anterior, verificamos que

$$\text{mdc}(12k + 3, 4) = \text{mdc}(3, 4),$$

de modo que $\text{mdc}(12k + 3, 4) = 1$. Portanto, independente de n ser par ou ímpar, temos que

$$\text{mdc}(6n - 3, 4) = 1.$$

Teste 2

Ache dois fatores de 70362379 pelo algoritmo de fatoração de Fermat.

Calculando a raiz quadrada de $n = 70362379$, encontramos $8388,228$, que não é um inteiro. Portanto o número dado não é um quadrado perfeito e precisamos calcular a tabela do algoritmo:

De modo que $x = 8398$ e $y = 405$. Logo os fatores são

$$x + y = 8398 + 405 = 8803 \text{ e}$$
$$x - y = 8398 - 405 = 7993.$$

x	$\sqrt{x^2-n}$	Inteiro?
8389	$113,76$	não
8390	$172,39$	não
8391	$215,64$	não
8392	$251,56$	não
8393	$282,96$	não
8394	$311,21$	não
8395	$337,11$	não
8396	$361,16$	não
8397	$383,70$	não
8398	405	sim

Para saber se estes números são mesmo fatores de n basta multiplicá-los; de fato

$$8803 \cdot 7993 = 70362379,$$

portanto o resultado está correto.

Teste 3

Seja $n > 3^{564231}$ um número inteiro. Mostre que se n é composto então n divide $(n-1)!$

Esta é a minha solução original. Ela é complicada e usa vários resultados do Capítulo 2:

Se n for composto, podemos usar o teorema da fatoração única para escrevê-lo na forma

$$n = p_1^{e_1} \cdots p_t^{e_t},$$

onde $p_1 < \cdots < p_t$ são primos e os expoentes $e_1, \ldots, e_t$ são todos positivos.

Vou supor primeiro que $t \geq 2$; quer dizer, que na fatoração de n há, pelo menos, dois fatores primos distintos. Neste caso,

$$p_j^{e_j} < n,$$

para $j = 1, \ldots, t$. Assim, $p_j^{e_j} \leq n-1$, de modo que $p_j^{e_j}$ divide $(n-1)!$. Como os p_j são primos distintos (e, portanto, primos entre si) segue do resultado auxiliar (2) provado em sala que o produto $p_1^{e_1} \cdots p_t^{e_t}$ divide $(n-1)!$. Como este produto é igual a n, provamos o que queríamos.

Suponhamos, agora, que $n = p^e$, onde p é um primo e $e > 1$ (pois n tem que ser composto). Neste caso, tanto p^{e-1} quanto $2p$ são menores que $n-1 = p^e - 1$, de modo que

$$2n = 2p \cdot p^{e-1}$$

divide $(n-1)!$, como desejávamos mostrar. Mas cuidado: este argumento é falso se $n = 4$ (por quê?).

Esta é a solução garimpada do que os alunos fizeram:

Se n é composto, então existem a e b inteiros, tais que

- $n = ab$ e
- $1 < a < n$ e $1 < b < n$.

Como a e b são menores que n, então a e b são menores ou iguais a $n-1$. Assim, se $a \neq b$ então tanto a quanto b são números que aparecem multiplicados quando calculamos $(n-1)!$. Mas isto significa que $n = ab$ divide $(n-1)!$. Resta discutir o caso $a = b$. Neste

quando $a \leq 1 - \sqrt{2}$ ou $a \geq 1 + \sqrt{2}$. Como só os as positivos nos interessam, podemos descartar $a \leq 1 - \sqrt{2}$. Por outro lado, o único inteiro que não satisfaz $a \geq 1 + \sqrt{2}$ é $a = 2$. Concluímos que $2a \leq n - 1$ só não vale se $n = 4$, que não ocorre por causa da restrição ao n dada no problema.

Teste 4

Seja $n > 3^{564231}$ um número inteiro *ímpar*.

1. Determine um inteiro positivo r tal que
$$2^n + 1 = 2M(r) + 3.$$
2. Use (1) e os resultados sobre números de Mersenne que estudamos para mostrar que $2^n + 1$ é múltiplo de 3.

Resolução

(1) Como n é ímpar, podemos escrevê-lo na forma $n = 2q+1$, para algum inteiro positivo q. Então
$$2^n + 1 = 2^{2q+1} + 1 = 2^{2q+1} - 2 + 3 = 2(2^{2q} - 1) + 3 = 2M(2q) + 3.$$

(2) Sabemos que se d divide n então $2^d - 1$ divide $2^n - 1$. Como 2 divide $2q$, segue que $2^2 - 1 = 3$ divide $2^{2q} - 1$. Portanto, $2^{2q} - 1 = 3k$, para algum inteiro positivo k. Substituindo em (1):
$$2^n + 1 = 2M(2q) + 3 = 2 \cdot 3k + 3 = 3(2k + 1),$$
de modo que 3 divide $2^n + 1$.

Teste 5

1. Determine as potências distintas de $\overline{9}$ em $\mathbb{Z}_{55}$.
2. Use (1) para calcular o resto de $9^{23456789}$ por 55.

Resolução

(1) As potências são as seguintes:

$$\begin{aligned}
\overline{9}^0 &= \overline{1} \\
\overline{9}^1 &= \overline{9} \\
\overline{9}^2 &= \overline{81} = \overline{26} \\
\overline{9}^3 &= \overline{981} = \overline{729} = \overline{14} \\
\overline{9}^4 &= \overline{914} = \overline{126} = \overline{16} \\
\overline{9}^5 &= \overline{916} = \overline{144} = \overline{34} \\
\overline{9}^6 &= \overline{934} = \overline{306} = \overline{31} \\
\overline{9}^7 &= \overline{931} = \overline{279} = \overline{4} \\
\overline{9}^8 &= \overline{94} = \overline{36} = \overline{36} \\
\overline{9}^9 &= \overline{936} = \overline{324} = \overline{49} \\
\overline{9}^{10} &= \overline{949} = \overline{441} = \overline{1}
\end{aligned}$$

onde todos estes cálculos foram realizados em $\mathbb{Z}_{55}$.

(2) Queremos achar $0 \leq r \leq 54$ tal que $\overline{9}^{20000} = \overline{r}$ em $\mathbb{Z}_{55}$. Mas,

$$\overline{9}^{23456789} = (\overline{9}^{10})^{2345678} \cdot \overline{9}^9 = (\overline{1})^{2345678} \cdot \overline{49} = \overline{49}.$$

Portanto, o resto da divisão de $9^{23456789}$ por 55 é 49.

Teste 6

Determine o inverso de $\overline{463}$ em $\mathbb{Z}_{51662}$.

Resolução

Aplicando o algoritmo euclidiano estendido, temos

Restos	Quocientes	x
51662	*	1
463	*	0
269	111	1
194	1	-1
75	1	2
44	2	-5
31	1	7
13	1	-12
5	2	31
3	2	-74
2	1	105
1	1	-179
0	*	*

Como $51662\alpha + 463\beta = 1$ e $\alpha = -179$, então

$$\beta = \frac{1 - 51662 \cdot (-179)}{463} = 19973.$$

Logo

$$51662 \cdot (-179) + 463 \cdot 19973 = 1,$$

e considerando esta equação em $\mathbb{Z}_{51662}$, obtemos

$$\overline{51662} \cdot \overline{-179} + \overline{463} \cdot \overline{19973} = \overline{1}.$$

Como $\overline{51662} = \overline{0}$ em $\mathbb{Z}_{51662}$, concluímos que

$$\overline{463} \cdot \overline{19973} = \overline{1}.$$

Portanto, o inverso de $\overline{463}$ em $\mathbb{Z}_{51662}$ é $\overline{19973}$.

Teste 7

Prove, por indução finita, que qualquer conjunto com n elementos tem $n(n-1)/2$ subconjuntos de 2 elementos. Explicite claramente cada etapa da demonstração: a base, a hipótese de indução e o passo de indução.

Resolução

A base da indução consiste em mostrar que o resultado vale para um conjunto com 1 elemento. Neste caso não há subconjuntos de 2 elementos. Por outro lado, tomando $n = 1$ em $n(n-1)/2$, obtemos 0, que é o valor correto.

Suponha, agora, que um conjunto de $k \geq 1$ elementos tem $k(k-1)/2$ subconjuntos de 2 elementos. Esta é a hipótese de indução. Queremos mostrar que uma fórmula semelhante vale para um conjunto com $k+1$ elementos, que é o passo de indução.

Mas um conjunto de $k+1$ elementos é constituído por um conjunto com k elementos S ao qual se juntou um elemento a. Os subconjuntos de 2 elementos de $S \cup \{a\}$ são de dois tipos: os que contêm a, e os que não contêm a. Mas um subconjunto de $S \cup \{a\}$ que não contém a é subconjunto de S e, pela hipótese de indução, temos $k(k-1)/2$ destes. Por outro lado, os subconjuntos de $S \cup \{a\}$ que contêm a são da forma $\{a, b\}$, onde b é um elemento de S. Como S tem k elementos, há k subconjuntos deste tipo. Com isto temos um total de

$$\frac{k(k-1)}{2} + k = \frac{k^2 - k + 2k}{2} = \frac{k(k+1)}{2},$$

subconjuntos de $S \cup \{a\}$. Mas isto corresponde a fazer $n = k+1$ na fórmula dada, o que completa o passo de indução. Portanto, pelo princípio de indução finita, todo conjunto de n elementos tem $n(n-1)/2$ subconjuntos de 2 elementos, qualquer que seja $n \geq 1$.

Teste 8

Seja $n = 697$. Sabe-se que $42^{87} \equiv 83 \pmod{n}$. Determine:

1. se n é um pseudoprimo forte para a base 42;
2. se n é um pseudoprimo para a base 42.

Resolução

(1) Precisamos aplicar o teste de Miller a $n = 697$. Fatorando a maior potência de 2 de $n - 1 = 696$, obtemos: $696 = 2^3 \cdot 87$. Devemos, agora, calcular a seqüência

$$42^8 7,\ 42^{2\cdot 87} \text{ e } 42^{2^2 \cdot 87},$$

módulo 697. Já sabemos que $42^{87} \equiv 83 \pmod{n}$. Disto concluímos que

$$42^{2\cdot 87} \equiv 83^2 \equiv 616 \pmod{697}$$

e que

$$42^{2^2 \cdot 87} \equiv 616^2 \equiv 288 \pmod{697}.$$

Como o primeiro elemento da seqüência não é congruente a 1, e nenhum elemento da seqüência é congruente a $696 \equiv -1 \pmod{697}$, concluímos que este número não é um pseudoprimo forte para a base 42.

(2) Para verificar se 697 é um pseudoprimo para a base 42, devemos calcular 42^{696} módulo 697. Contudo, $696 = 2^3 \cdot 87$, e já sabemos que $42^{2^2 \cdot 87} \equiv 288 \pmod{697}$. Logo,

$$42^{696} \equiv 42^{2^3 \cdot 87} \equiv (42^{2^2 \cdot 87})^2 \equiv 288^2 \equiv 1 \pmod{697}.$$

Portanto, 697 é um pseudoprimo para a base 42.

Teste 9

Determine o resto da divisão de 3^{2584} por 1581, usando o algoritmo chinês do resto.

Resolução

Fatorando 1581 temos que $1581 = 3 \cdot 17 \cdot 31$. Vamos determinar o resto de 3^{2584} por 3, por 17 e por 31 e colar o resultado usando o algoritmo chinês do resto. Mas

$$\begin{aligned} 3^{2584} &\equiv 0 \pmod{3} \\ 3^{2584} &\equiv (3^{16})^{161} \cdot 3^8 \equiv 3^8 \equiv 16 \pmod{17} \\ 3^{2584} &\equiv (3^{30})^{86} \cdot 3^4 \equiv 3^4 \equiv 19 \pmod{31} \end{aligned}$$

Portanto, para determinar o resto da divisão de 3^{2584} por 1581, precisamos resolver o sistema

$$\begin{aligned} r &\equiv 0 \pmod{3} \\ r &\equiv 16 \pmod{17} \\ r &\equiv 19 \pmod{31} \end{aligned}$$

pelo algoritmo chinês do resto. Para isto tiramos o valor de r da terceira equação, que é $r = 19 + 31y$ e substituímos na segunda, obtendo $19 + 31y \equiv 16 \pmod{17}$. Isto dá $14y \equiv 14 \pmod{17}$. Como 14 e 17 são primos entre si, então podemos cancelar 14 da equação, obtendo $y \equiv 1 \pmod{17}$. Daí $y = 1 + 17t$, donde

$$r = 19 + 31y = 19 + 31 \cdot (1 + 17t) = 50 + 527t.$$

Substituindo isto na primeira equação, obtemos $50 + 527t \equiv 0 \pmod{3}$; ou seja, $2t \equiv -2 \pmod{3}$. Como o mdc entre 2 e 3 é 1, podemos cancelar 2 módulo 3 obtendo $t \equiv -1 \pmod{3}$; ou ainda $t \equiv 2 \pmod{3}$. Assim, $t = 2 + 3w$, de modo que

$$r = 50 + 527t = 50 + 527 \cdot (2 + 3w) = 1104 + 1581w.$$

Portanto, o resto da divisão de 3^{2584} por 1581 é 1104.

Teste 7b

Prove, por indução em n que

$$1^2 - 2^2 + 3^2 - 4^2 + \cdots + (-1)^{n-1} n^2 = \frac{(-1)^{n-1} n(n+1)}{2},$$

para todo $n \geq 1$. Sua demonstração deve explicitar a base, a hipótese de indução, o passo de indução e a recorrência que está sendo usada para provar a fórmula acima.

Resolução

Para facilitar a notação, seja

$$S_n = 1^2 - 2^2 + 3^2 - 4^2 + \cdots + (-1)^{n-1} n^2.$$

A base da indução consiste em mostrar que o resultado vale para $n = 1$ elemento. Neste caso, $S_n = 1$ e

$$\frac{(-1)^{n-1} n(n+1)}{2} = \frac{(-1)^{1-1} 1(2)}{2} = 1,$$

de modo que a fórmula está correta para $n = 1$ e a base é verdadeira.

Suponha, agora, que

$$S_k = 1^2 - 2^2 + 3^2 - 4^2 + \cdots + (-1)^{k-1} k^2 = \frac{(-1)^{k-1} k(k+1)}{2},$$

para algum $k \geq 1$. Esta é a hipótese de indução.

Para provar o passo de indução, precisamos de uma recorrência que, neste caso, será

$$S_{k+1} = S_k + (-1)^k (k+1)^2.$$

Portanto,

$$\begin{aligned} S_{k+1} &= S_k + (-1)^k k^2 \quad \text{(pela recorrência)} \\ &= \frac{(-1)^{k-1} k(k+1)}{2} + (-1)^k (k+1)^2 \quad \text{(pela hipótese de indução).} \end{aligned}$$

Efetuando as contas, obtemos,

$$\frac{(-1)^{k-1} k(k+1)}{2} + (-1)^k (k+1)^2 = \frac{(-1)^k (k+1)(2(k+1) - k)}{2} = \frac{(-1)^k (k+1)(k+2)}{2}.$$

Logo,

$$S_{k+1} = \frac{(-1)^k (k+1)(k+2)}{2}.$$

Mas isto corresponde a fazer $n = k + 1$ na fórmula dada, o que completa o passo de indução. Portanto, pelo princípio de indução finita,

$$1^2 - 2^2 + 3^2 - 4^2 + \cdots + (-1)^{n-1} n^2 = \frac{(-1)^{n-1} n(n+1)}{2},$$

qualquer que seja $n \geq 1$.

Teste 10

1. Determine dois subgrupos não cíclicos de ordem 4 em $U(40)$.

2. Em sua viagem pelo Quadrante Delta a nave da Federação Voyager fez contato com uma civilização cujo nível cultural era equivalente ao da Terra no início do século XX. Infelizmente um outro povo deste Quadrante já havia chegado ao local, e o grupo avançado que desceu ao planeta foi capturado. Tendo conseguido fugir, mas estando sem seu comunicador, o oficial de segurança Tuvok usou um dos rádios locais para enviar uma mensagem à Voyager sobre o perigo na superfície. Para evitar que a mensagem fosse lida pelo inimigo, e sem ter acesso a nenhum computador, Tuvok codificou a mensagem à mão utilizando um velho código terrestre, o RSA. A mensagem enviada por Tuvok foi:

   $$(6667, 4331) \qquad 5810\text{–}2676\text{–}3692$$

   Decodifique-a e descubra qual o povo que havia invadido o planeta.

Resolução

(1) Um grupo não cíclico de ordem 4 tem o elemento neutro além de três elementos de ordem 2. Para começar $\phi(40) = \phi(8)\phi(5) = 4 \cdot 4 = 16$, que é divisível por 4. Portanto, pelo teorema de Lagrange, $U(36)$ pode ter subgrupos de ordem 4. Para determinar estes subgrupos precisamos achar os elementos de ordem 2. Para isso basta procurar os elementos cujo quadrado é igual a 1 módulo 40. Estes elementos são: $\overline{9}, \overline{11}, \overline{19}, \overline{21}, \overline{29}, \overline{31}$ e $\overline{39}$. Mas nem toda combinação de três destes elementos com a identidade produzirá um subgrupo. A maneira mais simples de achar os subgrupos é escolher dois dos elementos, multiplicá-los e assim achar quem é o terceiro. Por exemplo, escolhendo $\overline{9}$ e $\overline{11}$, vemos que $\overline{9} \cdot \overline{11} = \overline{19}$, de modo que $\{\overline{1}, \overline{9}, \overline{11}, \overline{19}\}$, é um dos subgrupos possíveis. Outro subgrupo possível é $\{\overline{1}, \overline{9}, \overline{39}, \overline{31}\}$.

(2) Fatorando $n = 6667$ pelo algoritmo de Fermat, descobrimos que $p = 59$ e $q = 113$. Portanto,

$$\phi(n) = \phi(6667) = \phi(59)\phi(113) = 58 \cdot 112 = 6496.$$

Usando o algoritmo euclidiano estendido para inverter $e = 4331$ módulo $\phi(n) = 6496$, obtemos que $d = 3$. Finalmente, podemos decodificar a mensagem:

$$\begin{aligned} 5810^3 &\equiv 2010 \pmod{6667} \\ 2676^3 &\equiv 352 \pmod{6667} \\ 3692^3 &\equiv 423 \pmod{6667} \end{aligned}$$

Mas 2010352423 = KAZON. Portanto, foram os Kazon que invadiram o planeta antes da chegada da Voyager.

Teste 11

1. Seja $p > 2$ um primo. Sabe-se que o máximo divisor comum entre $2^p - 1$ e 1000! é o número primo 431. Determine p.

2. Sabe-se que 1361 é primo e que $3^{1361} \equiv 3093 \pmod{8167}$. Use isto e o teste de Lucas para provar que 8167 é um número primo.

   SUGESTÃO: 1361 é fator de 8166.

Resolução

(1) Os fatores primos de $2^p - 1$ são todos da forma $2kp + 1$. Logo, se 431 é fator de $2^p - 1$, então tem que ser desta forma. Assim, $2kp = 430 = 2 \cdot 5 \cdot 43$. Portanto, p pode ser 2, 5 ou 43. Mas, $p > 2$, por hipótese e se p fosse 5 então $2^5 - 1 = 31 < 431$. Temos, então, que $p = 43$.

(2) Seja $n = 8167$. Fatorando $n - 1$, obtemos $8166 = 2 \cdot 3 \cdot 1361$. Portanto, para aplicar o teste de Lucas para a base 3, precisamos calcular 3^{n-1}, $3^{(n-1)/1361}$, $3^{(n-1)/2}$ e $3^{(n-1)/3}$. Mas sabemos que $3^{1361} \equiv 3093 \pmod{8167}$. Logo,

$$3^{(n-1)/3} \equiv (3^{1361})^2 \equiv (3093)^2 \equiv 3092 \pmod{8167},$$

e, de modo semelhante,

$$3^{(n-1)/2} \equiv (3^{1361})^3 \equiv (3093)^2 \cdot 3093 \equiv 3092 \cdot 3093 \equiv 8166 \equiv -1 \pmod{8167}.$$

Além disso,

$$3^{(n-1)/1361} \equiv 3^6 \equiv 729 \pmod{8167}.$$

Portanto, $3^{(n-1)/1361}$, $3^{(n-1)/2}$ e $3^{(n-1)/3}$ não são congruentes a 1 módulo 8167. Finalmente,

$$3^{(n-1)} \equiv (3^{(n-1)/2})^2 \equiv (-1)^2 \equiv 1 \pmod{8167},$$

de modo que provamos, pelo teste de Lucas, que 8167 é primo.

Universidade Federal do Rio de Janeiro
Departamento de Ciência da Computação

Números inteiros e criptografia—2003/2

Atenção

Neste semestre houve duas turmas de **Números inteiros e criptografia**. Em ambas as turmas foi realizado um teste com 2 questões a cada 15 dias, além da prova final. Este arquivo contém os testes e as provas das duas turmas e respectivos gabaritos. Os testes sem gabaritos foram preparados para serem feitos usando um sistema de computação algébrica. Neste semestre o sistema usado foi o YACAS.

2003/2 —Turma MAI–Teste 1

1. Seja $n > 2^{100!}$ um número inteiro. Use o algoritmo euclidiano estendido para calcular $d = \text{mdc}(5n+3, 3n+2)$ e dois inteiros α e β tais que $d = (5n+3)\alpha + (3n+2)\beta$.

2. Use o algoritmo de fatoração de Fermat para determinar dois fatores de 1212779.

Resolução

1. Vamos aplicar o algoritmo euclidiano estendido a estes dois números. Observando que $5n+3 > 3n+2$, temos

Restos	Quocientes	x	y
$5n+3$	*	1	0
$3n+2$	*	0	1
$2n+1$	1	1	-1
$n+1$	1	-1	2
n	1	2	-3
1	1	-3	5

Portanto, $\text{mdc}(5n+3, 3n+2) = 1$, ao passo que $\alpha = -3$ e $\beta = 5$. Para provar que o resultado está certo basta calcular

$$-3(5n+3) + 5(3n+2) = 15n - 9 + 15n + 10 = 1.$$

2. Calculando a raiz quadrada de $n = 1212779$, encontramos $1101,262457$, que não é um inteiro. Portanto o número dado não é um quadrado perfeito e precisamos calcular a tabela do algoritmo:

x	$\sqrt{x^2 - n}$	Inteiro?
1102	$40,311$	não
1103	$61,886$	não
1104	$77,698$	não
1105	$90,807$	não
1106	$102,259$	não
1107	$112,561$	não
1108	$122,004$	não
1109	$130,774$	não
1110	139	sim

De modo que $x = 1110$ e $y = 139$. Logo os fatores são

$$x + y = 1110 + 139 = 1249 \text{ e}$$
$$x - y = 1110 - 139 = 971.$$

Para saber se estes números são mesmo fatores de n basta multiplicá-los; de fato

$$971 \cdot 1294 = 1212779,$$

portanto o resultado está correto.

DCC-UFRJ–Números inteiros e criptografia–2003/2
Turma MAI–Teste 2

1. O objetivo desta questão é dar uma outra demonstração de que existem infinitos números primos. Para isso, suponha que exista um número finito de primos, que são todos menores que um número inteiro positivo $n \geq 3$.

   1. Mostre $\text{mdc}(n! - 1, n!)$ deve ser diferente de 1.
   2. Mostre que (1) leva a uma contradição, e use isto para provar que existem infinitos números primos.

2. Determine o resto da divisão de $2^{987657} + 5^{15}$ módulo 65.

Resolução

1. (1) Suponha que haja um número finito de primos, todos menores que $n \geq 3$. Então $n! \geq 2$ e $n! - 1 \geq 3$. Portanto, ambos são inteiros maiores ou iguais a 2, e pelo Teorema da Fatoração Única ambos têm fatores primos. Entretanto, como todos os primos são menores que n, então todos são fatores de $n!$. Portanto, qualquer que seja o fator primo de $n! - 1$, ele terá que dividir $n!$. Em particular, $n!$ e $n! - 1$ têm um fator comum, de modo que seu máximo divisor comum não pode ser igual a 1.

1. (2) Como $\text{mdc}(n!, n! - 1)$ divide $n!$ e $n! - 1$, então deve dividir $n! - (n! - 1) = 1$. Mas isto implica que $\text{mdc}(n!, n! - 1) = 1$, contradizendo (1). isto significa que a hipótese feita, no início da questão, de que todos os primos são menores que n tem que estar errada. Portanto, não existe nenhum inteiro $n \geq 3$ que seja maior que todos os primos. Mas isto só pode acontecer se houver infinitos números primos.

2. Por um lado,

$$2^6 \equiv 64 \equiv -1 \pmod{65},$$

por outro, as potências de 5 módulo 65 são

$$\begin{aligned} 5^1 &\equiv 5 \pmod{65} \\ 5^2 &\equiv 25 \pmod{65} \\ 5^3 &\equiv 60 \pmod{65} \\ 5^4 &\equiv 40 \pmod{65} \\ 5^5 &\equiv 5 \pmod{65}. \end{aligned}$$

Portanto,

$$2^{987657} + 5^{15} \equiv 2^{987654} \cdot 2^3 + (5^5)^3 \equiv (2^6)^{164609} \cdot (2^3) + 5^3 \equiv -8 + 60 \equiv 52 \pmod{65}.$$

DCC-UFRJ–Números inteiros e criptografia–2003/2
Turma MAI–Teste 3

1. Considere a soma

$$S_n = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{n \cdot (n+1)}.$$

   1. Tabele S_n para alguns valores pequenos de n ($n = 1, 2, 3$ e 4, por exemplo) e advinhe uma fórmula fechada F_n para S_n.

   2. Prove, por indução em n, que $S_n = F_n$ para todo inteiro $n \geq 1$. Explicite a base da indução, a hipótese de indução, a recursão que está sendo usada e o passo de indução.

2. Sabe-se que 701 é primo. Determine todos os valores inteiros de n para os quais $n^{701} + 699n + 1$ deixa resto zero na divisão por 701.

Resolução

1. (1) Tabelando S_n contra n temos

n	S_n
1	1/2
2	2/3
3	3/4
4	4/5

Logo, a fórmula parece ser $F_n = n/(n+1)$.

Queremos provar por indução que $S_n = F_n$ para qualquer $n \geq 1$.
Base da indução: A base corresponde a mostrar que a afirmação vale quando $n = 1$. Mas, $S_1 = 1/2$ pela tabela e $F_1 = 1/2$ por um cálculo direto. Logo $S_1 = F_1$ e a base da indução é verdadeira.
Hipótese de indução: Para algum $k \geq 1$ temos que $S_k = F_k$.
Recursão: $S_{k+1} = S_k + 1/(k+1)(k+2)$.

Passo de indução: Temos que

$$\begin{aligned}
S_{k+1} &= S_k + \frac{1}{(k+1)(k+2)} \quad \text{(recursão)} \\
&= F_k + \frac{1}{(k+1)(k+2)} \quad \text{(hipótese de indução)} \\
&= \frac{k}{(k+1)} + \frac{1}{(k+1)(k+2)} \\
&= \frac{1}{(k+1)}\left(k + \frac{1}{(k+2)}\right) \\
&= \frac{1}{(k+1)}\left(\frac{k(k+2)+1}{(k+2)}\right) \\
&= \frac{1}{(k+1)} \cdot \frac{(k+1)^2}{(k+2)} \quad \text{(produto notável)} \\
&= \frac{(k+1)}{(k+2)},
\end{aligned}$$

o que mostra que $S_k = F_k$ implica que $S_{k+1} = F_{k+1}$. Portanto, pelo Princípio de indução finita temos que $S_n = F_n$ para todo $n \geq 1$.

2. Pelo teorema de Fermat,

$$n^{701} + 699n + 1 \equiv n + 699n + 1 \equiv 700n + 1 \equiv -n + 1 \pmod{701}.$$

Mas, $-n + 1 \equiv 0 \pmod{701}$ só acontece se $n \equiv 1 \pmod{701}$. Portanto, a solução da congruência é $n = 1 + 701k$, qualquer que seja k inteiro.

DCC-UFRJ–Números inteiros e criptografia–2003/2
Turma MAI–Teste 4

Seja $n = 4123$.

1. Determine se n é um número de Carmichael.
2. Calcule, pelo algoritmo chinês do resto, o resto da divisão de 5^{2061} por n.
3. Determine se n é um pseudoprimo forte para a base 5.
4. Determine se n é um pseudoprimo para a base 5.

Resolução

(1) Vamos usar o teorema de Korselt. Cada primo tem multiplicidade um na fatoração de $n = 7 \cdot 19 \cdot 31$. Porém, $n \equiv 13 \not\equiv 1 \pmod{30}$, de modo que n não é um número de Carmichael.

(2) Usando o teorema de Fermat, temos que:

$$\begin{aligned} 5^{2061} &\equiv 5^3 \equiv 6 \pmod 7 \\ 5^{2061} &\equiv 5^9 \equiv 1 \pmod{19} \\ 5^{2061} \equiv 5^{21} \equiv (5^4)^5 \cdot 5 &\equiv 5^5 \equiv 1 \pmod{31}. \end{aligned}$$

Isto nos dá o sistema de congruências

$$\begin{aligned} r &\equiv 6 \pmod 7 \\ r &\equiv 1 \pmod{19} \\ r &\equiv 1 \pmod{31}. \end{aligned}$$

Pela unicidade do teorema chinês do resto, temos que as duas últimas congruências se tornam $r \equiv 1 \pmod{589}$. De modo que basta resolver o sistema

$$\begin{aligned} r &\equiv 6 \pmod 7 \\ r &\equiv 1 \pmod{589}. \end{aligned}$$

Tirando o valor de r da última congruência, obtemos $r = 1 + 589t$. Substituindo na primeira

$$1 + 589t \equiv 6 \pmod 7,$$

que é equivalente a $t \equiv 5 \pmod 7$. Assim,

$$r = 1 + 589(5 + 7y) = 2946 + 4123y.$$

Logo o resto desejado é 2946.

(3) Precisamos aplicar o teste forte de composição a 4123 na base 5. Mas $n-1 = 2 \cdot 2061$. Como

$$5^{2061} \equiv 2946 \not\equiv 1, 4122 \pmod{4123},$$

concluímos que o teste tem saída *composto* para base 5. Portanto, 4123 não é um pseudoprimo forte para a base 5.

(4) Para verificar se o número é pseudoprimo para a base 5, precisamos calcular 5^{4122} módulo 4123. Contudo,

$$5^{4122} \equiv 5^{2 \cdot 2061} \equiv (5^{2061})^2 \equiv 2946^2 \equiv 1 \pmod{4123}.$$

Portanto, 4123 é um pseudoprimo para a base 5.

DCC-UFRJ–Números inteiros e criptografia–MAI–2003/2–Teste 5

O premiado carneiro *Garoto Lanoso* estará em exposição na Feira do Estado. Como houve várias ameaças à sua segurança, o grande xerife Pepe Legal e seu fiel ajudante Babaloo foram contratados para protegê-lo. Decifre a mensagem abaixo e descubra o nome do vilão que deseja raptar o Garoto Lanoso para transformá-lo em churrasco.

$(10127333, 6069773)$ 2179193 - 7703087 - 2527011 - 6115153 - 6385721

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Espaço = 99.

DCC-UFRJ–Números inteiros e criptografia–MAI–2003/2–Teste 6

1. Determine todos os valores possíveis de n para os quais $\phi(n) = 164$.
2. Seja G um grupo abeliano e sejam $S_1 \neq S_2$ subgrupos de ordem p de G, onde p é um número primo. Prove que $S_1 \cap S_2$ consiste apenas do elemento neutro de G.
3. Seja $p > 10^{500}$ um número primo. Calcule $\text{mdc}(2^p - 1, p!)$. De que forma este resultado depende de p?
4. Considere o número $n = 2^2 \cdot 1063 + 1$. Sabe-se que $2^{1063} \equiv 561 \pmod{n}$. Use o teste de Lucas para provar que n é primo.

Resolução

1. Em primeiro lugar, $164 = 2^2 \cdot 41$. Por outro lado, se p é um primo que divide n, então $p - 1$ divide $\phi(n) = 164$. Portanto, De modo que os possíveis fatores primos de n são 2,

$p-1$	p
1	2
2	3
4	5
82	83
164	165

3, 5 e 83. Isto é, $n = 2^e \cdot 3^f \cdot 5^g \cdot 83^h$. Vamos analisar as escolhas de expoentes caso a caso.
Caso 1: $h > 0$.

Neste caso,

$$\begin{aligned}\phi(n) &= \phi(2^e \cdot 3^f \cdot 5^g)\phi(83^h) \\ &= \phi(2^e \cdot 3^f \cdot 5^g)83^{h-1}82.\end{aligned}$$

Para que isto seja igual a $164 = 2 \cdot 82$, devemos ter que $h = 1$ e que

$$\phi(2^e \cdot 3^f \cdot 5^g) = 2.$$

Mas esta última condição implica que $2^e \cdot 3^f \cdot 5^g$ é 3, 4 ou 6. Temos assim que n é $3 \cdot 83 = 249$ ou $4 \cdot 83 = 332$ ou $6 \cdot 83 = 498$.

Portanto, de agora em diante, podemos supor que $h = 0$.

Caso 2: $h = 0$.

Neste caso $n = 2^e \cdot 3^f \cdot 5^g$, de modo que os únicos fatores primos possíveis para $\phi(n)$ são $2, 3$ e 5 (já que $2 - 1 = 1$, $3 - 1 = 2$ e $5 - 1 = 4$). Assim, $\phi(n) = 164 = 4 \cdot 41$ não pode ter solução já que 41 é primo e não pode ser fator de $\phi(n)$.

2. Como S_1 tem ordem p, então é um subgrupo cíclico, e cada um de seus elementos diferentes de e (o elemento neutro) gera todo o S_1. O mesmo vale para S_2. Portanto, se $S_1 \cap S_2$ tivesse um elemento em comum, diferente de e, então este elemento seria tanto um gerador de S_1, quanto de S_2, de maneira que teríamos $S_1 = S_2$. Como os dois subgrupos são distintos, resta apenas a possibilidade de $S_1 \cap S_2 = \{e\}$.

3. Segundo a fórmula geral, todos os fatores primos de $2^p - 1$ são da forma $2pk + 1$ e, portanto, maiores que p. Mas $p!$ só tem fatores primos menores que p. Logo, mesmo que $2^p - 1$ seja composto, não pode ter nenhum fator em comum com $p!$. Assim, $\text{mdc}(2^p - 1, p!) = 1$, e este resultado é independente do valor de p.

4. Para aplicar o teste de Lucas a n, precisamos fatorar $n - 1$ e mostrar que

$$b^{n-1} \equiv 1 \pmod{n},$$

e que, para cada fator primo p de $n - 1$ vale

$$b^{(n-1)/p} \not\equiv 1 \pmod{n}.$$

Como $n = 2^2 \cdot 1063 + 1$, e como 1063 é primo, então os fatores primos de $n - 1$ são 2 e 1063. Por outro lado, $2^{1063} \equiv 561 \pmod{n}$ implica que

$$2^{2 \cdot 1063} \equiv (2^{1063})^2 \equiv 561^2 \equiv 4252 \pmod{n}$$

e também que,

$$2^{4 \cdot 1063} \equiv (2^{2 \cdot 1063})^2 \equiv 4252^2 \equiv 1 \pmod{n}.$$

Portanto,

$$\begin{aligned} 2^{n-1} &\equiv 2^{4 \cdot 1063} \equiv 1 \pmod{n}, \\ 2^{(n-1)/2} &\equiv 2^{2 \cdot 1063} \equiv 4252 \not\equiv 1 \pmod{n}, \\ 2^{(n-1)/1063} &\equiv 2^4 \equiv 16 \not\equiv 1 \pmod{n}, \end{aligned}$$

de modo que n é primo pelo teste de Lucas.

DCC-UFRJ–Números inteiros e criptografia–MAI–2003/2
Prova Final

1. Determine dois fatores de 925417 pelo algoritmo de Fermat.

2. Resolva a congruência $3421x \equiv 23 \pmod{139}$.

3. Dê exemplo de um inteiro $n > 10$ para o qual $\text{mdc}(2^n - 1, n!) \neq 1$.

4. Prove, por indução em n, que $3^n < n!$ para todo $n > 6$. Identifique claramente a base da indução, a hipótese de indução e o passo de indução.

5. Seja $n = 1387 = 19 \cdot 73$.

   (a) Determine o resto da divisão de 2^{693} por n, pelo algoritmo chinês do resto.

   (b) Use isto para verificar se n é um pseudoprimo para a base 2.

6. Seja G um grupo abeliano provido de uma operação $*$, e sejam a e b elementos de G de ordem 3. Suponha que $a \notin \langle b \rangle$.

   (a) Mostre que ab tem ordem 3.

   (b) Qual a ordem do menor subgrupo de G que contém a e b?

7. Uma implementação do RSA usa como chave pública o par $n = 600079$ e $e = 3$. Determine d sabendo-se que $\phi(n) = 598384$.

DCC-UFRJ–Números inteiros e criptografia–2003/2
Turma MAJ–Teste 1

1. Ache múltiplos de 155019 e 1389 cuja diferença seja 12

2. Sejam $2 < p < q$ dois primos ímpares e seja $n = pq$.

   1. Determine x e y (em função de p e q) tais que $n = x^2 - y^2$.

   2. Use (1) para determinar o número de tentativas para achar x que o algoritmo de fatoração de Fermat terá que fazer até obter um fator próprio de n.

Resolução

1. Vamos aplicar o algoritmo euclidiano estendido a estes dois números. Observando que $155019 > 1389$, temos

Restos	Quocientes	x
155019	*	1
1389	*	0
840	111	1
549	1	-1
291	1	2
258	1	-3
33	1	5
27	7	-38
6	1	43
3	4	-210

Portanto, $\text{mdc}(155019, 1389) = 3$, ao passo que $\alpha = -210$ e

$$\beta = \frac{3 - 155019 \cdot (-210)}{1389} = 23437.$$

Logo,

$$-155019 \cdot 210 + 1389 \cdot 23437 = 3,$$

e multiplicando tudo por 4:

$$-4 \cdot 155019 \cdot 210 + 4 \cdot 1389 \cdot 23437 = 12.$$

Assim, os múltiplos desejados são

$$4 \cdot 155019 \cdot 210 \text{ e } 4 \cdot 1389 \cdot 23437.$$

2. (1) Comparando $n = x^2 - y^2$ com $n = pq$, temos que

$$(x - y)(x + y) = pq,$$

donde $x - y = p$ e $x + y = q$, já que $p < q$. Resolvendo os dois sistemas lineares, obtemos

$$x = \frac{q+p}{2} \text{ e } y = \frac{q-p}{2}.$$

(2) Como o algoritmo inicia o cálculo da tabela a partir de $[\sqrt{n}] + 1$, então o número de x que precisa tentar até fatorar n é igual a

$$[\sqrt{n}] + 1 - \frac{q+p}{2}.$$

DCC-UFRJ–Números inteiros e criptografia–2003/2
Turma MAJ–Teste 2

1. Determine um fator primo ímpar de $3^{26302677} - 1$.

2. Mostre, usando congruências, que $3^{2n+1} + 2^{n+2}$ é divisível por 7, qualquer que seja $n \geq 1$ inteiro.

Resolução

1. Usando a identidade

$$3^{km} - 1 = (3^k - 1)(3^{k(m-1)} + 3^{k(m-2)} + \cdots + 3^2 + 3^k,$$

e o fato de que 26302677 é divisível por 3, temos que $3^-1 = 2 \cdot 13$ divide $3^{26302677} - 1$. Logo, um fator primo de $3^{26302677} - 1$ é 13.

2. Como

$$3^{2n+1} + 2^{n+2} = (3^2)^n \cdot 3 + 2^n \cdot 2^2 = 9^n \cdot 3 + 2^n \cdot 4,$$

obtemos, usando congruência módulo 7,

$$3^{2n+1} + 2^{n+2} \equiv 9^n \cdot 3 + 2^n \cdot 4 \equiv 2^n \cdot 3 + 2^n \cdot 4 \pmod 7.$$

Pondo 2^n em evidência

$$3^{2n+1} + 2^{n+2} \equiv 2^n(3+4) \equiv 2^n \cdot 7 \equiv 0 \pmod 7.$$

Portanto, $3^{2n+1} + 2^{n+2}$ é divisível por 7, qualquer que seja $n \geq 1$.

DCC-UFRJ–Números inteiros e criptografia–2003/2
Turma MAJ–Teste 3

1.

1. Determine, por tentativa, para que valores de n vale a desigualdade $2n + 3 \leq 2^n$?

2. Prove que a resposta obtiva em (1) está correta usando o Princípio de Indução Finita. Explicite a base da indução, a hipótese de indução e o passo de indução.

2. Seja $p > 10^{2000}$ um número primo. Determine o resto da divisão de

$$1^p + 2^p + 3^p + \cdots + (p-1)^p$$

por p.

Resolução

1. A desigualdade vale para todo $n \geq 4$. Vou provar isto por indução em n.

Base da indução: Para $n = 4$ temos que $2n + 3 = 2 \cdot 4 + 3 = 11$ ao passo que $2^4 = 16$, de modo que $2n + 3 \leq 2^n$ neste caso.

Hipótese de indução: $2k + 3 \leq 2^k$ para algum $k \geq 4$.

Passo de indução: Temos que

$$\begin{aligned} 2(k+1) + 3 &= 2k + 3 + 2 \\ &= 2^k + 2 \quad \text{(hipótese de indução)} \\ &\leq 2 \cdot 2^k \quad \text{(pois } 2 \leq 2^k\text{)} \\ &\leq 2^{k+1} \end{aligned}$$

o que mostra que $2k + 3 \leq 2^k$ implica que $2(k+1) + 3 \leq 2^{k+1}$. Portanto, pelo Princípio de indução finita temos que $2n + 3 \leq 2^n$ para todo $n \geq 1$.

2. Pelo teorema de Fermat $a^p \equiv a \pmod{p}$. Portanto,

$$1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 1 + 2 + 3 + \cdots + (p-1) \pmod{p}.$$

Contudo, pela fórmula da soma de uma PA,

$$1 + 2 + 3 + \cdots + (p-1) = \frac{(p-1)p}{2}.$$

Observe que se trata de um número inteiro, já que p é ímpar e, portanto, 2 divide $p - 1$. Mas isto significa que p divide a soma, donde

$$1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 1 + 2 + 3 + \cdots + (p-1) \equiv 0 \pmod{p}.$$

Logo, o resto é 0.

DCC-UFRJ–Números inteiros e criptografia–2003/2
Turma MAI–Teste 4

1. Seja $n = 340561$.

1. Determine se n é um número de Carmichael.

2. Determine se n é um pseudoprimo forte para a base 7.

3. Determine o menor inteiro positivo b para o qual n não é um pseudoprimo para a base b.

2. Use o algoritmo chinês do resto para achar o menor número que, se dividido por 9 deixa resto 3, se dividido por 11 deixa resto 4, e se dividido por 5 deixa resto 2.

DCC-UFRJ–Números inteiros e criptografia–MAJ–2003/1–Teste 5A

Em uma festa embalada ao som dos *Impossíveis* um criminoso de helicóptero roubou uma tiara de um milhão de dólares. Avisados pelo Grande Chefe, Os Impossíveis saíram à caça do criminoso. Decifre a mensagem abaixo e descubra quem foi o ladrão da tiara.

$(14371121, 3916391)$ 6112117 -10286021 - 7213824.

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Espaço = 99.

DCC-UFRJ–Números inteiros e criptografia–MAJ–2003/2–Teste 6

1. Determine todos os valores de $n > 1$ para os quais $\phi(n^2) = n$.

2. Quais são os subgrupos de ordem 4 de $U(563)$?

3. Seja $p > 2$ um número primo. Prove que, se $2^p - 1$ é composto, então seu menor fator primo não pode dividir o número de Fermat $F(p)$.

4. Use o Teste de Primalidade para provar que 79 é um número primo.

Resolução

1. Seja $n = p_1^{e_1} \cdots p_k^{e_k}$ a fatoração de n em primos $p_1 < \cdots < p_k$, onde $e_j > 0$ para $j = 1, \ldots, k$. Então,

$$\begin{aligned}\phi(n^2) &= \phi(p_1^{2e_1} \cdots p_k^{2e_k}) \\ &= p_1^{2e_1-1} \cdots p_k^{2e_k-1}(p_1 - 1) \cdots (p_k - 1) \\ &= (p_1^{e_1} \cdots p_k^{e_k}) p_1^{e_1-1} \cdots p_k^{e_k-1}(p_1 - 1) \cdots (p_k - 1) \\ &= n\phi(n).\end{aligned}$$

Assim, $\phi(n^2) = n\phi(n) = n$ implica que $\phi(n) = 1$, o que só pode ocorrer se $n = 2$.

2. O grupo $U(563)$ tem ordem $\phi(563) = 562 = 2 \cdot 281$, que não é divisível por 4. Logo, pelo Teorema de Lagrange, este grupo não tem nenhum subgrupo de ordem 4.

3. Seja q o menor fator primo de $2^p - 1$, e suponhamos que q divide $F(p)$. Neste caso, deveremos ter que $q = 2^{p+1}\ell + 1$, para algum $\ell \geq 1$. Como q é o menor fator de $2^p - 1$, então $q \leq \sqrt{2^p - 1} \leq 2^{p/2}$, donde

$$2^{p+1}\ell + 1 \leq 2^{p/2},$$

que implica

$$\ell \leq \frac{2^{p/2} - 1}{2^{p+1}} < 1,$$

que é uma contradição. Logo q não pode dividir $F(p)$.

4. Temos que $n = 79$. Fatorando $n - 1 = 78 = 2 \cdot 3 \cdot 13$. Escolhendo 2 como base, para começar, temos que

$$2^{(n-1)/13} \equiv 2^6 \equiv 64 \pmod{79} \text{ e } 2^{(n-1)/3} \equiv 2^{26} \equiv 23 \pmod{64},$$

contudo, $2^{(n-1)/2} \equiv 2^{39} \equiv 1 \pmod{79}$. Como

$$2^{n-1} \equiv 2^{78} \equiv (2^{39})^2 \equiv 1 \pmod{79},$$

a base 2 serve para os primos 13 e 3, mas não para 2. Vamos tentar a base 3 para o primo 2, obtemos

$$3^{(n-1)/2} \equiv 3^3 9 \equiv 78 \pmod{79},$$

além disso, evidentemente,

$$3^{(n-1)} \equiv (3^3 9)^2 \equiv 78^2 \equiv 1 \pmod{79},$$

de modo que 3 serve como base para o primo 2. Isto mostra que 79 é primo pelo Teste de Primalidade.

DCC-UFRJ–Números inteiros e criptografia–MAJ–2003/2
Prova Final

1. Seja $n = 1043957$ uma chave pública do RSA. Fatore n pelo algoritmo de Fermat e determine o menor valor possível para o parâmetro de codificação e.

2. Resolva a congruência $4547x + 87 \equiv 23 \pmod{8779}$.

3. Seja p um fator primo de um número ímpar n. Prove que se

$$\text{mdc}(p, (\frac{n-1}{2})!) = 1,$$

   então n é primo.

4. Sabe-se que 6361 é fator primo de um número de Mersenne $2^p - 1$, onde $p > 1$ é primo. Determine p.

5. Seja $n = 49141 = 157 \cdot 313$.

   (a) Determine o resto da divisão de 2^{12285} por n, pelo algoritmo chinês do resto.

   (b) Use isto para verificar se n é um pseudoprimo forte para a base 2.

6. Sabe-se que 269 é primo e que $13^{269} \equiv 1454 \pmod{p}$, onde $p = 8 \cdot 269 + 1$. Determine dois geradores de $U(p)$.

7. Sabe-se que $p > 1$ é um primo e que $3^{2p} + 2^{p-1} + 1 \equiv 0 \pmod{p}$. Determine p.

8. Prove, por indução em n que 9 divide $n^3 + (n+1)^3 + (n+2)^3$ para todo $n \geq 1$.

DCC-UFRJ–Números inteiros e criptografia–2004/1
Gabarito do Teste 1

1. Seja $n > 2^{100!}$ um número inteiro. Use o algoritmo euclidiano estendido para calcular $d = \text{mdc}(3^{2n} + 2, 3^n + 1)$ e dois inteiros α e β tais que $d = \alpha(3^{2n} + 2) + \beta(3^n + 1)$.

2. Use o algoritmo de fatoração de Fermat para determinar dois fatores de 1062097.

Resolução

1. Vamos aplicar o algoritmo euclidiano estendido. Note que, para dividir $3^{2n} + 2$ por $3^n + 1$, usamos o produto notável

$$3^{2n} - 1 = (3^n + 1)(3^n - 1),$$

de modo que

$$3^{2n} + 2 = (3^n + 1)(3^n - 1) + 3.$$

Logo, o resto da divisão de $3^{2n} + 2$ por $3^n + 1$ é 3. A próxima divisão será de $3^n + 1$ por 3, que dá resto 1 e quociente 3^{n-1}. Organizando tudo na tabela do algoritmo estendido, obtemos

Restos	Quocientes	x	y
$3^{2n} + 2$	*	1	0
$3^n + 1$	*	0	1
3	$3^n - 1$	1	$1 - 3^n$
1	3^{n-1}	-3^{n-1}	$1 - 3^{n-1}(1 - 3^n)$

Logo $\text{mdc}(3^{2n} + 2, 3^n + 1) = 1$. Além disso, como

$$1 - 3^{n-1}(1 - 3^n) = 3^{2n-1} - 3^{n-1} + 1,$$

concluímos que

$$\alpha = -3^{n-1} \text{ e que } \beta = 3^{2n-1} - 3^{n-1} + 1.$$

Não custa verificar que não cometemos nenhum erro, calculando $\alpha(3^{2n} + 2) + \beta(3^n + 1)$, que dá

$$(-3^{n-1})(3^{2n} + 2) + (3^{2n-1} - 3^{n-1} + 1)(3^n + 1)$$

multiplicando tudo, obtemos

$$-3^{3n-1} - 2 \cdot 3^{n-1} + 3^{3n-1} - 3^{2n-1} + 3^n + 3^{2n-1} - 3^{n-1} + 1$$

e depois de cancelar os termos comuns sobra

$$-3 \cdot 3^{n-1} + 3^n + 1 = 1,$$

como esperávamos.

x	$\sqrt{x^2 - n}$	Inteiro?
1031	54.10175598	não
1032	54.10175598	não
1033	70.65408693	não
1034	84.01785525	não
1035	95.54056730	não
1036	105.8253278	não
1037	115.2041666	não
1038	123.8830093	não
1039	132.0000000	sim

2. Calculando a raiz quadrada de $n = 1062097$, encontramos 1030.580904, que não é um inteiro. Portanto o número dado não é um quadrado perfeito e precisamos calcular a tabela do algoritmo:

De modo que $x = 1039$ e $y = 132$. Logo os fatores são

$$x + y = 1039 + 132 = 1171 \text{ e}$$
$$x - y = 1039 - 132 = 907.$$

Para saber se estes números são mesmo fatores de n basta multiplicá-los; de fato

$$907 \cdot 1171 = 1062097,$$

portanto o resultado está correto.

DCC-UFRJ–Números inteiros e criptografia–2004/1
Gabarito do Teste 2

1. Considere o seguinte fato:

Se a é um inteiro e p é um fator primo ímpar de a^2+1 então $p \equiv 1 \pmod 4$.

Use este fato para mostrar que existem infinitos primos que deixam resto 1 na divisão por 4.
Sugestão: Se $\{p_1, \ldots, p_s\}$ são primos que deixam resto 1 na divisão por 4, considere $N = (2p_1 \cdots p_s)^2 + 1$.

2. Determine o resto da divisão de $2^{250!} + 5^{450!}$ por 129.

Resolução

1. Suponha, por contradição, que $S = \{p_1, \ldots, p_s\}$ seja o conjunto de todos os primos positivos que deixam resto 1 na divisão por 4, e considere o número

$$N = (2p_1 \cdots p_s)^2 + 1.$$

Como N é ímpar, todos os seus fatores primos têm que ser ímpares. Mas, pelo fato enunciado no exercício, todos os fatores primos ímpares de N têm que deixar resto 1 na divisão por 4.

Seja, agora, q um fator primo de N. Vamos mostrar que $q \notin S$. Entretanto, se q estivesse em S, então $q = p_j$ para algum $1 \leq j \leq s$, e assim

$$N = q \cdot c = p_j \cdot c,$$

para algum inteiro positivo c. Logo,

$$(2p_1 \cdots p_s)^2 + 1 = p_j \cdot c,$$

donde

$$1 = p_j(c - p_j(2p_1 \cdots p_{j-1}p_{j+1} \cdots p_s)^2).$$

Como $p_j > 1$ é um primo, esta equação não pode ser verdadeira. Portanto, q não pode pertencer ao conjunto S. Com isto construímos um primo que não está em S, mas que deixa resto 1 na divisão por 4; o que contradiz nossa hipótese sobre S e prova o resultado desejado.

2. Em $\mathbb{Z}_{129}$ temos que

$$\overline{2}^7 = \overline{128} = \overline{-1}$$

e também que

$$\overline{5}^3 = \overline{125} = \overline{-4} = -\overline{2}^2.$$

Destas duas igualdades, segue que

$$\overline{5}^{21} = (\overline{5}^3)^7 = (-\overline{2}^2)^7 = -(\overline{2}^7)^2 = -(\overline{-1})^2 = -\overline{1}.$$

Como 250! é múltiplo de 14 e 450! é múltiplo de 42, podemos escrever $250! = 14k$ e $450! = 42\ell$, onde k e ℓ são inteiros positivos. Portanto, em $\mathbb{Z}_{129}$,

$$\overline{2}^{250!} + \overline{5}^{450!} = \overline{2}^{14k} + \overline{5}^{42\ell} = (\overline{2}^{14})^k + (\overline{5}^{42})^\ell = ((-\overline{1})^2)^k + ((-\overline{1})^2)^\ell = 2.$$

Logo o resto o resto da divisão de $2^{250!} + 5^{450!}$ por 129 é 2.

DCC-UFRJ–Números inteiros e criptografia–2004/1
Gabarito do Teste 3

1. Prove, por indução em n, que

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} \geq \sqrt{n}.$$

Explicite a base da indução, a hipótese de indução, a recorrência e o passo de indução.

2. Determine todos os números primos ímpares para os quais

$$31^{p^2} + 62^{p^2-1} + (p-1)^p - 12$$

é divisível por p.

Resolução

1. Para simplificar a notação, vamos escrever

$$S_n = \frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}}.$$

Começamos provando a base da indução que, neste caso, corresponde a tomar $n = 1$.

Base: Fazendo $n = 1$, a soma da esquerda dá $S_1 = 1/\sqrt{1} = 1$, a a expressão da direita dá $\sqrt{1} = 1$; de modo que a desigualdade é verificada.

Hipótese de indução: Suponha que, para algum inteiro $n \geq 1$ temos que

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} \geq \sqrt{n};$$

isto é, $S_n \geq \sqrt{n}$.

Para encerrar precisamos mostrar que $S_{n+1} \geq \sqrt{n+1}$, a partir da hipótese de indução e da recorrência, que neste caso é

$$S_{n+1} = S_n + \frac{1}{\sqrt{n+1}}.$$

Passo de indução: Temos que

$$\begin{aligned}
S_{n+1} &= S_n + \frac{1}{\sqrt{n+1}} \quad \text{(Recorrência)} \\
&\geq \sqrt{n} + \frac{1}{\sqrt{n+1}} \quad \text{(Hipótese de indução)} \\
&\geq \frac{(\sqrt{n})(\sqrt{n+1}) + 1}{\sqrt{n+1}} \\
&\geq \frac{n+1}{\sqrt{n+1}} \quad \text{(Já que } \sqrt{n+1} \geq \sqrt{n}\text{)} \\
&\geq \sqrt{n+1},
\end{aligned}$$

como queríamos verificar.

Portanto, pelo Princípio de indução finita, a desigualdade

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} \geq \sqrt{n}$$

é verdadeira para todo $n \geq 1$.

2. Se $31^{p^2} + 62^{p^2-1} + (p-1)^p - 12$ é divisível por p, então

$$31^{p^2} + 62^{p^2-1} + (p-1)^p - 12 \equiv 0 \pmod{p}.$$

Mas, pelo teorema de Fermat, se $p \neq 31$, então $62^{p-1} \equiv 1 \pmod{p}$, já que $62 = 2 \cdot 31$. Logo, usando Fermat, e supondo que $p \neq 5$, obtemos

$$\begin{aligned} 31^{p^2} &\equiv (31^p)^p \equiv 31^p \equiv 31 \pmod{p} \\ 62^{p^2-1} &\equiv (62^{p-1})^{p+1} \equiv 1^{p+1} \equiv 1 \pmod{p} \end{aligned}$$

Por outro lado

$$(p-1)^p \equiv (-1)^p \equiv -1 \pmod{p}.$$

Substituindo tudo isto na congruência original, obtemos

$$0 \equiv 31^{p^2} + 62^{p^2-1} + (p-1)^p - 12 \equiv 31 + 1 - 1 - 12 \equiv 19 \pmod{p}.$$

Mas para que $19 \equiv 0 \pmod{p}$ devemos ter que $p = 19$.

Como o que fizemos depende de $p \neq 31$, precisamos verificar se há alguma solução com $p = 31$. Neste caso,

$$31^{p^2} + 62^{p^2-1} + (p-1)^p - 12 \equiv -13 \not\equiv 0 \pmod{31}.$$

Portanto, a única solução é $p = 19$.

DCC-UFRJ–Números inteiros e criptografia–2004/1
Turma MAI–Teste 4

Seja $n = 2465 = 5 \cdot 17 \cdot 29$.

1. Determine se n é um número de Carmichael.
2. Calcule, pelo algoritmo chinês do resto, o resto da divisão de 11^{77} por n.
3. Determine se n é um pseudoprimo forte para a base 11.
4. Determine se n é um pseudoprimo para a base 11.

Resolução

(1) Vamos usar o teorema de Korselt. Cada primo tem multiplicidade um na fatoração de $n = 5 \cdot 17 \cdot 29$. Além disso,

$$\begin{aligned} n &\equiv 1 \pmod 5 \\ n &\equiv 1 \pmod{17} \\ n &\equiv 1 \pmod{29}. \end{aligned}$$

Logo, n é um número de Carmichael.

(2) Usando o teorema de Fermat, temos que:

$$\begin{aligned} 11^{77} \equiv 11 \equiv 1 &\pmod 5 \\ 11^{77} \equiv 11^1 3 \equiv 2^6 \cdot 11 \equiv 7 &\pmod{17} \\ 11^{77} \equiv 11^{21} \equiv (11^6)^3 \cdot 11^3 \equiv 9^3 \cdot 11^3 \equiv 17 &\pmod{29}. \end{aligned}$$

Isto nos dá o sistema de congruências

$$\begin{aligned} r &\equiv 1 \pmod 5 \\ r &\equiv 7 \pmod{17} \\ r &\equiv 17 \pmod{29}. \end{aligned}$$

Da última equação temos que $r = 17 + 29y$. Substituindo na segunda congruência, obtemos $29y \equiv 7 \pmod{17}$, donde $12y \equiv -10 \pmod{17}$. Como 2 é inversível módulo 17, podemos cancelá-lo, obtendo $6y \equiv -5 \pmod{17}$. Contudo,

$$-5 \equiv 12 \pmod{17},$$

donde $y \equiv 2 \pmod{17}$. Assim,

$$r = 17 + 29(2 + 17t) = 75 + 493t.$$

Substituindo, agora, esta expressão na primeira congruência, e reduzindo módulo 5 resta

$$3t \equiv 1 \pmod 5.$$

Como o inverso de 3 módulo 5 é 2, temos que $t \equiv 2 \pmod 5$, donde

$$r = 75 + 493(2 + 5z) = 1061 + 2465z.$$

Logo o resto desejado é 1061.

(3) Precisamos aplicar o teste forte de composição (teste de Miller) a 2465 na base 11. Mas $n - 1 = 2^5 \cdot 77$. Como $k = 5$ e $q = 77$, devemos calcular os seguintes termos da seqüência

$$\begin{aligned}
11^{77} &\equiv 1061 \not\equiv \pm 1 \pmod n \\
11^{77\cdot 2} &\equiv 1061^2 \equiv 1681 \not\equiv -1 \pmod n \\
11^{77\cdot 2^2} &\equiv 1681^2 \equiv 871 \not\equiv -1 \pmod n \\
11^{77\cdot 2^3} &\equiv 871^2 \equiv 1886 \not\equiv -1 \pmod n \\
11^{77\cdot 2^4} &\equiv 1886^2 \equiv 1 \not\equiv -1 \pmod n.
\end{aligned}$$

Concluímos que o teste tem saída *composto* para base 5. Portanto, 2465 não é um pseudoprimo forte para a base 11.

(4) Como n é um número de Carmichael e 11 é primo com n, então n tem que ser um pseudoprimo para a base 11. Outra maneira de argumentar é notar que, de acordo com a seqüência anterior,

$$11^{2464} \equiv 11^{2^5\cdot 77} \equiv (11^{2^4\cdot 77})^4 \equiv 1 \pmod{2465}.$$

DCC-UFRJ–Números inteiros e criptografia–2004/1
Turma MAI–Teste 5

Os oficiais da estação *Deep Space Nine* foram instruídos a receber uma delegação Maquis para conversas diplomáticas. Entretanto, agentes cardassianos infiltrados na estação pretendem envenenar um dos oficiais e pôr a culpa nos Maquis. O traidor é descoberto, mas foge a tempo. Porém, em seu alojamento é encontrada a mensagem

$$(246, 182) - (71, 94) - (46, 187)$$

que foi codificada no El Gamal com chave pública $p = 251$, $g = 6$ e $h = 187$. Quebre o código usando o algoritmo Baby Step/Giant Step e descubra qual o oficial que corre o risco de ser envenenado.

Resolução

Tabela para os Baby Steps

r										
g^r										

r										
g^r										

Tabela para os Giant Steps

q	

DCC-UFRJ–Números inteiros e criptografia–2004/1
Turma MAI–Gabarito do Teste 6

1. Ache todos os valores de n para os quais $\phi(n) = 44$.

2. Os clientes do Banco Enterprise SA enviam mensagens para ao banco codificando-as com o RSA com chave pública (n, e). Entretanto, todas as mensagens enviadas ao banco são interceptadas por Silik, um funcionário mal intencionado. Sejam m_1 e m_2 duas mensagens codificadas interceptadas por Silik. Mostre que se Silik conseguir decodificar corretamente estas duas mensagens então ele saberá decodificar corretamente a mensagem $m_3 \equiv m_1 m_2 \pmod{n}$.

3. Sabe-se que $p = 1000000000000223$ e $q = 2p + 1$ são primos e que $3^p \equiv 1 \pmod{q}$.
   (a) Qual a ordem de $-\overline{3}$ em $U(q)$?
   (b) Ache um elemento de ordem p e um elemento de ordem 2 em $U(q)$.

Resolução

1. Sabemos que se p é um fator primo de n então $p-1$ deve ser fator de $\phi(n)$. Tabelando as possibilidades quando $\phi(n) = 44$, e excluindo os valores de p que não são pirmos, obtemos Portanto, $n = 2^e 3^f 5^g 23^h$.

p	$p-1$
2	1
3	2
5	4
23	22

Primeiro caso: $h > 0$.
Neste caso,

$$\phi(n) = \phi(2^e 3^f 5^g)\phi(23^h) = \phi(2^e 3^f 5^g)23^{h-1}22 = 44,$$

que implica que $h = 1$ e que $\phi(2^e 3^f 5^g) = 2$. Mas já sabemos que $\phi(m) = 2$ só ocorre se $m = 3$, 4 ou 6. Isto nos dá as soluções $n = 3 \cdot 23$, $n = 4 \cdot 23$ ou $n = 6 \cdot 23$ para $\phi(n) = 44$.
Segundo caso: $h = 0$.
Neste caso,

$$\phi(n) = \phi(2^e 3^f 5^g).$$

Contudo, os fatores primos de $\phi(2^e 3^f 5^g)$ serão todos menores que 5, de forma que 11 não pode dividir $\phi(2^e 3^f 5^g)$ neste caso. Contudo, 11 divide 44. Portanto, não há soluções neste caso e as únicas soluções de $\phi(n) = 44$ são as que já foram descobertas acima.

2. O sistema RSA utilizado tem chave pública (n, e). Suponhamos que a chave secreta seja d–que é desconhecida de Silik. Mas, se Silik conseguiu decodificar m_1 e m_2 de alguma maneira, então ele conhece $r_1 \equiv m_1^d \pmod{n}$ e $r_2 \equiv m_2^d \pmod{n}$. Portanto, Silik conhece

$$r_1 r_2 \equiv m_1^d m_2^d \equiv (m_1 m_2)^d \equiv m_3^d \pmod{n},$$

que é decodificação de m_3.

3. (a) Como p é um número ímpar,

$$(-3)^p \equiv -3^p \equiv -1 \pmod{q}.$$

Logo $-\overline{3}$ não tem ordem p em $U(q)$. Mas

$$(-3)^2 \equiv 9 \pmod{q},$$

de modo que a ordem de $-\overline{3}$ também não pode ser 2. Entretanto, como q e p são primos, as possíveis ordens de elementos, diferentes de $\overline{1}$ de $U(q)$ são 2, p ou $2q$. Contudo, já vimos que $-\overline{3}$ não tem ordem 2, nem q; de modo que deve ter ordem $2q$. Logo, $-\overline{3}$ tem que ter ordem $2q$.
(b) Pelo Lema Chave, como $3^p \equiv 1 \pmod{q}$, então a ordem de $\overline{3}$ em $U(q)$ tem que dividir p. Como p é primo, então a ordem de $\overline{3}$ será 1 ou p. Mas $\overline{3} \neq \overline{1}$, de modo que a ordem de $\overline{3}$ não pode ser 1. Portanto, $\overline{3}$ tem ordem p em $U(q)$.

Como $((-3)^p) \equiv 1 \pmod{q}$ então a ordem de $(\overline{-3})^p$ divide 2. Um argumento semelhante ao descrito acima mostra que $(\overline{-3})^p$ tem ordem 2.

DCC-UFRJ–Números inteiros e criptografia–MAI–2004/1
Gabarito da Prova Final

Justifique cuidadosamente as suas respostas.

1. Considere o RSA de chave pública $n = 1536569$ e $e = 101$.
   (a) Use o algoritmo de Fermat para fatorar n e descobrir p e q.
   (b) Use o algoritmo euclidiano estendido para calcular o parâmetro d de decodificação desta implementação do RSA.

2. Seja p um fator primo de $1200! + 1$.
   (a) Mostre que $p > 1200$.
   (b) 1200 é invertível módulo p? Se for qual o seu inverso módulo p?

3. Use o teorema de Fermat e o algoritmo chinês do resto para determinar o resto da divisão de $2^{450!} + 3^{890!} + 15^{900!}$ por 30.

4. Prove, por indução em n, que $n! \geq 4^n$ para todo $n \geq 9$. Explicite a base da indução, a hipótese de indução e o passo de indução.

5. Sabe-se que $p > 10^{901}$ é primo e que $n = 4p + 1$ satisfaz $2^p \equiv 3 \pmod{n}$.
   (a) Determine se n é um pseudoprimo forte para a base 2.
   (b) Mostre que a equação $\phi(x) = 4p$ só pode ter solução se $2p+1$ for primo. Quais são as possíveis soluções quando isto acontece?

6. Determine os subgrupos de ordem 4 de $U(36)$, identificando quais são so subgrupos cíclicos e quais não são cíclicos.

Solução

1. (a) Como a parte inteira da raiz de n é 1239 e $1239^2 \neq n$, então devemos executar a tabela:

x	$\sqrt{x^2 - n}$
1240	$32,109$
1241	$59,26$
1242	$77,42$
1243	$92,08$
1244	$104,72$
1245	116

Portanto, os fatores de n são $x + y = 1361$ e $x - y = 1129$.
(b) Aplicando o algoritmo euclidiano estendido a

$$\phi(n) = (p-1)(q-1) = 1534080,$$

e $e = 101$, temos

restos	quocientes	x
1534080	*	1
101	*	0
92	15188	1
9	1	-1
2	10	11
1	4	-45

Portanto, $(-45)\phi(n) + ye = 1$, logo

$$y = \frac{1 + 45 \cdot 1534080}{101} = 683501.$$

Passando ao módulo $\phi(n)$, obtemos

$$ye \equiv 1 \pmod{\phi(n)},$$

de modo que o inverso de e módulo $\phi(n)$ é $y = 683501$.

2. (a) Se p fosse menor ou igual que 1200 então dividiria 1200!. Mas p também divide $1200! + 1$ por hipótese. Logo, p dividiria

$$(1200! + 1) - 1200! = 1,$$

o que não é possível. Assim, p não pode ser menor ou igual a 1200. Portanto, $p > 1200$.
(b). Como p é fator de $1200! + 1$, então $1200! + 1 \equiv 0 \pmod{p}$, de modo que $1200! \equiv -1 \pmod{p}$. Assim,

$$1200(-(1199!)) \equiv 1 \pmod{p}.$$

Logo, 1200 é invertível módulo p e seu inverso é $-(1199!)$.

3. Seja $m = 2^{450!} + 3^{890!} + 15^{900!}$. Temos, pelo teorema de Fermat, que

$$\begin{aligned} m &\equiv 3^{890!} + 15^{900!} \equiv 2 \equiv 0 \pmod 2 \\ m &\equiv 2^{450!} \equiv 1 \pmod 3 \\ m &\equiv 2^{450!} + 3^{890!} \equiv 2 \pmod 5 \end{aligned}$$

que nos dá o sistema

$$\begin{aligned} m &\equiv 0 \pmod 2 \\ m &\equiv 1 \pmod 3 \\ m &\equiv 2 \pmod 5. \end{aligned}$$

Resolvendo pelo algoritmo chinês do resto, tiramos o valor de m da última equação, obtendo $m = 2 + 5y$. Substituindo na segunda equação, obtemos $2 + 5y \equiv 1 \pmod 3$, que dá $2y \equiv 2 \pmod 3$, donde $y \equiv 1 \pmod 3$. Assim, $y = 1 + 3t$ e

$$x = 2 + 5(1 + 3t) = 7 + 15t.$$

Substituindo na primeira equação, $7 + 15t \equiv 0 \pmod 2$ dá $t \equiv 1 \pmod 2$; isto é, $t = 1 + 2s$. Finalmente,

$$x = 7 + 15(1 + 2s) = 22 + 30t.$$

4. A base da inução corresponde a $n = 9$. Neste caso,

$$9! = 362880 \geq 4^9 = 262144,$$

de forma que a base da inudção é verdadeira.

Suponha, agora, que $k! \geq 4^k$ para algum $k \geq 9$. Esta é a hipótese de indução. Para executar o passo de indução precisamos passar de k a $k + 1$, mas

$$\begin{aligned} (k+1)! &= (k+1)k! \text{definição de fatorial} \\ &\geq (k+1)4^k \text{hipótese de indução} \\ &\geq 4 \cdot 4^k \text{já que } k \geq 9 \\ &\geq 4^{k+1}, \end{aligned}$$

como queríamos mostrar. Portanto, segue do Princípio de indução finita que $n! \geq 4^n$ para todo $n \geq 9$.

5. (a) Como $n - 1 = 2p$ e p é um primo ímpar, então, para aplicar o teste de composição forte (Miller) precisamos calcular

$$2^p \equiv 3 \pmod n \text{ e } 2^{2p} \equiv 9 \pmod n.$$

Como $3 \not\equiv \pm 1 \pmod n$ e $9 \not\equiv -1 \pmod n$, pois $n > 10$, então o teste tem saída composto. Portanto, n não é um pseudoprimo forte para a base 2.
(b) Sabemos que se q é fator primo de x então $q - 1$ é fator de $\phi(x)$. Tabelando os possíveis valores de $q - 1$, e levando em conta que q precisa ser primo, temos

$q-1$	q
1	2
2	3
$2p$	$2p+1$ (se for primo)

Note que $q = 4p+1$ não figura na tabela porque, pela item anterior $4p+1$ é composto. Da mesma maneira, $2p+1$ só vai poder estar na tabela se for primo. Mas se $2p+1$ não for primo, então $x = 2^e 3^f$ e $\phi(x) = \phi(2^e 3^f)$ só tem 2 e 3 como fatores primos, de modo que não pode ser igual a $4p$, já que $p > 10$ é primo.

Por outro lado, supondo que $2p+1$ é primo, temos que

$$x = 2^e 3^f (2p+1)^g.$$

Se $g > 0$, então,

$$\phi(x) = \phi(2^e 3^f)\phi((2p+1)^g) = \phi(2^e 3^f)2p(2p+1)^{g-1} = 4p,$$

donde $g = 1$ e $\phi(2^e 3^f) = 2$. Logo, $2^e 3^f = 3, 4$ ou 6 e as possíveis soluções são $3(2p+1)$, $4(2p+1)$ e $6(2p+1)$.

6. Como $U(36)$ não tem elementos de ordem 4, então não admite subgrupos cíclicos de ordem 4. Mas $U(36)$ tem 3 elementos de ordem 2, portanto, tem um subgrupo não cíclico de ordem 4 dado por $\{\overline{1}, \overline{17}, \overline{19}, \overline{35}\}$.

DCC-UFRJ–Números inteiros e criptografia–2007/1–Prova 1

Justifique cuidadosamente as suas respostas.

1. Prove, por indução em n, que $n^5 - n$ é divisível por 5 para todo inteiro $n \geq 1$.

2. Alberto costumava receber R$ 1239,00 de salário, mas teve um aumento, e seu salário passou para R$ 1455,00. Para uma prestação de contas ele precisa saber o número m de meses durante os quais recebeu o salário menor e o número n de meses durante os quais recebeu o maior. A única coisa que Alberto sabe é que recebeu um total de R$ 21786,00 no período da prestação de contas.

   (a) Formule o problema como uma equação diofantina em m e n e ache sua solução geral.

   (b) Usando a solução geral, determine m e n.

3. Use o algoritmo de fatoração de Fermat para determinar dois fatores de 1793093.

Resolução

Questão 1: Considere o conjunto:

$$V = \{n \in \mathbb{N} : n^5 - n \text{ é divisível por } 5\}.$$

Usaremos o Princípio de Indução Finita para mostrar que $V = \mathbb{N}$. Para isto devemos provar que:

1. $1 \in V$;
2. se $n \in V$, então $n + 1 \in V$.

Para começar mostramos a base da indução; mas se $n = 1$, então

$$n^5 - n = 1 - 1 = 0,$$

logo 1 de fato pertence a V.

Suponha, agora, que $n \in V$. Isto significa que $n^5 - n$ é múltiplo de 5. Queremos usar isto para mostrar que $(n+1)^5 - (n+1)$ também é múltiplo de 5. Contudo,

$$(n+1)^5 - (n+1) = n^5 + 5\,n^4 + 10\,n^3 + 10\,n^2 + 4\,n$$

que podemos reescrever na forma

$$(n+1)^5 - (n+1) = (n^5 - n) + 5(\,n^4 + 2\,n^3 + 2\,n^2 + \,n).$$

Como $n^5 - n$ é divisível por 5, é claro que o resultado desta expressão é divisível por 5; afinal, soma de múltiplos de 5 é múltiplo de 5. Portanto, $(n+1)^5 - (n+1)$ é múltiplo de 5. Portanto, pelo Princípio de Indução Finita, $V = \mathbb{N}$, como queríamos mostrar.

Resto	Quociente	x
1455	**	1
1239	**	0
216	1	1
159	5	- 5
57	1	6
45	2	- 17
12	1	23
9	3	- 86
3	1	109
0	3	- 413

QUESTÃO 2: Os salarios são $a = 1455$ e $b = 1239$ e o valor total é $D = 21786$. A equação diofantina a ser resolvida é

$$1239\ n + 1455\ m = 21786$$

Aplicando o algoritmo euclidiano estendido a a e b:

Calculando y:

$$y = (3 - ax)/b = -128$$

Logo, a solução geral da equação diofantina é

$$x = -\frac{1239}{3}\ k + 791558 = -413k + 791558$$
$$y = \frac{1455}{3}\ k - 929536 = 485k - 929536$$

Uma verificação mostra que nenhum valor de k produz valores positivos para x e y, de modo que o problema ficou sem solução.

QUESTÃO 3: O valor de n é $n = 1793093$. Aplicando o algoritmo de Fermat calculamos primeiro a parte inteira de $\sqrt{n}$, que é 1339. Como

$$1339^2 = 1792921 \neq n,$$

devemos calcular a tabela do algoritmo, que é dada na próxima página.

x	$[\sqrt{x^2 - n}]$	$x^2 - y^2 - n = 0$?
1340	50	n
1341	72	n
1342	88	n
1343	102	n
1344	115	n
1345	126	n
1346	136	n
1347	146	s

Com isto obtemos: que os fatores são

$$x + y = 1493 \text{ e } \quad y = 1201.$$

Testando:

$$1493 \cdot 1201 = 1793093 = n.$$

2007/1–Prova 2

1. Considere a seguinte recorrência

$$N_1 = 2 \quad \text{e} \quad N_{k+1} = N_k \cdot (N_k + 1).$$

(a) Prove, por indução em k, que N_k tem, pelo menos, k fatores primos *distintos*.

(b) Use (a) para provar que existem infinitos números primos.

Sugestão para (a): $\text{mdc}(N_k, N_k + 1) = 1$ qualquer que seja o inteiro $n > 1$.

Sejam a e n inteiros positivos. A *ordem* de a módulo n é igual ao menor inteiro positivo $k > 0$ tal que a^k deixa resto 1 na divisão por n. Entretanto, um tal k pode não existir. Isto é, há inteiros positivos a e n para os quais a ordem de a módulo n não está definida.

2. Calcule a ordem de 3 módulo 91 e use isto para calcular 3^{500} módulo 91.

3. Explique porque a ordem de 13 módulo 91 não está definida. Em outras palavras, explique porque não existe nenhum inteiro positivo k tal que $a^k \equiv 1 \pmod{91}$.

Resolução

1(a). Considere o conjunto

$$V = \{k \in \mathbb{N} : N_k \quad \text{tem, pelo menos } k \text{ fatores primos distintos} \quad \}.$$

Vamos provar por indução finita que $V = \mathbb{N}$.

A base da indução consiste em provar que $1 \in V$. Mas isto é fácil de ver, porque, por definição, $N_1 = 2$ que é primo. Logo N_1 tem apenas um fator, de modo que $1 \in V$.

Suponha, agora, que $k \in V$. Mostraremos que $k + 1 \in V$. Contudo, se $k \in V$, então N_k tem, pelo menos k fatores primos distintos. Por outro lado,

$$\text{mdc}(N_k, N_k + 1) = 1,$$

de modo que N_k e $N_k + 1$ não têm fatores primos distintos. Como $N_k + 1$ tem que ter, pelo menos um fator primo (pelo teorema da fatoração única), então o produto

$$N_k(N_k + 1) = N_{k+1}$$

tem, pelo menos, $k + 1$ fatores primos distintos, a saber:

- os k fatores primos distintos de N_k e
- um fator primo de $N_k + 1$, que não pode dividir N_k.

Isto mostra que $k+1 \in V$ e conclui a indução. Pelo Princípio de indução finita isto basta para garantir que $V = \mathbb{N}$.

1(b). Suponha, por contradição, que exista uma quantidade finita m de primos. Contudo, acabamos de mostrar que N_{m+1} tem $m+1$ fatores primos distintos. Temos, assim, uma contradição. Portanto, o número de primos não pode ser finito.

Esta demonstração da infinidade dos primos foi criada por Filip Saidak e publicada em 2006 no American Mathematical Monthly (vol. 113). O artigo original pode ser encontado em `http://www.uncg.edu/~f_saidak/`.

2. Calculando as potências de 3 módulo 91 obtemos

$$\begin{aligned} 3^1 &\equiv 3 \pmod{91} \\ 3^2 &\equiv 9 \pmod{91} \\ 3^3 &\equiv 27 \pmod{91} \\ 3^4 &\equiv 81 \pmod{91} \\ 3^5 &\equiv 61 \pmod{91} \\ 3^6 &\equiv 1 \pmod{91}. \end{aligned}$$

Como $3^6 \equiv 1 \pmod{91}$ mas $3^r \not\equiv 1 \pmod{91}$ se $1 \leq r \leq 5$, concluímos que 3 tem ordem 6 módulo 91. Usando isto, podemos dividir 500 por 6 obtendo resto 2 e quociente 83, o que nos dá:

$$3^{500} \equiv (3^6)^{83} \cdot 3^2 \equiv 1^{83} \cdot 9 \equiv 9 \pmod{91}.$$

3. Calculando as potências de 13 módulo 91, vemos que

$$\begin{aligned} 13^1 &\equiv 13 \pmod{91} \\ 13^2 &\equiv -13 \pmod{91} \end{aligned}$$

são as únicas potências distintas. Portanto,

$$13^r \equiv \begin{cases} 13 & \text{se } r \text{ for par} \\ -13 & \text{se } r \text{ for ímpar} \end{cases} \pmod{91}$$

Desta forma não há como obter $13^k \equiv 1 \pmod{91}$ para nenhum inteiro positivo k.

Outra maneira de fazer, inspirada na solução de alguns alunos, é a seguinte. Suponha que exista um inteiro positivo k tal que $13^k \equiv 1 \pmod{91}$. Isto significa que, para algum inteiro q, temos

$$13^k - 1 = 91q.$$

Em outras palavras,

$$1 = 13^k - 91q = 13(13^{k-1} - 7q).$$

Contudo, isto implica que 13 divide 1, o que é obviamente falso. Logo, $13^k \equiv 1 \pmod{91}$ não pode ser verdadeiro para nenhum inteiro positivo k.

Prova 3

1. Seja n um inteiro positivo ímpar e composto que é pseudoprimo *forte* para as bases 2 e 3. Então, podemos escrever

$$n - 1 = 2^k q, \text{ onde } k > 0 \text{ e } q \text{ é ímpar.}$$

Mostre que, se $\overline{2}$ tem ordem $2^m q$ e $\overline{3}$ tem ordem $2^{m+1} q$ em $\mathbb{Z}_n$, para algum $0 \leq m \leq k-1$, então n também é pseudoprimo forte para a base 6.

2. Sabe-se que p é um número primo para o qual $2^p - 1$ é composto. Determine se $2^p - 1$ é, ou não, um pseudoprimo (fraco) para a base 2.

3. Pouco antes de ser completamente destruído, um cubo Borg enviou uma transmissão de emergência, criptografada por um código primitivo com o número da espécie que os atacou (os Borgs, *como todos sabem*, identificam as várias espécies que encontram por números). A transmissão foi interceptada pela Voyager e uma pesquisa nos bancos de dados da frota revelou que se tratava de uma codificação feita usando o RSA com chave pública $n = 1692209$ e $e = 482743$ e que a mensagem era

786345

Decodifique a mensagem e descubra o número da espécie que atacou os Borgs. Para isto faça a "decodificação" módulo cada um dos fatores primos de n e "cole" o resultado usando o teorema chinês do resto.

Resolução

1. Como n é um pseudoprimo forte para a base 3, devemos ter que

$$3^q \equiv 1 \pmod{n}.$$

ou então que

$$3^{2^t q} \equiv -1 \pmod{n},$$

para algum $0 \leq t < k$. Contudo, se a primeira possiblidade ocorresse, 3 teria ordem menor ou igual do que q módulo n. Contudo, a ordem foi dada como sendo $2^{m+1} q$, que é sempre maior que q pois $m \geq 0$. Por outro lado, segue da segunda possibilidade que

$$3^{2^{t+1} q} \equiv (3^{2^t q})^2 \equiv 1 \pmod{n};$$

de modo que a ordem de 3 módulo n deve ser exatamente $2^t q$. Logo, levando em conta a hipótese, $t = m$. Finalmente, levando em conta as conclusões acima e o fato de 2 tem ordem $2^m q$ módulo n, obtemos

$$6^{2^m q} \equiv (2^{2^m q})(3^{2^m q}) \equiv 1 \cdot (-1) \equiv -1 \pmod{n};$$

donde segue que n é pseudoprimo forte para a base 6.

2. Basta verificar o que ocorre se calcularmos

$$2^{(2^p-1)-1} = (2^{2^{p-1}-1})^2$$

módulo $2^p - 1$. Contudo, pelo teorema de Fermat $2^{p-1} - 1 \equiv 0 \pmod{p}$. A propósito, note que o fato de $2^p - 1$ ser composto significa que $p \neq 2$, tornando possível a aplicação de Fermat acima. Em outras palavras, $2^{p-1} - 1 = rp$ para algum inteiro positivo r. Assim,

$$2^{(2^p-1)} - 1 \equiv (2^{2^{p-1}-1})^2 \equiv (2^p)^{2r} \pmod{2^p - 1}.$$

Como,

$$2^p \equiv 1 \pmod{2^p - 1},$$

concluímos que

$$2^{(2^p-1)} - 1 \equiv (2^p)^{2r} \equiv (1)^{2r} \equiv 1 \pmod{2^p - 1}.$$

Portanto, todas as vezes que $2^p - 1$ for composto, será um pseudoprimo para a base 2.

3. Fatorando n pelo algoritmo de Fermat, obtemos (após 5 laços) os fatores 1201 e 1409. Logo,

$$\phi(n) = 1200 \cdot 1408 = 1689600.$$

Calculando o inverso de $e = 482743$ módulo 1689600 descobrimos que $d = 7$ (em 2 laços). Para decodificar basta calcular 786345^7 módulo n. Faremos isto módulo cada um dos primos e colaremos o resultado usando o algoritmo chinês do resto. Mas,

$$786345^7 \equiv 891^7 \equiv (891^2)^3 \cdot 891 \equiv 20^3 \cdot 891 \equiv 65 \pmod{1201};$$

ao passo que

$$786345^7 \equiv 123^7 \equiv (123^2)^3 \cdot 891 \equiv 1039^3 \cdot 891 \equiv 227 \cdot 1039 \cdot 123 \equiv 18 \pmod{1409}.$$

Portanto, devemos resolver o sistema

$$\begin{aligned} x &\equiv 65 \pmod{1201} \\ x &\equiv 18 \pmod{1409}. \end{aligned}$$

Da segunda equação, $x = 18 + 1409y$. Substituindo na primeira equação:

$$18 + 1409y \equiv 65 \pmod{1201}.$$

Logo, $y = 6$; donde $x = 8472$. Para que um cubo Borg pudesse ser derrotado a espécie que os atacou foi, evidentemente, a 8472.

Prova Final

1. Mostre *por indução* em n que

$$(1+t)(1+t^2)(1+t^4)\dots(1+t^{2^{n-1}}) = \frac{t^{2^n}-1}{t-1}.$$

Explicite cada etapa da indução claramente.

2. Pierre costumava receber R$ 3093,00 de salário, mas teve um aumento, e seu salário passou para R$ 4227,00. Para uma prestação de contas ele precisa saber o número m de meses durante os quais recebeu o salário menor e o número n de meses durante os quais recebeu o maior. A única coisa que Pierre sabe é que recebeu um total de R$ 33507,00 no período da prestação de contas. Formule o problema como uma equação diofantina em m e n, ache sua solução geral e use-a para determinar m e n.

3. Calcule o resto da divisão de 2^{500} por 527 usando o algoritmo chinês do resto e o teorema de Fermat.

4. Sabe-se que p é um número primo para o qual $2^p - 1$ é composto. Determine se $2^p - 1$ é, ou não, um pseudoprimo (fraco) para a base 2.

5. A mensagem $1844-7768-994$ foi codificada usando o RSA com chave pública $n = 7979$ e $e = 3343$. Fatore n usando o algoritmo de Fermat e decodifique a mensagem.

6. Determine os subgrupos de ordem 4 de $U(21)$. Indique quais são cíclicos e quais não são.

Primeira Prova

1. Prove por indução finita que $2^{3n} - 1$ é divisível por 7, para todo $n \geq 1$. Indique claramente cada etapa da indução.

2. Ache *todas* as soluções inteiras da equação $23303x + 2359y = 21$.

3. Determine k de modo que $65k - 3147$ seja o menor fator positivo (e maior que 1) de $1079k + 45$.

Resolução

1. Seja

$$V = \{n \in \mathbb{N} : 2^{3n} - 1 \text{ é divisível por } 7 \}.$$

Se mostrarmos que:

1. $1 \in V$; e
2. sempre que $k \in V$, temos também que $k + 1 \in V$;

podemos usar o princípio de indução finita para concluir que $V = \mathbb{N}$ que equivale ao enunciado desejado.

A base da indução corresponde a $n = 1$, mas

$$2^3 - 1 = 8 - 1 = 7, \text{ que é divisível por } 7.$$

Portanto, $1 \in V$

Para fazer o passo de indução, suponha que $k \in V$; isto é, que $2^{3k} - 1$ é divisível por 7. Contudo,

$$2^{3(k+1)} - 1 = 2^{3k} \cdot 8 - 1 = (2^{3k} - 1) \cdot 8 + 7$$

é divisível por 7, já que $2^{3k} - 1$ é múltiplo de 7, pela hipótese de indução. Portanto, pelo princípio de indução finita, $V = \mathbb{N}$. Mas isto equivale a dizer que $2^{3n} - 1$ é divisível por 7, para todo $n \geq 1$.

2. Aplicando o algoritmo euclidiano estendido, temos

Restos	Quocientes	x
23303	**	1
2359	**	0
2072	9	1
287	1	- 1
63	7	8
35	4	- 33
28	1	41
7	1	- 74
0	**	**

Disto segue que $\alpha = -74$, onde

$$7 = 23303\alpha + 2359\beta.$$

Calculando o valor de β, obtemos $\beta = 731$. Logo, a equação reduzida é

$$3329 \cdot x + 337 \cdot y = 3,$$

que dá como solução geral

$$\begin{aligned} x &= 3\alpha(-74) + 337k = 337k - 222 \\ y &= 3\beta - 3329k = -3329k + 2193. \end{aligned}$$

2. Como $p = 65k - 3147$ é o menor fator de $n = 1079k + 45$, devemos ter que

$$0 \leq n - p^2 = -4225k + 410189k - 9903564.$$

Resolvendo a equação, descobrimos que suas raízes são aproximadamente iguais a $1667/32$ e $1441/32$. Calculando p para os valores inteiros de k entre as duas raízes acima, obtemos

$$-222, -157, -92, -27, 38, 103, 168, 233$$

Como $p > 0$ é o menor fator, então tem que ser primo. Com isso, só temos duas possibilidades, $p = 103$ ou $p = 233$, que correspondem a $k = 50$ e $k = 52$, respectivamente. Contudo, 103 não divide $1079 \cdot 50 + 45$; já 233 divide

$$1079 \cdot 52 + 4556153$$

tendo 241 como co-fator. Logo, $k = 52$.

Segunda Prova

1. Fatore 31877 pelo algoritmo de Fermat.

2. Considere a seqüência infinita de números inteiros positivos definida por

$$a_0 = 2 \quad \text{e} \quad a_{n+1} = a_n^2 - a_n + 1.$$

   (a) Prove, por indução em n, que a seguinte afirmação é verdadeira para todo $n \geq 1$:

   todo primo p que divide a_k, para algum $0 \leq k < n$ também divide $a_n - 1$.

   (b) Use (a) para mostrar que se p_k é um primo que divide a_k então p_k *não* divide a_n *para nenhum* $n > k$ e explique porque isto implica que há infinitos números primos.

3. Calcule:

   (a) a ordem de 5 módulo 14 e a ordem de 7 módulo 113.

   (b) o resto da divisão de $7^{25^{100}}$ por 113.

Resolução

1. Aplicando o algoritmo de Fermat, temos que

$$[\sqrt{n}] = 178,541...$$

de modo que precisamos recorrer à tabela, que nos dá

x	$\sqrt{x^2 - n}$
179.0	12.8062484748 65697373
180.0	22.8691932520 58543047
181.0	29.7321374946 37011045
182.0	35.3128871660 19150069
183.0	40.1497197997 69462401
184.0	44.4859528390 70447407
185.0	48.4561657583 42869529
186.0	52.1440312979 34761807
187.0	55.6057550978 31375461
188.0	58.8812364000 62116902
189.0	62.0

Portanto, os fatores são

$$x - y = 189 - 62 = 127 \quad \text{e} \quad x + y = 189 + 62 = 251.$$

1(a). Seja

$V = \{n \in \mathbb{N} :$ todo primo p que divide a_k, para algum $0 \leq k < n$ também divide $a_n - 1\}$.

Se mostrarmos que:

1. $1 \in V$; e

2. sempre que $k \in V$, temos também que $k+1 \in V$;

podemos usar o princípio de indução finita para concluir que $V = \mathbb{N}$ que equivale ao enunciado desejado.

Se $n = 1$ e $0 \leq k < n$ então $k = 0$, de modo que a base consiste em mostrar que se um primo p divide a_0 então também divide $a_1 - 1$. Como $a_0 = 2$, isto significa que p só pode ser igual a 2. Por outro lado,

$$a_1 - 1 = a_0^2 - a_0 = 2^2 - 2 = 2$$

que é claramente divisível por 2. Logo $1 \in V$.

Suponha, agora, que $n \in V$, para algum $n \geq 1$; isto é, que vale a afirmação

todo primo p que divide a_k, para algum $0 \leq k < n$ também divide $a_n - 1$.

Queremos usar isto para provar que $n+1 \in V$; isto é, que

todo primo p que divide a_ℓ, para algum $0 \leq \ell < n+1$ também divide $a_{n+1} - 1$.

Seja, então, p um primo que divide a_ℓ para algum $0 \leq \ell < n+1$. Se $\ell < n$ então, pela hipótese de indução p divide $a_n - 1$. Se $\ell = n$ então p divide a_n. De qualquer forma, p divide $a_n(a_n - 1)$ e portanto divide

$$a_{n+1} - 1 = a_n(a_n - 1),$$

provando, assim, que $n+1 \in V$, o que completa o passo de indução. Portanto, pelo Princípio de Indução Finita, a afirmação

todo primo p que divide a_k, para algum $0 \leq k < n$ também divide $a_n - 1$.

é verdadeira para todo $n \geq 1$, como precisávamos mostrar.

1(b). Por (a), se p_k divide a_k, então divide $a_n - 1$ qualquer que seja $n > k$. Como $\text{mdc}(a_n, a_n - 1) = 1$, temos que p_k não divide a_n. Portanto, para cada elemento da seqüência $\{a_n : n \geq 0\}$ temos um primo que não divide nenhum dos demais elementos. Como a seqüência é infinita, produzimos infinitos primos desta maneira.

3(a). Fazendo as contas das potências verificamos que a ordem de 5 módulo 14 é 6 e a ordem de 7 módulo 113 é 14. Na prova devem constar os cálculos com todas as potências de 5 módulo 14 até a sexta potência e de 7 módulo 113 até a décima quarta potência mostrando que nenhuma potência anterior é nula.

3(b). Como 7 tem ordem 14 módulo 113, devemos calcular o resto da divisão de 25^{100} por 14. Mas, 5 tem ordem 6 módulo 14. Como

$$25^{100} = 5^{200}$$

e $200 = 6 \cdot 33 + 2$, obtemos

$$25^{100} \equiv 5^{200} \equiv (5^6)^{33} \cdot 5^2 \equiv 25 \equiv 11 \pmod{14}.$$

Assim,

$$7^{25^{100}} \equiv 7^{11} \equiv 85 \pmod{113}.$$

Prova 3

1. Seja $p \geq 2$ um número primo. Usando congruências e o teorema de Fermat, prove que a soma

$$1^{(p-1)n+1} + 2^{(p-1)n+1} + 3^{(p-1)n+1} + \cdots + (p-1)^{(p-1)n+1}$$

é divisível por p, para todo inteiro $n \geq 1$.

2. Determine se 21 é

(a) número de Carmichael;

(b) pseudoprimo forte para a base 13;

(c) pseudoprimo para a base 13.

3. Use o *algoritmo chinês do resto* para determinar a quantidade de inteiros positivos menores que 10^5 que têm a seguinte propriedade:

- a divisão por 2 deixa resto 1;
- a divisão por 3 deixa resto 2;
- a divisão por 4 deixa resto 3;
- a divisão por 5 deixa resto 4;
- a divisão por 6 deixa resto 5.

Resolução

1. Aplicando o teorema de Fermat a um número da forma $k^{(p-1)n+1}$, com $1 \leq k \leq p-1$, temos que

$$k^{(p-1)n+1} \equiv (k^{(p-1)})^n \cdot k \equiv k \pmod{p}.$$

Portanto,

$$1^{(p-1)n+1} + 2^{(p-1)n+1} + 3^{(p-1)n+1} + \cdots + (p-1)^{(p-1)n+1} \equiv 1 + 2 + \cdots + (p-1) \pmod{p}.$$

Contudo, esta soma é igual a

$$\frac{p(p-1)}{2}$$

que é divisível por p.

2. Como $21 = 3 \cdot 7$ só tem dois fatores primos, não pode ser número de Carmichael. Para saber se 21 é pseudoprimo forte, fatoramos $20 = 2^2 \cdot 5$. Em seguida aplicamos o teste

forte de composição para a base 13. Para isso, vamos calcular 13^5 módulo 3 e módulo 7. Mas,

$$13^5 \equiv 1 \pmod 3 \tag{1}$$
$$13^5 \equiv (-1)^5 \equiv 6 \pmod 7. \tag{2}$$

Mas isto implica que

$$13^5 \not\equiv 1, -1 \pmod{21},$$

de modo que precisamos calcular o próximo número da seqüência, que é o resto de $13^{2\cdot 5}$ por 21. Para isto, elevamos ao quadrado cada uma das congruências acima, obtendo

$$(13^5)^2 \equiv 1^2 \equiv 1 \pmod 3 \tag{3}$$
$$(13^5)^2 \equiv (-1)^2 \equiv 1 \pmod 7. \tag{4}$$

Logo,

$$13^5 \not\equiv -1 \pmod{21},$$

e 21 não pode ser pseudoprimo forte para a base 13. Finalmente, o último par de congruências módulos 3 e 7 nos diz que

$$13^5 \equiv 1 \pmod{21},$$

de modo que 21 é um pseudoprimo para a base 13.

3. Montando as congruências:

- a divisão por 2 deixa resto 1 equivale a $x \equiv 1 \pmod 2$;
- a divisão por 3 deixa resto 2 equivale a $x \equiv 2 \pmod 3$;
- a divisão por 4 deixa resto 3 equivale a $x \equiv 3 \pmod 4$;
- a divisão por 5 deixa resto 4 equivale a $x \equiv 4 \pmod 5$;
- a divisão por 6 deixa resto 5 equivale a $x \equiv 5 \pmod 6$.

Começando da última congruência, temos $x = 5 + 6y_1$ que na penúltima da

$$5 + 6y_1 \equiv 4 \pmod 5;$$

portanto,

$$y_1 \equiv 4 \pmod 5;$$

donde $y_1 = 4 + 5y_2$. Assim, $x = 29 + 30y_2$. Substituindo na terceira congruência

$$29 + 30y_2 \equiv 3 \pmod 4;$$

isto é,

$$2y_2 \equiv 2 \pmod 4.$$

Mas isto equivale a

$$2y_2 - 2 = 4y_3,$$

que nos dá $y_2 = 1 + 2y_3$. Substituindo em $x = 29 + 30y_2$, obtemos

$$x = 29 + 30y_2 = 59 + 60y_3.$$

Pondo isto na segunda equação,

$$59 + 60y_3 \equiv 2 \pmod 3;$$

que não impõe nenhuma restrição em y_3. Finalmente, substituindo $x = 59 + 60y_3$ na primeira equação

$$59 + 60y_3 \equiv 1 \pmod 2,$$

que também não impõe nenhuma restrição extra. Assim, a solução geral do sistema de congruências é $x = 59 + 60y_3$. Como queremos que

$$1 \leq x \leq 10^5,$$

obtemos

$$1 \leq 59 + 60y_3 \leq 10^5,$$

isto é,

$$-58/60 \leq y_3 \leq 10^5/60.$$

Como y_3 tem que ser inteiro,

$$0 \leq y_3 \leq 1665.$$

Portanto, existem 1666 inteiros satisfazendo às condições desejadas.

Prova 4

1. Sejam $p < q$ primos ímpares e $n = pq$. Prove que $\phi(n) \leq n - \sqrt{n}$.

2. A mensagem

$$17523 - 9183$$

foi codificada usando o RSA com chave pública $n = 26797$ e $e = 4811$. Fatore n usando o algoritmo de Fermat e decodifique a mensagem.

3. Sabe-se que $p = 1093$ é primo e que

$$3^{8\times 1093} \equiv 17488 \pmod{q},$$

onde $q = 16p + 1$. Aplique o teste de Lucas a $q = 16p + 1$ e determine se a saída é *primo*, *composto* ou *indeterminado*.

Resolução

1. Se $n = pq$ então

$$\phi(n) = (p-1)(q-1) = pq - (p+q) + 1 = n - (p+q-1).$$

Para provar o resultado basta mostrar que

$$\sqrt{n} \leq p + q - 1.$$

Contudo, como p é o menor fator primo de n,

$$p \leq \sqrt{n};$$

que implica que

$$q = \frac{n}{p} \geq \frac{n}{\sqrt{n}} = \sqrt{n}.$$

Por outro lado, como p é primo, temos que $p - 1 > 0$. Mas,

$$q \geq \sqrt{n} \text{ e } \quad p - 1 > 0$$

implicam que

$$q + (p-1) \geq \sqrt{n},$$

que é o que precisávamos mostrar.

2. Fatorando $n = 26797$ encontramos os fatores $p = 127$ e $q = 211$. Logo,

$$\phi(n) = 126 \cdot 210 = 26460.$$

Calculando o inverso de $e = 4811$ pelo algoritmo euclidiano estendido, obtemos $d = 11$ (o algoritmo executa quatro etapas). Decodificando

$$17523^{11} \equiv 272 \pmod{n}$$
$$9183^{11} \equiv 810 \pmod{n}$$

A mensagem é 272810; isto é, RSA.

3. Para aplicar o teste de Lucas, fatoramos

$$q - 1 = 2^4 \cdot 1093.$$

Temos dois fatores primos, a saber 2 e 1093. Precisamos calcular, os restos

$$\begin{aligned} r_1 &\equiv 3^{q-1} \pmod{q} \\ r_2 &\equiv 3^{(q-1)/2} \pmod{q} \\ r_3 &\equiv 3^{(q-1)/1093} \pmod{q}. \end{aligned}$$

Como sabemos que

$$3^{8\times 1093} \equiv 17488 \pmod{q},$$

podemos calcular facilmente r_1, já que

$$q - 1 = 16 \cdot 1093 = 2 \cdot (8 \cdot 1093).$$

Isto nos dá,

$$r_1 \equiv (3^{8p})^2 \equiv 17488^2 \equiv 1 \pmod{q}.$$

Por outro lado,

$$r_2 \equiv 3^{(q-1)/2} \equiv 3^{8p} \equiv 17488 \pmod{q}.$$

Finalmente,

$$r_3 \equiv 3^{(q-1)/1093} \equiv 3^{16} \equiv 6292 \pmod{q}.$$

Como $r_1 = 1$, ao passo que $r_2 \neq 1$ e $r_3 \neq 1$, podemos concluir que a saída do teste neste caso é que o número é *primo*.

Prova Final

1. A função $a(n)$ satisfaz $a(1) = a(2) = 1$ e $a(n) = a(n-1) + 2a(n-2) + 1$ para todo $n \geq 3$. Mostre *por indução* em n que

$$a(n) = 2^{n-1} - \frac{(-1)^n + 1}{2}.$$

Explicite cada etapa da indução claramente.

2. Calcule o inverso de 11351 módulo 12347.

3. Considere o número $825265 = 5 \cdot 7 \cdot 17 \cdot 19 \cdot 73$.

   (a) Verifique se 825265 é um número de Carmichael.

   (b) Calcule o resto da divisão de $3^{4126330}$ por 825265.

   (c) Determine o menor inteiro $b > 1$ para o qual 825265 não é pseudoprimo para a base b.

4. Seja $p \geq 2$ um número primo e $n \geq 10^6$ um inteiro. Calcule o resto da divisão de

$$1^{(p-1)n+1} + 2^{(p-1)n+1} + 3^{(p-1)n+1} + \cdots + (p-1)^{(p-1)n+1}$$

por p.

5. Sabe-se que $n = 7025443$ é o produto de dois primos distintos e $\phi(n) = 7012528$. Fatore n e determine o menor inteiro positivo e para o qual o par (n, e) é chave pública de uma versão do RSA.

6. Seja $p > 11$ um número primo e $n = 4p+1$. Tendo aplicado o teste forte de composição a n na base 2, obtivemos a saída inconclusivo. Além disso, sabe-se que $2^{2p} \equiv n - 1 \pmod{n}$. Use esta informação e o teste de Lucas, para mostrar que n é primo.

Primeira Prova–2008/1

1. Prove por indução finita que, para todo $n \geq 1$,

$$2! \cdot 4! \cdot 6! \cdots (2n)! \geq ((n+1)!)^{n-1}.$$

Indique claramente cada etapa da indução.

2. Use o algoritmo euclidiano estendido para determinar um inteiro a de modo que $6765 \cdot a - 1$ seja divisível por 10946.

3. Seja d um número inteiro. Um número $\alpha \in \mathbb{Z}[\sqrt{d}]$ é uma *unidade* se existe $\beta \in \mathbb{Z}[\sqrt{d}]$ tal que $\alpha\beta = 1$.

   (a) Mostre que as únicas unidades de $\mathbb{Z}[\sqrt{-5}]$ são ± 1.

   (b) Determine uma unidade diferente de ± 1 em $\mathbb{Z}[\sqrt{5}]$.

   Sugestão: use as propriedades da norma.

Resolução

1. Seja

$$V = \{n \in \mathbb{N} \mid 2! \cdot 4! \cdot 6! \cdots (2n)! \geq ((n+1)!)^{n-1}\}.$$

Provaremos por indução em n que $V = \mathbb{N}$ o que garante que a desigualdade vale para todo inteiro positivo.

Começamos pela base da indução, que corresponde a mostrar que $1 \in V$. Mas, tomando $n = 1$, verificamos que

$$2! \geq ((1+1)!)^0 = 1$$

de modo que a desigualdade vale neste caso. Portanto, é realmente verdade que $1 \in V$.

Passando, agora, ao passo de indução, precisamos provar que se $k \in V$ então $k+1 \in V$. Contudo, dizer que $k \in V$ equivale a dizer que vale a desigualdade

$$2! \cdot 4! \cdot 6! \cdots (2k)! \geq ((k+1)!)^{k-1}.$$

Multiplicando ambos os membros desta desigualdade por $2(k+1)$, obtemos

$$2! \cdot 4! \cdot 6! \cdots (2k)!(2(k+1))! \geq ((k+1)!)^{k-1}(2(k+1))!. \tag{5}$$

Por outro lado,

$$(2(k+1))! = (k+2)! \cdot (k+3) \cdots (2k).$$

Como $k+i \geq k+2$ se $i \geq 2$ obtemos

$$(2(k+1))! \geq (k+2)! \cdot (k+2)^{k-2};$$

Donde

$$((k+1)!)^{k-1}(2(k+1))! \geq ((k+1)!)^{k-1}(k+2)! \cdot (k+2)^{k-2}$$

cujo lado direito é

$$((k+1)!)^{k-1}(k+2)! \cdot (k+2)^{k-2} = ((k+1)!(k+2))^{k-2}(k+2)! \cdot (k+1)! > ((k+2)!)^{k-1}.$$

assim,

$$((k+1)!)^{k-1}(k+2)! \cdot (k+2)^{k-2} > ((k+2)!)^{k-1}. \tag{6}$$

Combinando as desigualdades em (5) e (6), temos

$$2! \cdot 4! \cdot 6! \cdots (2(k+1))! \geq ((k+2)!)^{k-1}.$$

mostrando que $k+1 \in V$. Portanto, pelo *Princípio de Indução Finita*, $V = \mathbb{N}$ e a desigualdade $2! \cdot 4! \cdot 6! \cdots (2n)! \geq ((n+1)!)^{n-1}$, realmente vale para todo $n \geq 1$.

2. Aplicando o algoritmo euclidiano estendido a 6765 e 10946, obtemos a tabela

resto	quociente	x
10946	**	1
6765	**	0
4181	1	1
2584	1	- 1
1597	1	2
987	1	- 3
610	1	5
377	1	- 8
233	1	13
144	1	- 21
89	1	34
55	1	- 55
34	1	89
21	1	- 144
13	1	233
8	1	- 377
5	1	610
3	1	- 987
2	1	1597
1	1	- 2584

donde concluímos que,

$$\alpha = -2584 \text{ e } \quad \beta = \frac{1 + 2584 \cdot 10946}{6765} = 4181,$$

satisfazem

$$\alpha 10946 + \beta \cdot 6765 = \text{mdc}(6765, 10946) = 1.$$

Portanto,

$$1 - \beta \cdot 6765 = -\alpha 10946$$

e o valor de a é igual ao de β, que é 4181.

3(a). Seja $\alpha \in \mathbb{Z}[\sqrt{-5}]$ uma unidade. Pelas propriedades da norma sabemos que isto significa que $N(\alpha) = 1$. Mas se $\alpha = a + b\sqrt{-5}$, então

$$1 = N(\alpha) = \alpha \cdot \overline{\alpha} = a^2 + 5b^2.$$

Como a^2 e b^2 são positivos e $5b^2 > 1$, precisamos ter $b = 0$. Portanto, $a^2 = 1$ e, como a é inteiro, $a = \pm 1$.

3(b). Seja $\alpha \in \mathbb{Z}[\sqrt{5}]$ uma unidade. Se $\alpha = a + b\sqrt{-5}$ então, pelas propriedades da norma,

$$1 = N(\alpha) = \alpha \cdot \overline{\alpha} = a^2 - 5b^2.$$

Em outras palavras, $1+5b^2 = a^2$. Uma saída a partir daqui é simplesmente tabelar $1+5b^2$ para $b \geq 1$ inteiro e tentar achar um que dê quadrado. O primeiro valor para o qual isto ocorre é $b = 4$ que dá $a = 9$. Contudo, vou proceder de uma maneira mais sistemática. Como $1+5b^2$ deixa resto 1 na divisão por 5, quero saber quais as possibilidades de a para as quais a^2 deixa resto 1 na divisão por 5. Contudo, dividindo a por 5 temos

$$a = 5q + r \text{ onde } \quad 0 \leq r \leq 4.$$

Assim,

$$a^2 = (5q + r)^2 = 5(2qr + 5q^2) + r^2$$

que deixa resto 1 se e somente se r^2 deixa resta 1 na divisão por 5. Testando os casos temos que isto ocorre quando $r = 1$ ou $r = 4$. Logo $a = 5q + 1$ ou $a = 5q + 4$. Contudo $a \neq \pm 1$ implica que $b \geq 1$, donde

$$a = \sqrt{1 + 5b^2} \geq \sqrt{6} = 2,44\ldots.$$

Levando em conta as fórmulas $a = 5q + 1$ ou $a = 5q + 4$ os primeiros valores possíveis para a são

$$6, 9, 11, \ldots$$

Como $36 = 1 + 5 \cdot 7$ e 7 não é quadrado perfeito, passamos a 9 que nos dá $81 = 1 + 5 \cdot 16$. Mas $16 = 4^2$, nos dá $b = 4$ e uma unidade possível é $9 + 4\sqrt{5}$.

Segunda Prova–2008/1

1. Fatore 32881 usando o algoritmo de Fermat.

2. Calcule o resto da divisão de $3^{2^{1024}}$ por 31.

3. Considere a recorrência definida por

$$S_0 = 4 \text{ e } S_{k+1} = S_k^2 - 2.$$

e seja $\omega = 2 + \sqrt{3}$. Prove, por indução em n, que

$$S_n = \omega^{2^n} + \overline{\omega}^{2^n},$$

para todo $n \geq 1$.

1. Como 32881 tem raiz quadrada igual a $181,331...$ devemos calcular a tabela começando com $[181,331...] + 1 = 182$: Portanto, os fatores são

x	$\sqrt{x^2 - n}$	Inteiro?
182	15.58	não
183	24.65	não
184	31.22	não
185	36.66	não
186	41.41	não
187	45.69	não
188	49.62	não
189	53.29	não
190	56.73	não
191	60	sim

$$x + y = 191 + 60 = 251 \text{ e } x - y = 191 - 60 = 131.$$

2. Por Fermat,

$$3^{30} \equiv 1 \pmod{31},$$

Precisamos, portanto, calcular o resto da divisão de 2^{1024} por 30. Contudo,

$$2^5 \equiv 32 \equiv 2 \pmod{30},$$

de modo que

$$2^{10} \equiv (2^5)^2 \equiv 4 \pmod{30}.$$

Assim,

$$\begin{aligned}
2^{1024} &\equiv 2^{1020} \cdot 2^4 \pmod{30} \\
&\equiv (2^{10})^{102} \cdot 2^4 \pmod{30} \\
&\equiv (4)^{102} \cdot 2^4 \pmod{30} \\
&\equiv (2)^{204} \cdot 2^4 \pmod{30} \\
&\equiv (2^{10})^{20} \cdot 2^8 \pmod{30} \\
&\equiv 2^{40} \cdot 16 \pmod{30} \\
&\equiv (2^{10})^4 \cdot 16 \pmod{30} \\
&\equiv (2^2)^4 \cdot 16 \pmod{30} \\
&\equiv 2^{12} \pmod{30} \\
&\equiv 2^{10} \cdot 2^2 \pmod{30} \\
&\equiv 2^4 \equiv 16 \pmod{30}.
\end{aligned}$$

Logo,

$$2^{1024} = 30 \cdot q + 16,$$

para algum inteiro positivo q. Finalmente,

$$3^{2^{1024}} \equiv 3^{30 \cdot q + 16} \equiv (3^{30})^q \cdot 3^{16} \pmod{31}.$$

Usando o teorema de Fermat e uma calculadora,

$$(3^{30})^q \cdot 3^{16} \equiv 3^{16} \equiv 28 \pmod{31}.$$

Assim, o resto da divisão é 28.

3. Seja V o conjunto definido por

$$V = \{n \in \mathbb{N} \cup \{0\} : S_n = \omega^{2^n} + \overline{\omega}^{2^n}\}.$$

De acordo com o Princípio de Indução Finita, se mostrarmos que

(a) $0 \in V$;

(b) se $k \in V$ então $k + 1 \in V$;

então podemos concluir que $V = \mathbb{N} \cup \{0\}$.

Comecemos com a base da indução. Por definição da recorrência, $S_0 = 4$ enquanto que

$$\omega^{2^0} + \overline{\omega}^{2^0} = \omega^1 + \overline{\omega}^1.$$

Contudo,

$$\omega + \overline{\omega} = (2 + \sqrt{3}) + (2 - \sqrt{3}) = 4,$$

confirmando que $0 \in V$.

A hipótese de indução nos diz que

$$S_k = \omega^{2^k} + \overline{\omega}^{2^k},$$

para algum $k \in V$ e, a partir dela, queremos mostrar que

$$S_{k+1} = \omega^{2^{k+1}} + \overline{\omega}^{2^{k+1}}.$$

Para isto usamos a recorrência

$$S_{k+1} = S_k^2 - 2.$$

Substituindo a hipótese de indução na recorrência,

$$S_{k+1} = (\omega^{2^k} + \overline{\omega}^{2^k})^2 - 2.$$

Elevando ao quadrado,

$$S_{k+1} = (\omega^{2^k})^2 + (\overline{\omega}^{2^k})^2 + 2\omega^{2^k}\overline{\omega}^{2^k} - 2.$$

Contudo,

$$\omega\overline{\omega} = N(\omega) = 1;$$

de forma que

$$\omega^{2^k}\overline{\omega}^{2^k} = (\omega\overline{\omega})^{2^k} = 1,$$

e assim

$$S_{k+1} = (\omega^{2^k})^2 + (\overline{\omega}^{2^k})^2 = \omega^{2^{k+1}} + \overline{\omega}^{2^{k+1}},$$

que era o que queríamos provar. Logo, pelo Princípio de Indução Finita, podemos concluir que $V = \mathbb{N} \cup \{0\}$ como desejávamos.

Terceira Prova–2008/1

1. Use o algoritmo chinês do resto para determinar se 217 é pseudoprimo forte para a base 6.

2. Seja $n = 5 \cdot p \cdot (p + 12)$. Calcule os resíduos de $n - 1$ módulo $q - 1$ para $q = 5$, $q = p$ e $q = p + 12$ e use isto para determinar o menor primo $p > 5$ para o qual n é um número de Carmichael. Explique cada etapa do seus cálculos. **Soluções por tentativa não serão aceitas!**

3. Seja p um número inteiro *primo*. Prove que se a é um inteiro que satisfaz $a \not\equiv 0 \pmod{p}$, então $a+b\sqrt{p}$ é inversível relativamente à congruência módulo p em $\mathbb{Z}[\sqrt{p}]$.

Resolução

1. Em primeiro lugar $n = 7 \cdot 31$ é composto e ímpar. Como $n - 1 = 216 = 2^3 \cdot 27$, temos que $k = 3$ e $q = 27$. Devemos aplicar o teste forte de composição e, para isto, precisamos calcular

$$\begin{aligned} r_0 &\equiv 6^{27} \pmod{7} \\ r_0 &\equiv 6^{27} \pmod{31}. \end{aligned}$$

Mas $6 \equiv -1 \pmod{7}$, o que nos dá

$$r_0 \equiv 6^{27} \equiv (-1)^{27} \equiv -1 \equiv 6 \pmod{7}.$$

Por outro lado, $2^5 \equiv 1 \pmod{31}$ e $3^3 \equiv -4 \pmod{31}$, donde

$$r_0 \equiv 6^{27} \equiv (2^5)^5 \cdot 2^2 \cdot (3^3)^9 \equiv 4 \cdot -4^9 \equiv -4^{10} \equiv 30 \pmod{31}.$$

Com isto obtemos o sistema

$$\begin{aligned} r_0 &\equiv 6 \pmod{7} \\ r_0 &\equiv 30 \pmod{31}, \end{aligned}$$

que vamos resolver pelo algoritmo chinês do resto. Tomando o valor de r_0 da segunda congruência, obtemos

$$r_0 = 30 + 31x,$$

que, quando substituído na primeira congruência nos dá

$$30 + 31x \equiv 6 \pmod{7}; \text{ isto é, } 3x \equiv -24 \pmod{7}.$$

Como 3 e 7 são primos entre si, podemos cancelar 3 nesta congruência obtendo

$$x \equiv -8 \equiv 6 \pmod{7}.$$

Assim,

$$x = 6 + 7t$$

donde

$$r_0 = 30 + 31(6 + 7t) = 216 + 217t.$$

Como

$$r_0 = 216$$

já podemos parar e concluir que a saída do teste forte de composição é *inconclusivo*, de modo que 217 é mesmo pseudoprimo forte para a base 6.

Pensando um pouco, poderíamos ter evitado a aplicação do algoritmo chinês. Bastava observar que

$$\begin{aligned} r_0 &\equiv 6 \equiv -1 \pmod 7 \\ r_0 &\equiv 30 \equiv -1 \pmod{31}, \end{aligned}$$

de modo que, como 7 e 31 são primos entre si,

$$r_0 \equiv -1 \pmod{217};$$

o que garante, imediatamente, que 217 é pseudoprimo forte para a base 6.

2. Pelo teorema de Korselt, para que $n = 5 \cdot p \cdot (p+12)$ seja Carmichael, devemos ter que as multiplicidades de cada primo é um (que é obviamente verificado para n) e que

$$\begin{aligned} n - 1 &\equiv 0 \pmod 4 \\ n - 1 &\equiv 0 \pmod{p-1} \\ n - 1 &\equiv 0 \pmod{p+11}. \end{aligned}$$

Contudo, fazendo as contas diretamente da definição de n, obtemos

$$\begin{aligned} n - 1 &\equiv p^2 - 1 \pmod 4 \\ n - 1 &\equiv 64 \pmod{p-1} \\ n - 1 &\equiv -56 \pmod{p+11}. \end{aligned}$$

Em particular, da segunda congruência, $p-1$ tem que dividir $64 = 2^6$, o que nos dá

$$p - 1 = 2^k \text{ para algum } \quad 1 \leq k \leq 4.$$

Como, para que a primeira congruência seja satisfeita precimos de $k \geq 2$, temos

$$p = 1 + 2^k \text{ para algum } \quad 2 \leq k \leq 4.$$

Isto implica, pela terceira congruência, que

$$p + 11 = 12 + 2^k$$

deve dividir 56. Entretanto, $k = 2$ nos dá $p + 11 = 16$, $k = 3$ nos dá $p + 11 = 20$, nenhum dos quais divide 56. Resta-nos, apenas, $k = 4$ que nos dá $p + 11 = 28$ que divide 56. Por outro lado, $k = 4$ significa que

$$p = 17 \text{ e } \quad p + 12 = 29,$$

ambos primos. Portanto, o número de Carmichael será

$$n = 5 \cdot 17 \cdot 29 = 2465.$$

3. Seja $\alpha = a + b\sqrt{p}$ e vamos multiplicá-lo por seu inverso $\overline{\alpha}$,

$$\alpha \cdot \overline{\alpha} = a^2 - b^2 p.$$

Tomando isto módulo p, vemos que

$$\alpha \cdot \overline{\alpha} \equiv a^2 - b^2 p \equiv a^2 \pmod{p}.$$

Levando em conta que p é primo, vemos que se $a \not\equiv 0 \pmod{p}$ então a é inversível módulo p. Se a' for o inverso de a módulo p, então

$$\alpha \cdot (a')^2 \overline{\alpha} \equiv (a')^2 \cdot a^2 \equiv (a' \cdot a)^2 \equiv 1 \pmod{p};$$

de forma que α tem inverso $(a')^2 \overline{\alpha}$ módulo p.

Quarta Prova–2008/1

1. Em sua viagem de volta ao quadrante Alfa, a *Voyager* encontrou uma nave da federação abandonada a centenas de anos. A nave havia sido atacada e os tripulantes desapareceram. Uma mensagem codificada usando o RSA havia sido deixada identificando os agressores. O código usado tinha chave pública $n = 53671$ e $e = 35467$ e a mensagem era

$$44231 - 4403 - 8178.$$

Quebre o código, decodifique a mensagem e descubra quem foram os agressores.

2. "Resolvi aplicar o teste de composição forte a um número ímpar $n > 10^6$. Determinei k e q de modo que $n - 1 = 2^k q$ e q é ímpar, e um cálculo adicional mostrou que $2^q \equiv -1 \pmod{n}$. Neste momento, observei que k era igual a ..... e que q era ..... e isto me permitiu usar imediatamente o teste de Lucas e concluir que n era um número primo". Preencha as lacunas, justificando cuidadosamente a sua resposta.

3. Seja $p > 10^8$ um primo tal que $p \equiv 2 \pmod{3}$.

   (a) Use o teorema de Fermat para mostrar que se $\alpha = a + b\sqrt{p}$, então $\alpha^3 \equiv a - b \pmod{3}$.

   (b) Use (b) para determinar todos os elementos de $U(\mathbb{Z}_3[\sqrt{p}])$ e a ordem de cada um deles. Este grupo é cíclico?

Prova Final–2008/1

1. (2,0 pontos) Prove, por indução em n, que

$$\sum_{j=1}^{n} k \cdot k! = (n+1)! - 1.$$

2. (1,0 ponto) Ache a solução geral da equação diofantina $8713x + 877y = 12$.

3. (1,5 pontos) Calcule a ordem de 7 módulo 29 e use isto para determinar o resto da divisão de $7^{8^{1024}}$ por 29.

4. (2,0 pontos) Considere o número 91.

   (a) Verifique se 91 é um número de Carmichael.

   (b) Calcule o resto da divisão de 9^{45} por 91 pelo algoritmo chinês do resto.

   (c) Determine se 91 é um pseudoprimo para a base 9.

   (d) Determine se 91 é um pseudoprimo *forte* para a base 9.

5. (2,0 pontos) Considere $n = 1089307$ e $e = 465943$.

   (a) Fatore n usando o algoritmo de Fermat.

   (b) Decodifique a mensagem 774203 sabendo-se que foi utilizado o RSA com chave pública (n, e). A mensagem é um número mas, se você decodificar corretamente, vai saber que acertou.

6. (1,5 pontos) Calcule a ordem do grupo $U(\mathbb{Z}_7[\sqrt{7}])$ e determine se este grupo é cíclico.

Primeira Prova–2008/2

1. Seja F_n o n-ésimo número de Fibonacci; isto é:

$$F_0 = 0, \quad F_1 = 1 \quad \text{e} \quad F_{n+1} = F_n + F_{n-1}.$$

Prove, *por indução em* n que F_{3n} é par para todo $n \geq 0$. Indique claramente cada etapa da indução.

2. Determine uma infinidade de múltiplos de 12354 e de 7854 cuja soma seja 18.

3. Seja $p > 0$ um número primo. Um número $\alpha \in \mathbb{Z}[\sqrt{-p}]$ é *irredutível* se seus únicos divisores são ± 1 e $\pm\alpha$.

   (a) Mostre que se a norma de $\alpha \in \mathbb{Z}[\sqrt{-p}]$ é um número inteiro primo, então α é irredutível em $\mathbb{Z}[\sqrt{-p}]$.

   (b) Use (a) para determinar elementos irredutíveis em $\mathbb{Z}[\sqrt{-3}]$ e em $\mathbb{Z}[\sqrt{-7}]$.

Resolução

1. Seja

$$V = \{n \in \mathbb{N} \,|\, F_{3n} \text{ é par } \}.$$

Provaremos por indução em n que $V = \mathbb{N}$ o que garante que a desigualdade vale para todo inteiro não negativo.

Começamos pela base da indução, que corresponde a mostrar que $0 \in V$. Mas, tomando $n = 0$, verificamos que

$$F_0 = 0$$

que é um número par. Portanto, é realmente verdade que $0 \in V$.

Passando, agora, ao passo de indução, precisamos provar que se $k \in V$ então $k+1 \in V$. Contudo, dizer que $k \in V$ equivale a dizer que F_{3k} é par. Mas, pela recorrência de Fibonacci,

$$F_{3(k+1)} = F_{3k+2} + F_{3k+1}.$$

Usando a recorrência novamente,

$$F_{3k+2} = F_{3k+1} + F_{3k}.$$

Substituindo na equação anterior,

$$F_{3(k+1)} = F_{3k+2} + F_{3k+1} = (F_{3k+1} + F_{3k}) + F_{3k+1};$$

donde

$$F_{3(k+1)} = 2F_{3k+1} + F_{3k}.$$

resto	quociente	x
12354	**	1
7854	**	0
4500	1	1
3354	1	- 1
1146	1	2
1062	2	- 5
84	1	7
54	12	- 89
30	1	96
24	1	- 185
6	1	281

Mas F_{3k} é par pela hipótese de indução e o outro termo é claramente múltiplo de 2. Como soma de números pares dá um número par, concluímos que $F_{3(k+1)}$ é par. Logo, $k+1 \in V$. Portanto, pelo *Princípio de Indução Finita*, $V = \mathbb{N}$; isto é F_{3n} é par para todo $n \geq 0$.

2. Aplicando o algoritmo euclidiano estendido a 12354 e de 7854, obtemos a tabela donde concluímos que,

$$\alpha = 281 \text{ e } \beta = \frac{6 - 281 \cdot 12354}{7854} = -442,$$

satisfazem

$$\alpha \cdot 12354 + \beta \cdot 7854 = \text{mdc}(12354, 7854) = 6.$$

Uma escolha de infinitos múltiplos cuja soma dão 18 é

$$12354 \cdot 3 \cdot (281 - 7854k) \text{ e } 7854 \cdot 3 \cdot (-442 + 12354k).$$

3(a). Seja $\alpha \in \mathbb{Z}[\sqrt{-p}]$ e suponhamos que $N(\alpha) = q$ um primo (que pode ser igual ou diferente de p). Digamos que $\alpha = \beta\gamma$, onde β e γ são elementos de $\mathbb{Z}[\sqrt{-p}]$. Pelas propriedades da norma, temos que

$$N(\alpha) = N(\beta)N(\gamma).$$

Mas $N(\alpha) = q$, de modo que

$$q = N(\beta)N(\gamma).$$

Como q é primo isto significa que uma das normas, digamos a de β, tem que ser igual a 1 (não pode ser -1 porque as normas de elementos de $\mathbb{Z}[\sqrt{-p}]$ são todas positivas). Logo, $N(\beta) = 1$. Contudo, se $\beta = a + b\sqrt{-p}$ então

$$1 = N(\beta) = a^2 + pb^2.$$

Como $p > 1$, isto implica que $b = 0$ e que $a^2 = 1$. Logo, $a = \pm 1$ e, portanto, $\beta = \pm 1$. Mas isto significa que

$$\beta = \pm 1 \text{ e } \gamma = \pm\alpha$$

é a única fatoração possível para α. Logo provamos que α é irredutível.

3(b). Tentaremos construir elementos cuja norma é um primo, tanto em $\mathbb{Z}[\sqrt{-3}]$, quanto em $\mathbb{Z}[\sqrt{-7}]$. Mas $a + b\sqrt{-3}$ tem norma

$$a^2 + 3b^2;$$

de modo que $a = 2$ e $b = 1$ nos dá $4+3 = 7$ que é primo e $a = 1$, $b = 2$ nos dá $1+3\cdot 4 = 13$. Assim, por (a),

$$2 + \sqrt{-3} \text{ e } 1 + 2\sqrt{-3}$$

são irredutíveis em $\mathbb{Z}[\sqrt{-3}]$. Procedendo de maneira semelhante, verificamos que

$$2 + \sqrt{-7} \text{ e } 1 + 2\sqrt{-7}$$

Segunda Prova–2008/2

1. Fatore 1994653 usando o algoritmo de Fermat.

2. Sabe-se que $3^{2^7} \equiv 256 \pmod{257}$.
   (a) Calcule a ordem de 3 módulo 257 e determine quantos são os resíduos diferentes das potências de 3 módulo 257.
   (b) Calcule o resíduo de 3^{2307} módulo 257.

3. Seja d um inteiro livre de quadrados. Prove que, se α é irredutível em $\mathbb{Z}[\sqrt{d}]$, então seu conjugado $\widehat{\alpha}$ também é.

Resolução

1. Para começar temos que

$$\sqrt{1994653} = 1412,32$$

que não é inteiro. Construindo a tabela a partir de

$$[\sqrt{1994653}] = 1413$$

temos:

x	$\sqrt{x^2 - n}$	Inteiro?
1413	43,77	não
1414	68,86	não
1415	87,01	não
1416	101,99	não
1417	115,04	não
1418	126,77	não
1419	137,50	não
1420	147,46	não
1421	156,80	não
1422	165,62	não
1423	174	sim

Portanto, os fatores são

$$x + y = 1423 + 174 = 1597 \text{ e } \quad x - y = 1423 - 174 = 1249.$$

2. (a) Como

$$3^{2^7} \equiv 256 \equiv -1 \pmod{257},$$

temos que

$$(3^{2^7})^2 \equiv (-1)^2 \equiv 1 \pmod{257}.$$

Pelo lema chave, a ordem de 3 módulo 257 tem que dividir 2^8, mas não pode ser menor que 2^8 porque $3^{2^7} \not\equiv 1 \pmod{257}$. Logo a ordem é exatamente 2^8 e, portanto, existem 2^8 resíduos diferentes de potências módulo 257

(b) Já vimos que

$$3^{2^8} \equiv 1 \pmod{257}.$$

Como $2307 = 2^8 \cdot 9 + 3$, temos que

$$3^{2307} \equiv (3^{2^8})^9 \cdot 3^3 \equiv 9 \pmod{257}.$$

Portanto o resíduo desejado é 9.

3. Seja d um inteiro livre de quadrados e suponhamos que α é irredutível em $\mathbb{Z}[\sqrt{d}]$. Neste caso, se

$$\widehat{\alpha} = \beta\gamma,$$

onde $\beta, \gamma \in \mathbb{Z}[\sqrt{d}]$, então pelas propriedades do conjugado

$$\alpha = \widehat{\widehat{\alpha}} = \widehat{\beta}\widehat{\gamma}.$$

Como α é irredutível, então $\widehat{\beta}$ ou $\widehat{\gamma}$ tem que ser uma unidade. Se $\widehat{\beta}$ for a unidade, então

$$N(\widehat{\beta}) = \pm 1.$$

Como a norma de um elemento e de seu conjugado coincidem, então

$$N(\beta) = N(\widehat{\beta}) = \pm 1,$$

de modo que β também é uma unidade. Mas isto implica que $\widehat{\alpha}$ é irredutível.

Terceira Prova–2008/2

1. Determine:

   (a) se 65 é pseudoprimo forte para a base 8;

   (b) a menor base para a qual 65 não é pseudoprimo.

2. Use o algoritmo chinês do resto para resolver o seguinte problema:

   > Uma velha senhora vai ao mercado e um cavalo pisa em sua cesta e quebra dois dos ovos que lá estão. O cavaleiro se oferece para pagar pelo dano e lhe pergunta quantos ovos ela havia trazido. Ela não lembra o número exato mas, ao removê-los aos pares, sobra apenas um ovo; ao removê-los de três em três, sobram 2 ovos, e ao removê-los de 5 em 5 sobram 3 ovos. Qual o menor número de ovos que podia haver na cesta quando ela saiu de casa?

3. Seja $\alpha = 1 + 2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Calcule α^3 módulo 11, determine a ordem módulo 11 do resíduo obtido deste cálculo e use isto para determinar a ordem de α módulo 11.

Resolução

1.(a) $65-1 = 64 = 2^8$, de modo que $k = 8$ e $q = 1$ na notação do teste forte de composição usada em aula. Portanto, devemos calcular

$$r_0 \equiv 8^1 \pmod{65},$$

do qual nada podemos concluir porque não é congruente a 1 nem a 64. Contudo,

$$r_1 \equiv r_0^2 \equiv 64 \pmod{65},$$

de modo que $r_1 \equiv -1 \pmod{65}$ e, portanto, 65 tem por saída inconclusivo no teste forte de composição. Como 65 é composto e ímpar, trata-se de um pseudoprimo forte para a base 8.

1.(b) A menor base é 2, porque

$$(2^{64}) \equiv ((2)^8)^8 \equiv (-1)^8 \equiv 1 \pmod{65}.$$

não é congruente a 1 módulo 65.

2. Seja x o número de ovos na sesta depois que os dois ovos foram quebrados. Como

- removendo os ovos aos pares, sobra apenas um ovo: $x \equiv 1 \pmod{2}$;
- removendo os ovos de três em três, sobram 2 ovos: $x \equiv 2 \pmod{3}$;

- removendo os ovos de 5 em 5 sobram 3 ovos: $x \equiv 3 \pmod 5$.

Resolvendo o sistema pelo algoritmo chinês do resto temos, da última congruência, que

$$x = 3 + 5y.$$

Substituindo na segunda congruência:

$$3 + 5y \equiv 2 \pmod 3,$$

de modo que

$$2y \equiv 2 \pmod 3.$$

Como $\text{mdc}(2, 3) = 1$ podemos cancelar 2 obtendo $y \equiv 1 \pmod 3$, donde

$$x = 3 + 5(1 + 3k) = 8 + 15k.$$

Substituindo isto na primeira equação:

$$8 + 15k \equiv 1 \pmod 2;$$

que nos dá

$$k \equiv 1 \pmod 2.$$

Assim, $k = 1 + 2t$ e obtemos finalmente,

$$x = 8 + 15k = 8 + 15(1 + 2t) = 23 + 30t.$$

Logo, a menor quantidade de ovos possível *depois* que o cavalo quebrou dois é de 23 ovos. Portanto, ao sair de casa a velha senhora tinha, *no mínimo*, 25 ovos.

Esta é uma variante de um problema proposto pelo matemático indiano Brahmagupta, nascido em 598 d.C..

3. Temos que

$$\alpha^3 = 25 + 22\sqrt{2},$$

de modo que

$$\alpha^3 \equiv 3 \pmod{11}.$$

Pelo teorema de Fermat,

$$3^{10} \equiv 1 \pmod{11}.$$

Logo, pelo lema chave, 3 tem ordem 2, 5 ou 10 módulo 11. Como $3^2 = 9 < 11$ é claro que a ordem não pode ser 2. Por outro lado,

$$3^5 \equiv 3^4 \cdot 3 \equiv 4 \cdot 3 \equiv 1 \pmod{11}.$$

Portanto, 3 tem ordem 5 módulo 11. Então,

$$(\alpha^3)^5 \equiv 3^5 \equiv 1 \pmod{11}.$$

Logo, pelo lema chave, α tem ordem 5 ou 15 (3 já foi descartado). Mas,

$$\alpha^5 \equiv 3 \cdot \alpha^2 \equiv 3 \cdot (4 + 9\sqrt{2}) \equiv 1 + 5\sqrt{2} \pmod{11}.$$

Podemos, pois, concluir que α tem ordem 15 módulo 11.

1. De férias em Betazed, a conselheira Troi recebe uma caixa de seu chocolate Ktariano favorito, juntamente com uma mensagem criptografada do remetente revelando sua identidade. Uma rápida pesquisa em seu tricorder revela a Troi que se trata de um velho código terrestre chamado RSA que está obsoleto desde o fim do século XXI. Sabendo que a mensagem é

$$4454 - 7384$$

e que foi codificada usando o par $(11659, 7627)$ como chave pública, decodifique-a e descubra quem enviou o chocolate à conselheira Troi.

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

2. Seja $n = 3 \cdot 2^{12} + 1$. Sabe-se que $11^{2^{11}} \equiv 6241 \pmod{n}$. Use estes dados e o teste de Lucas para provar que n é primo.

3. Seja $p > 10^{987655}$ um número primo e $d > 0$ um inteiro livre de quadrados.

   (a) Prove que $\overline{-1 + pk\sqrt{d}}$ tem ordem $2p$ em $U(\mathbb{Z}_{p^2}[\sqrt{d}])$, qualquer que seja $0 < k < p$.

   (b) O que (a) nos diz sobre a ordem de $|U(\mathbb{Z}_{p^2}[\sqrt{d}])|$?

Resolução

1. Aplicando o algoritmo de Fermat a $n = 11659$ obtemos na terceira etapa que $x = 110$ e $y = 21$, de modo que os fatores são

$$p = x + y = 131 \text{ e } \quad q = x - y = 89.$$

Logo,

$$\phi(n) = (p-1)(q-1) = 11440.$$

Invertendo $e = 7627$ módulo $\phi(n)$ pelo algoritmo euclidiano estendido, descobrimos que $d = 3$. Decodificando temos que

$$4454^3 \equiv 1310 \pmod{11569}$$
$$7384^3 \equiv 1310 \pmod{11569}$$

de modo que quem enviou o presente foi o DATA.

2. Como $n-1=3\cdot 2^{12}$, então, para aplicar o teste de Lucas na base 5 devemos mostrar que

$$11^{3\cdot 2^{12}}\equiv 1 \pmod{3\cdot 2^{12}+1};$$

e também que

$$11^{3\cdot 2^{11}}\not\equiv 1 \pmod{3\cdot 2^{12}+1};\ \text{e}$$
$$11^{\cdot 2^{12}}\not\equiv 1 \pmod{3\cdot 2^{12}+1}.$$

Contudo, como foi dado que $2^{2^{11}}\equiv -189 \pmod{n}$, então

$$11^{3\cdot 2^{11}}\equiv (11^{2^{11}})^3\equiv (6241)^3\equiv 12288 \pmod{n}; 11^{2^{12}} \equiv (11^{2^{11}})^2\equiv (6241)^2\equiv 6240 \pmod{n}$$

nenhum dos quais não é congruente a 1. Portanto, só falta verificar a primeira das congruências acima. Mas,

$$11^{3\cdot 2^{12}}\equiv ((11^{2^{11}})^2)^3\equiv (6240)^3\equiv 1 \pmod{3\cdot 2^{12}+1};$$

como desejado. Logo, o teste de Lucas confirma que $=3\cdot 2^{12}+1$ é mesmo um número primo.

3. Seja $p>10^{987655}$ um número primo e $d>0$ um inteiro livre de quadrados. Começamos calculando $(-1+pk\sqrt{d})^{2p}$ módulo p^2. Mas, pelo binômio de Newton,

$$(-1+pk\sqrt{d})^{2p}=(-1)^{2p}+\sum_{j=1}^{2p}\binom{2p}{j}(-1)^{2p-j}(pk\sqrt{d})^j$$

de modo que aparece um p^2 multiplicando todos os termos com $j\geq 2$. Com isso,

$$(-1+pk\sqrt{d})^{2p}\equiv 1+\binom{2p}{1}(-1)^{2p-1}(pk\sqrt{d}) \pmod{p^2};$$

isto é,

$$(-1+pk\sqrt{d})^{2p}\equiv 1+2p(-1)^{2p-1}(pk\sqrt{d})\equiv 1 \pmod{p^2}.$$

Portanto, a ordem de $\overline{-1+pk\sqrt{d}}$ em $U(\mathbb{Z}_{p^2}[\sqrt{d}])$ divide $2p$. Como p é primo, a ordem ou será 1, ou 2 ou p. Entretanto, $\overline{-1+pk\sqrt{d}}\neq\overline{1}$, pois $pk\not\equiv 0 \pmod{p^2}$ se $0<k<p$. Logo, a ordem não pode ser 1. Por outro lado,

$$\overline{(-1+pk\sqrt{d})}^2=\overline{1-2pk\sqrt{d}+p^2k^2\sqrt{d}}=\overline{1-2pk\sqrt{d}}\neq 1$$

pela mesma razão anterior (lembrando que $p>2$); de modo que a ordem também não é igual a 2. Finalmente,

$$(-1+pk\sqrt{d})^{p}\equiv -1+\binom{p}{1}(-1)^{p-1}(pk\sqrt{d}) \pmod{p^2};$$

isto é,

$$(-1+pk\sqrt{d})^{p}\equiv -1+p(-1)^{p-1}(pk\sqrt{d})\equiv -1 \pmod{p^2};$$

e a ordem não é p. Portanto, a ordem tem que ser mesmo $2p$.

Passando a letra (b), como $\overline{-1+pk\sqrt{d}}$ tem ordem $2p$ em $U(\mathbb{Z}_{p^2}[\sqrt{d}])$, então $2p$ tem que dividir $|U(\mathbb{Z}_{p^2}[\sqrt{d}])|$.

Prova Final–2008/2

1. (2,0 pontos) Seja F_n o n-ésimo número de Fibonacci. Isto é: $F_1 = F_2 = 1$ e $F_{n+1} = F_n + F_{n-1}$. Mostre, *por indução em* n, que

$$F_1^2 + F_2^2 + \cdots + F_n^2 = F_n F_{n+1}.$$

   Explicite cada etapa da indução claramente.

2. (2,0 pontos) Calcule a ordem de 5 módulo 28 e use isto para achar o resto da divisão de $3^{5^{1024}}$ por 29.

3. (2,0 pontos) Considere o número $6601 = 7 \cdot 23 \cdot 41$.

   (a) Verifique se 6601 é um número de Carmichael.

   (b) Calcule o resto da divisão de 2^{825} por 6601 pelo algoritmo chinês do resto.

   (c) Determine se 6601 é um pseudoprimo *forte* para a base 2.

4. (2,0 pontos) Considere $n = 19291$.

   (a) Fatore n usando o algoritmo de Fermat e determine seus fatores p e q.

   (b) Construa uma chave pública (n, e) para o RSA usando o valor de n acima e determine a chave secreta correspondente.

   (c) Codifique a palavra $FINAL$ usando sua chave pública.

5. (2,0 pontos) Seja $\alpha = 1 + 2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Calcule α^3 módulo 11, determine a ordem módulo 11 do resíduo obtido deste cálculo e use isto para determinar a ordem de α módulo 11.

Primeira Prova–2009/1

1. Seja $m \geq 10^{900}$ um inteiro fixado. Prove, *por indução em* n, que

$$\binom{n+m}{m} \geq 2(n+1)$$

para todo $n \geq 1$. Indique claramente cada etapa da indução.

2. Considere o número 36031.

   (a) Ache os dois fatores primos de n usando o algoritmo de Fermat.

   (b) Se aplicarmos o algoritmo usual de fatoração (`acha fator`) a n, quantos laços ele executaria até parar?

3. Sabe-se que todos os elementos invertíveis de $\mathbb{Z}[\sqrt{17}]$ são da forma $\pm\omega^n$ para algum $n \in \mathbb{Z}$, em que $\omega = 4 + \sqrt{17}$.

   (a) Prove que o conjunto G dos elementos de norma *um* em $\mathbb{Z}[\sqrt{17}]$ é um grupo.

   (b) Determine todos os elementos de G.

Resolução

1. Seja

$$V = \{n \in \mathbb{N} \setminus \{0\} \mid \binom{n+m}{m} \geq 2(n+1)\}.$$

Provaremos por indução em n que $V = \mathbb{N} \setminus \{0\}$ o que garante que a desigualdade vale para todo inteiro positivo.

Começamos pela base da indução, que corresponde a mostrar que $0 \in V$. Mas, tomando $n = 1$, verificamos que

$$\binom{n+m}{m}|_{n=1} = \binom{m+1}{m} = m+1;$$

ao passo que $2(n+1) = 4$. Dada a restrição sobre m, a desigualdade é evidentemente verdadeira. Portanto, $0 \in V$.

Passando, agora, ao passo de indução, precisamos provar que se $k \in V$ então $k+1 \in V$. Contudo, dizer que $k \in V$ equivale a dizer que

$$\binom{k+m}{m} \geq 2(k+1)$$

é verdadeira. Contudo,

$$\binom{k+m+1}{m} = \frac{(k+m+1)!}{m!(k+1)!}$$

donde,

$$\binom{k+m+1}{m} = \frac{(k+m+1)}{k+1}\frac{(k+m)!}{m!k!}$$

e, assim,

$$\binom{k+m+1}{m} = \frac{(k+m+1)}{k+1}\binom{k+m}{m}.$$

Usando a hipótese de indução, vemos que

$$\binom{k+m+1}{m} = \frac{(k+m+1)}{k+1} \geq 2(k+1).$$

Portanto,

$$\binom{k+m+1}{m} \geq \frac{(k+m+1)}{k+1}2(k+1).$$

Entretanto, o lado direito desta última equação é igual a

$$2(m+k+1) > 2(k+2),$$

pois $m > 1$. Combinando estas as duas desigualdades acima, concluímos que

$$\binom{k+m+1}{m} \geq 2(k+2),$$

o que prova que $k+1 \in V$. Portanto, pelo *Princípio de Indução Finita*, $V = \mathbb{N} \setminus \{0\}$; isto é

$$\binom{n+m}{m} \geq 2(n+1)$$

para todo $n \geq 1$.

2. Para começar temos que

$$\sqrt{36031} = 189,81$$

que não é inteiro. Construindo a tabela a partir de

$$[\sqrt{36031}] = 190$$

temos:

x	$\sqrt{x^2-n}$	Inteiro?
190	$8,306$	não
191	$21,213$	não
192	$28,861$	não
193	$34,899$	não
194	$40,062$	não
195	$44,654$	não
196	$48,836$	não
197	$52,706$	não
198	$56,329$	não
199	$59,749$	não
200	63	sim

Portanto, os fatores são

$$x + y = 200 + 63 = 263 \text{ e } \quad x - y = 200 - 63 = 137.$$

3(a). O conjunto G é um grupo se

1. $1 \in G$;
2. se $\alpha, \beta \in G$, então $\alpha\beta \in G$;
3. se $\alpha \in G$, então $1/\alpha \in G$.

Verificaremos cada uma destas propriedades separadamente. Em primeiro lugar, é claro que $1 \in G$, porque 1 tem norma igual a 1, que é a propriedade que define a pertinência de um elemento de $\mathbb{Z}[\sqrt{17}]$ a G.

Em segundo lugar, se

$$\alpha, \beta \in \mathbb{Z}[\sqrt{17}]$$

têm norma igual a 1, então

$$N(\alpha\beta) = N(\alpha)N(\beta) = 1 \cdot 1 = 1.$$

Logo, o produto $\alpha\beta$ também tem norma 1, de modo que $\alpha\beta \in G$.

Finalmente, se

$$\alpha \in \mathbb{Z}[\sqrt{17}]$$

têm norma igual a 1, então

$$N(\alpha\frac{1}{\alpha}) = N(1) = 1,$$

mas, também temos que

$$N(\alpha\frac{1}{\alpha}) = N(\alpha)N(\frac{1}{\alpha}) = N(\frac{1}{\alpha}),$$

pelas propriedades da norma. Logo, $1/\alpha$ também tem norma 1, de modo que $1/\beta \in G$.

3(b). Temos que todo elemento invertível de $\mathbb{Z}[\sqrt{17}]$ é da forma $\pm\omega^n$, para algum $n \in \mathbb{Z}$. Como $\omega = 4 + \sqrt{17}$ tem norma -1, para obter $N(\alpha) = 1$, devemos ter que α é, a menos de sinal, uma potência par de ω. Portanto,

$$G = \{\pm\omega^{2k} | k \in \mathbb{Z}\}.$$

Segunda Prova–2009/1

1. Prove, por indução em n, que

$$7 + 5 + 3 + \cdots + (9 - 2n) = -n^2 + 8n.$$

Indique claramente cada etapa da indução.

2. O objetivo desta questão é mostrar que existem infinitos primos positivos p que satisfazem a condição $p \equiv 5 \pmod 6$. Suponha, por contradição, que $p_1, \ldots, p_m$ são *todos* os primos diferentes de 5, que deixam resto 5 na divisão por 6. Seja $N = p_1 \cdots p_m$.

   (a) Calcule os possíveis resíduos de $6N + 5$ módulo 6.

   (b) Prove que (a) implica que $6N + 5$ tem que ter um fator *primo* que deixa resto 5 na divisão por 6.

   (c) Use $\text{mdc}(N, 6N + 5) = 1$ e (b) para provar que existem infinitos números primos que deixam resto 5 na divisão por 6.

3. Sabe-se que 3 tem ordem 126 módulo 127. **Use isto** para:

   (a) determinar as ordens de 9 e de 27 módulo 127;

   (b) calcular o resto da divisão de 9^{250049} por 127.

   A sua resposta à letra (a) deve ser cuidadosamente justificada utilizando os resultados provados em aula.

Resolução

1. Seja

$$S_n = 7 + 5 + 3 + \cdots + (9 - 2n).$$

Nosso objetivo é provar por indução em n que

$$S_n = -n^2 + 8n,$$

para todo $n \geq 1$. Seja

$$V = \{n \in \mathbb{N}_{\geq 1} | S_n = -n^2 + 8n\}.$$

Vamos mostrar, usando o princípio de indução finita, que $V = \mathbb{N}_{\geq 1}$.

Começamos com a base, que consiste em mostrar que $1 \in V$. Como

$$S_1 = 7 \text{ e } \quad -1^2 + 8 \cdot 1 = 7,$$

temos que $S_1 = (-n^2 + 8n)|_{n=1}$, o que confirma a validade da base.

Para o passo de indução suporemos que $k \in V$, para algum inteiro $k \geq 1$. Em outras palavras, a *hipótese de indução* nos diz que

$$S_k = -k^2 + 8k.$$

Já o que queremos mostrar é que $k+1 \in V$; isto é, que

$$S_{k+1} = -(k+1)^2 + 8(k+1).$$

Contudo,

$$S_{k+1} = S_k + (9 - 2k).$$

Usando a hipótese de indução, isto fica igual a

$$S_{k+1} = -k^2 + 8k + (9 - 2(k+1)) = -k^2 - 2k - 1 + 8k + 8,$$

que pode ser reescrito na forma

$$S_{k+1} = -(k^2 + 2k + 1) + 8(k+1) = -(k+1)^2 + 8(k+1),$$

como queríamos mostrar. Portanto,

$$1 \in V \text{ e toda vez que } k \in V \text{ também temos que } k+1 \in V.$$

Logo, pelo P. I. F., $V = \mathbb{N}_{\geq 1}$.

2. Como

$$6N + 5 \equiv 5 \pmod 6,$$

temos que $6N+5$ tem que deixar resto 5 na divisão por 6, não importa qual seja o inteiro positivo N escolhido. Por outro lado, como $p_i \equiv 1 \pmod 6$, temos que

$$p_1 \cdots p_m \equiv 1^m \equiv 1 \pmod 6.$$

Portanto, se todo os fatores primos de $6N+5$ deixassem resto um na divisão por 6, então $6N+5$ também teria que ter resto um na divisão por 6. Como já sabemos que isto é falso, podemos concluir que $6N+5$ tem que ter algum fator primo que deixa resto 5 na divisão por 6. Acontece que, por hipótese, estamos supondo que

$$5, p_1, \ldots, p_m$$

são *todos* os primos que deixam resto 5 na divisão por 6. Logo, $6N+5$ teria que ser divisível por um destes primos. Mas isto não é possível porque

$$\text{mdc}(6N+5, N) = 1.$$

Como 5 não divide N, teremos que tratá-lo separadamente. Mas se 5 dividisse $6N+5$, então dividiria $6N$, o que não é possível pela definição de N. Obtemos, assim, uma contradição e a demonstração está completa.

3. (a) Para fazer (a) precisamos usar o *lema chave*:

se $a^r \equiv 1 \pmod n$, então a ordem de a módulo n tem que dividir r.

Como sabemos que 3 tem ordem 126 módulo 127, podemos concluir que

$$3^{126} \equiv 1 \pmod{127}, \text{ e que } 3^m \not\equiv 1 \pmod{127},$$

qualquer que seja $1 \leq m \leq 125$. Contudo, $126 = 2 \cdot 63$, de modo que

$$9^{63} \equiv 3^{2 \cdot 63} \equiv 1 \pmod{127}.$$

Pelo lema chave isto significa que a ordem de 9 módulo 127 divide 63. Por outro lado, se a ordem se 9 módulo 127 fosse $k < 63$, então

$$9^k \equiv 3^{2 \cdot k} \equiv 1 \pmod{127},$$

de modo que 3 teria ordem

$$2k < 2 \cdot 63 = 126,$$

módulo 3; o que é falso por hipótese. Logo, a ordem de 9 módulo 127 é realmente igual a 63. Um argumento análogo mostra que, como $126 = 3 \cdot 42$, então de

$$27^{42} \equiv 3^{3 \cdot 42} \equiv 1 \pmod{127}.$$

segue que 27 tem ordem 42 módulo 127.

Para fazer (b) basta dividir 250049 pela ordem de 9 que é 63, o que nos dá

$$250049 = 63 \cdot 3969 + 2.$$

Assim,

$$9^{250049} \equiv (9^{63})^{3969} \cdot 9^2 \equiv 1 \cdot 81 \pmod{127}.$$

Logo, o resto desejado é 81.

DCC-UFRJ–Números inteiros e criptografia–Terceira Prova–2009/1

Nome: _____

Justifique cuidadosamente as suas respostas.

1. Seja $p > 2^{100}$ um número primo tal que $2p + 1$ também é primo. Use o teorema de Fermat para calcular a ordem de 9 módulo $2p + 1$.

   Sugestão: aplique Fermat à base 3.

2. Seja $p > 2^{100}$ um número primo tal que $2p+1$ também é primo. Prove que $3p(2p+1)$ não pode ser um número de Carmichael.

3. Seja $n = 13981 = 11 \cdot 31 \cdot 41$.

4. Seja $n = 13981 = 11 \cdot 31 \cdot 41$. Calcule o resto da divisão de 2^{3495} por n pelo algoritmo chinês do resto e use isto para determinar se n é pseudoprimo forte e/ou fraco para a base 2.

Resolução

1. Pelo teorema de Fermat,

$$3^{2p} \equiv 1 \pmod{2p+1},$$

pois $2p + 1$ é um primo maior que 3. Mas,

$$3^{2p} \equiv 9^p \pmod{2p+1}.$$

Portanto,

$$9^p \equiv 1 \pmod{2p+1},$$

Disto e do Lema Chave, temos que a ordem de 9 módulo $2p+1$ tem que dividir p. Como p é primo, 9 tem que ter ordem 1 ou p módulo $2p + 1$. Contudo, se a ordem fosse um teríamos

$$9 \equiv 1 \pmod{2p+1},$$

de modo que $2p+1$ teria que dividir 8, o que é obviamente falso. 9 tem ordem p módulo $2p + 1$.

2. Se $3p(2p + 1)$ fosse Carmichael, teríamos que

$$3p(2p+1) \equiv 9 \pmod{p-1}$$

pois

$$p \equiv 1 \pmod{p-1}.$$

Como $p > 2^{100}$ não é possível que isto ocorra. Portanto, $3p(2p+1)$ não pode ser um número de Carmichael.

3(a). Pelo teorema de Fermat

$$\begin{aligned} 2^{10} &\equiv \pmod{11} \\ 2^{30} &\equiv \pmod{31} \\ 2^{40} &\equiv \pmod{41} \end{aligned}$$

Como $n = 13981 = 11 \cdot 31 \cdot 41$, e

$$\begin{aligned} 3495 &\equiv 5 \pmod{10} \\ 3495 &\equiv 15 \pmod{30} \\ 3495 &\equiv 15 \pmod{40}. \end{aligned}$$

Portanto,

$$\begin{aligned} 2^{3495} &\equiv 2^5 \equiv -1 \equiv 10 \pmod{11} \\ 2^{3495} &\equiv 2^{15} \equiv (2^5)^3 \equiv 1 \pmod{31} \\ 2^{3495} &\equiv 2^{15} \equiv (2^5)^3 \equiv (-9)^3 \equiv 9 \pmod{41}. \end{aligned}$$

Logo, se r for o resto de 2^{3495} por n teremos que

$$\begin{aligned} r &\equiv 10 \pmod{11} \\ r &\equiv 1 \pmod{31} \\ r &\equiv 9 \pmod{41}. \end{aligned}$$

Resolvendo pelo algoritmo chinês do resto, tiramos o valor de r da última congruência,

$$r = 9 + 41t,$$

e substituímos na segunda,

$$9 + 41t \equiv 1 \pmod{31},$$

donde

$$10t \equiv -8 \pmod{31}.$$

Multiplicando por 3:

$$30t \equiv -24 \pmod{31};$$

donde

$$-t \equiv -24 \pmod{31};$$

que equivale a

$$t \equiv 24 \pmod{31}.$$

Assim,

$$t = 24 + 31y.$$

Substituindo em r,

$$r = 993 + 31 \cdot 41y.$$

Levando isto à primeira congruência, obtemos

$$993 + 31 \cdot 41y \equiv 10 \pmod{11};$$

isto é,

$$3 - 5y \equiv 10 \pmod{11}.$$

Assim,

$$6y \equiv 7 \pmod{11}.$$

Multiplicando tudo por 2;

$$y \equiv 3 \pmod{11}.$$

Logo,

$$y = 3 + 11z,$$

donde,

$$r = 4806 + nz.$$

Para aplicar o teste de composição forte, escrevemos $n - 1 = 2^2 \cdot 3495$. Como

$$2^{3495} \equiv 4806 \not\equiv 1, n - 1 \pmod{n},$$

e como

$$2^{2 \cdot 3495} \equiv (4806)^2 \equiv 1024 \not\equiv n - 1 \pmod{n},$$

concluímos que n não é pseudoprimo forte para a base 2. Por outro lado,

$$2^{n-1} \equiv 2^{4 \cdot 3495} \equiv (1204)^2 \equiv 1 \not\equiv n - 1 \pmod{n},$$

de modo que n é um pseudoprimo para a base 2.

1. Seja $p = 12539$ que é um número primo. Sabe-se que:

   - $3^{2p} \equiv 14050 \pmod{2p+1}$;
   - $3^{4p} \equiv 6561 \pmod{4p+1}$;
   - $3^{4p} \equiv 8p \pmod{8p+1}$;

   Use os dados acima para calcular *todos* os inteiros $x > 1$ para os quais

   $$\phi(x) = 8p.$$

2. Em seu primeiro contato com um planeta com que a Federação deseja estabelecer relações diplomáticas, os oficiais da *Enterprise* foram convidados para uma festa. Infelizmente o planeta foi conquistado por Nero que deseja capturar um dos membros da tripulação. A oficial de comunicações Uhura intercepta uma transmissão codificada do planeta que contém o nome do oficial a ser capturado. A mensagem é

   $$18786 - 22882$$

   com chave

   $$n = 59881 \quad \text{e} \quad e = 39595$$

   que Uhura identificou ter sido codificada utilizando um primitivo código conhecido na Terra do século XXI como RSA. Decodifique a mensagem e determine quem é o oficial que Nero deseja capturar.

3. Sabe-se que $p = 16 \cdot 1237 + 1$ é um número primo. Ache um elemento de ordem 32 em $U(p) \times U(16)$ ou prove que um tal elemento não pode existir.

Resolução

1. Usando que se p divide x, então $p-1$ divide $\phi(x) = n_6 - 1$, vamos listar todos os possíveis divisores pares de $n_6 - 1$, que são os únicos, além de um, que podem corresponder a primos, quando somamos uma unidade. A lista completa é dada abaixo: Para determinar que $2p+1$ e $4p+1$ são compostos usamos o teste fraco e as duas primeiras congruências dadas. Para determinar que $8p+1$ é primo usamos o teste de Lucas e as congruências:

$$\begin{aligned} 3^{8p} \equiv (3^{4p})^2 \equiv (8p)^2 \equiv (-1)^2 \equiv 1 \pmod{8p+1}; \\ 3^{4p} \equiv 8p \equiv -1 \not\equiv 1 \pmod{8p+1}; \\ 3^8 \equiv 6561 \pmod{8p+1}; \end{aligned}$$

fator	fator mais um	status
1	2	primo
2	3	primo
4	5	primo
3	8	composto
$2p$	$2p+1$	composto
$4p$	$4p+1$	composto
$8p$	$8p+1$	primo

em que a última congruência vem de $3^8 = 6561 < 8 * p + 1$. Disto vemos que as possíveis fatorações de x são todas da forma

$$x = 2^{e_1}3^{e_2}5^{e_3}(8p+1)^{e_4},$$

para alguma escolha dos expoentes e_1, e_2, e_3, e_4. Se $e_4 > 0$, temos

$$\phi(x) = \phi(2^{e_1}3^{e_2}5^{e_3})\phi((8p+1)^{e_4});$$

que nos dá

$$\phi(x) = \phi(2^{e_1}3^{e_2}5^{e_3})(8p+1)^{e_4-1}8p.$$

Para que isto seja igual a $8p$ devemos ter que $e_4 = 1$ e que

$$\phi(2^{e_1}3^{e_2}5^{e_3}) = 1$$

que só pode ocorrer se $e_1 = 0$ ou $e_1 = 1$ e $e_2 = e_3 = 0$. Temos, neste caso, duas respostas possíveis:

$$x = 8p+1 \quad \text{ou} \quad x = 2(8p+1).$$

Supondo, agora, que $e_4 = 0$, obtemos

$$\phi(x) = \phi(2^{e_1}3^{e_2}5^{e_3}) = 8p.$$

Como p é um primo maior que 5, não há como obtê-lo a partir de $\phi(2^{e_1}3^{e_2}5^{e_3})$, de modo que as únicas soluções possíveis são as que já encontramos.

2. Aplicando o algoritmo de Fermat a $n = 59881$ obtemos os fatores $p = 233$ e $q = 257$. Logo,

$$\phi(n) = (p-1)(q-1) = 59392.$$

Invertendo $e = 39595$ módulo $\phi(n)$ pelo algoritmo euclidiano estendido, descobrimos que $d = 3$. Decodificando temos que

$$18786^3 \equiv 2518 \pmod{11569}$$
$$22882^3 \equiv 2014 \pmod{11569}$$

de modo que o oficial ameaçado foi o capitão PIKE.

3. Se

$$(\overline{a}, \overline{b}) \in U(p) \times U(16),$$

e $k > 0$ é um inteiro, então

$$(\overline{a}, \overline{b})^k = (\overline{a}^k, \overline{b}^k).$$

Portanto, se $(\overline{a}, \overline{b})$ tiver ordem 32, então a ordem de $\overline{a}$, assim como a ordem de $\overline{b}$ têm que dividir 32. Mas

$$|U(p)| = \phi(p) = p - 1 = 2^4 \cdot 1237,$$

de modo que um elemento de $U(p)$ cuja ordem é uma potência de 2 não pode ter ordem maior que 16. Já a maior ordem possível em $U(16)$ é 8. Portanto, se as ordens de $\overline{a}$ e $\overline{b}$ forem potências de 2, então têm que ser ambas menores que 16; donde

$$(\overline{a}, \overline{b})^{16} = (\overline{a}^{16}, \overline{b}^{16}) = (\overline{1}, \overline{1}).$$

Prova Final–2009/1

Leia as instruções antes de prosseguir:

- justifique cuidadosamente todas as suas respostas;
- se está fazendo a final porque faltou a prova n, então resolva as questões $n.1$, $n.2$ e uma outra questão qualquer de sua escolha;
- se está fazendo esta prova como final, resolva as questões 1.1, 2.1, 3.1, 4.1 e duas outras de sua escolha.

1.1 Prove, por indução em n que

$$1^2 - 2^2 + 3^2 - 4^2 + \cdots + (-1)^{n-1} n^2 = \frac{(-1)^{n-1} n(n+1)}{2},$$

para todo $n \geq 1$. Indique claramente cada etapa da indução.

1.2 Fatore 60031 pelo algoritmo de Fermat.

2.1 Calcule a ordem de $\overline{3}$ sabendo-se que *não* é um gerador de $U(347)$.

2.2 Calcule, se existir, o inverso de 9875 módulo 54367.

3.1 Use o algoritmo chinês do resto para calcular o resto de 5^{195} na divisão por 781.

3.2 781 é um número de Carmichael? É um pseudoprimo forte para a base 5? É um pseudoprimo para a base 5?

4.1 Decodifique a mensagem 28362, que foi codificada com o RSA de chave pública $n = 30301$ e $e = 11981$.

4.2 Sabe-se que $p = 16 \cdot 1237 + 1$ é um número primo. Ache um elemento de ordem 32 em $U(2p) \times U(16)$ ou prove que um tal elemento não pode existir.

Primeira Prova–2009/2

1. Seja $q > 2^{910029}$ um inteiro positivo para o qual $(n+1)^q - n^q - 1$ é divisível por q qualquer que seja o valor $n \in \mathbb{N}$. Use isto para provar, por indução em n, que $n^q - n$ é divisível por q, para todo $n \in \mathbb{N}$.

2. Pierre costumava receber R$ 1301,00 de diárias por mês mas, depois de um aumento, passou a receber R$ 1801,00. Para fazer sua prestação de contas, ele precisa saber o número m de meses durante os quais recebeu a diária menor e o número n de meses durante os quais recebeu a maior. Infelizmente, Pierre perdeu seus comprovantes e, como é muito tímido, não quer procurar o setor de financeiro da empresa. A única outra coisa que Pierre sabe é que recebeu um total de R$ 19112,00 no período da prestação de contas.

   (a) Formule o problema como uma equação diofantina em m e n e ache sua solução geral.

   (b) Usando a solução geral, determine m e n, para que Pierre possa fazer sua prestação de contas.

3. Determine *todos* os inteiros $n > 0$ para os quais existem $x > 0$ e $y > 0$ que são soluções da equação $x^2 - n^2y^2 = 9$. Você deve provar que sua resposta está correta!

   Sugestão: produto notável.

Resolução

1. Seja

$$V = \{n \in \mathbb{N} \,|\, n^q - n \text{ é divisível por } q\}.$$

Provaremos por indução em n que $V = \mathbb{N}$ o que garante que a desigualdade vale para todo inteiro positivo.

Começamos pela base da indução, que corresponde a mostrar que $0 \in V$. Mas, tomando $n = 0$, verificamos que

$$0^q - 0 = 0;$$

que é divisível por q pois $0 = 0 \cdot q$. Portanto, $0 \in V$.

Passando, agora, ao passo de indução, precisamos provar que se $k \in V$ então $k+1 \in V$. Contudo, dizer que $k \in V$ equivale a dizer que

$$k^q - k \text{ é divisível por } q.$$

Contudo, foi dito que

$$(k+1)^q - k^q - 1 \text{ é divisível por } q.$$

Como a soma de dois múltiplos de q tem que ser múltiplo de q, temos que

$$((k+1)^q - k^q - 1) + (k^q - k) \text{ é divisível por } q;$$

de modo que

$$(k+1)^q - k - 1 \text{ é divisível por } q;$$

o que prova que $k+1 \in V$. Portanto, pelo *Princípio de Indução Finita*, $V = \mathbb{N} \setminus \{0\}$; isto é

$$n^q - n \text{ é divisível por } q;$$

para todo $n \geq 0$.

2. Aplicando o algoritmo euclidiano estendido a 1801 e 1301, obtemos a tabela

resto	quociente	x
1801	**	1
1301	**	0
500	1	1
301	2	- 2
199	1	3
102	1	- 5
97	1	8
5	1	-13
2	19	255
1	2	- 523
0	$\star$	$\star$

donde concluímos que,

$$\alpha = -523 \text{ e } \beta = \frac{1 - 523 \cdot 1801}{1301} = 724,$$

satisfazem

$$\alpha \cdot 1801 + \beta \cdot 1301 = 1.$$

A solução geral será, então,

$$x = -19112 \cdot 523 + 1301k \text{ e } y = 19112 \cdot 724 - 1801k.$$

Como m e n têm que ser inteiros positivos, precisamos que

$$-19112 \cdot 523 + 1301k > 0 \text{ e que } 19112 \cdot 724 - 1801k > 0;$$

donde obtemos as desigualdades

$$\frac{19112 \cdot 523}{1301} < k < \frac{19112 \cdot 724}{1801};$$

isto é,

$$7682,9946\cdots < k < 7683,002\ldots.$$

Portanto, $k = 7683$, e assim,

$$n = -19112 \cdot 523 + 1301 \cdot 7683 = 7$$
$$m = 19112 \cdot 724 - 1801 \cdot 7683 = 5.$$

Em outras palavras, Pierre ganhou 1801 reais de diária por 7 meses e 1301 reais por 5 meses.

3. Fatorando o lado esquerdo de $x^2 - n^2y^2 = 9$ temos que

$$(x - ny)(x + ny) = 9.$$

Como todos os números são inteiros, e levando em conta que $y > 0$, devemos ter

$$x - ny < x + ny,$$

há apenas duas possibilidades para $x + ny$ e $x - ny$, a saber:

$$x - ny = 1 \text{ e } \quad x + ny = 9;$$

ou então,

$$x - ny = -9 \text{ e } \quad x + ny = -1;$$

Resolvendo o primeiro sistema, encontramos

$$x = 5 \text{ e } \quad y = 4/n;$$

e, resolvendo o segundo,

$$x = -5 \text{ e } \quad y = 4/n.$$

Como, tanto x quando y devem ser inteiros, devemos ter que

$$n = 1, 2, \text{ ou } \quad 4.$$

Segunda Prova–2009/2

1. Prove, *por indução*, em n que

$$2^3 + 4^3 + \cdots + (2n)^3 = 2n^2(n+1)^2$$

para todo $n \geq 1$. Indique claramente cada etapa da indução.

2. Ache dois fatores de $n = 1908691$ pelo algoritmo de Fermat.

3. Sabe-se que 2 tem ordem 359 módulo $p = (2 \cdot 359) + 1 = 719$.
   (a) Calcule a ordem de -2 módulo p.
   (b) Calcule o resto da divisão de 717^{9694} por p.

Resolução

1. Seja

$$V = \{n \in \mathbb{N}_{\geq 1} \,|2^3 + 4^3 + \cdots + (2n)^3 = 2n^2(n+1)^2\}.$$

Queremos provar, por indução em n, que $V = \mathbb{N}_{\geq 1}$. Começamos com a base, que consiste em mostrar que $1 \in V$. Mas,

$$\sum_{i=1}^{1} (2i)^3 = 2^3 = 8,$$

ao passo que

$$2n^2(n+1)^2|vert_{n=1} = 2 \cdot 1 \cot 2^2 = 8,$$

o que comprova a igualdade desejada e confirma que $1 \in V$. Em seguida devemos provar o passo de indução, que consiste em supor que $k \in V$ e provar que $k+1 \in V$. Neste exemplo, devemos supor que

$$2^3 + 4^3 + \cdots + (2k)^3 = 2k^2(k+1)^2$$

que é a hipótese de indução e, a partir disto, mostrar que

$$2^3 + 4^3 + \cdots + (2(k+1))^3 = 2(k+1)^2(k+2)^2.$$

Mas,

$$2^3 + 4^3 + \cdots + (2(k+1))^3 = 2^3 + 4^3 + \cdots + (2k)^2 + (2(k+1))^3.$$

Usando a hipótese de indução concluímos que

$$2^3 + 4^3 + \cdots + (2(k+1))^3 = 2k^2(k+1)^2 + (2(k+1))^3.$$

Pondo $2(k+1)^2$ em evidência, obtemos

$$2^3 + 4^3 + \cdots + (2(k+1))^3 = 2(k+1)^2(k^2 + 4(k+1)).$$

Contudo,

$$k^2 + 4(k+1) = (k+2)^2,$$

de modo que

$$2^3 + 4^3 + \cdots + (2(k+1))^3 = 2(k+1)^2(k+2)^2;$$

como queríamos mostrar. Portanto, pelo Princípio de Indução Finita, $V = \mathbb{N}_{geq1}$ e a igualdade vale para todo $n \geq 1$.

2. A tabela começa com $[\sqrt{1908691}] + 1 = 1382$ e tem nove linhas, a última das quais nos dá

$$x = 1390 \text{ e } \quad y = 153,$$

donde

$$x + y = 1543 \text{ e } \quad x - y = 1237.$$

3. De

$$2^{359} \equiv 1 \pmod{p},$$

obtemos

$$(-2)^{2\cdot 359} \equiv 1 \pmod{p}.$$

Logo, pelo Lema Chave, a ordem de -2 divide $2 \cdot 359$. Como $[\sqrt{359}] = 18$, é fácil verificar que 359 é primo. Logo, -2 tem ordem 1, 2, 359 ou $2 \cdot 359$. Contudo,

$$(-2)^1 \equiv -2 \not\equiv 1 \pmod{p}$$
$$(-2)^2 \equiv 4 \not\equiv 1 \pmod{p}$$
$$(-2)^{359} \equiv -1 \not\equiv 1 \pmod{p}$$

de modo que a ordem de -2 módulo p só pode mesmo ser $2 \cdot 359$. Passando a letra (b), temos que

$$717 \equiv -2 \pmod{p}.$$

Portanto,

$$717^{9694} \equiv (-2)^{9694} \equiv 2^{9694} \pmod{p};$$

já que 9694 é par. Como 2 tem ordem 359 módulo p, segue de $9694 \equiv 1 \pmod{359}$ que

$$717^{9694} \equiv 2^{9694} \equiv 2^1 \equiv 2 \pmod{p}.$$

Concluímos, portanto, que 717^{9694} deixa resto 2 na divisão por p.

DCC-UFRJ–Números inteiros e criptografia–Terceira Prova–2009/2

Nome: _____

Justifique cuidadosamente as suas respostas.

1. Considere a propriedade:

   se um inteiro x satisfaz $x^2 \equiv 1 \pmod{3^n}$ então $x \equiv \pm 1 \pmod{3^n}$.

   Prove, por indução em n, que esta propriedade vale para todo $n \geq 1$.

   Sugestão: para o passo de indução use que se $x^2 \equiv 1 \pmod{3^{k+1}}$, então $x^2 \equiv 1 \pmod{3^k}$. Explique porque isto é verdade.

2. Calcule:

   (a) o resto da divisão de 6^{15} por 481 pelo algoritmo chinês do resto;

   (b) o resto da divisão de 6^{30} por 481;

   (c) a ordem de 6 módulo 481.

3. Determine se 481 é:

   (a) número de Carmichael;

   (b) pseudoprimo forte para a base 6;

   (c) pseudoprimo para a base 6.

Resolução

1. Considere

$$V = \{n \,|\, \text{se } x^2 \equiv 1 \pmod{3^n} \text{ então } x \equiv \pm 1 \pmod{3^n}\}.$$

Queremos provar por indução que $V = \mathbb{N}_{\geq 1}$. Para estabelecer a base basta verificar que as únicas soluções de $x^2 \equiv 1 \pmod 3$ são congruentes a 1 e 2 módulo 3. Mas neste caso isto é óbvio porque o único outro resíduo possível módulo 3 é zero e é claro que $x \equiv 0 \pmod 3$ não satisfaz $x^2 \equiv 1 \pmod{3^n}$.

Passando ao passo de indução, digamos que, para um dado $k \geq 1$ as únicas soluções de $x^2 \equiv 1 \pmod{3^k}$ sejam congruentes a ± 1 módulo 3^k. Digamos que $x^2 \equiv 1 \pmod{3^{k+1}}$. Mas esta congruência implica que $x^2 \equiv 1 \pmod{3^k}$. Assim, pela hipótese de indução

$x \equiv \pm 1 \pmod{3^k}$. Mas isto significa que $x = \pm 1 + c3^k$ para algum inteiro c. Substituindo na congruência original,

$$(\pm 1 + c3^k)^2 \equiv x^2 \equiv 1 \pmod{3^{k+1}};$$

que nos dá,

$$1 + 2c3^k + (c3^k)^2 \equiv 1 \pmod{3^{k+1}}.$$

Como $2k \geq k + 1$ para todo $k \geq 1$, a terceira parcela do lado esquerdo é congruente a zero módulo 3^{k+1} e resta apenas

$$1 + 2c3^k \equiv 1 \pmod{3^{k+1}};$$

donde

$$2c3^k \equiv 0 \pmod{3^{k+1}}.$$

Em outras palavras, 3^{k+1} divide $2c3^k$. Logo, 3 tem que dividir c. Escrevendo, $c = 3c'$, temos que

$$x = \pm 1 + c3^k = \pm 1 + c'3^{k+1}.$$

Mas isto implica que $x \equiv \pm 1 \pmod{3^{k+1}}$, concluindo assim a demonstração do passo de indução. Logo, pelo princípio de indução finita, $V = \mathbb{N}_{\geq 1}$, como devíamos mostrar.

2. Fatorando $481 = 13 \cdot 37$. Portanto, se r é o resíduo de 6^{15} módulo 481, então,

$$\begin{aligned} r &\equiv 6^{15} \pmod{13} \\ r &\equiv 6^{15} \pmod{37}. \end{aligned}$$

Aplicando o Teorema de Fermat ao primo 13, verificamos que $6^{12} \equiv 1 \pmod{13}$, donde,

$$6^{15} \equiv 6^3 \cdot 6^{12} \equiv 6^3 \cdot 1 \equiv 8 \pmod{13}.$$

Não adianta aplicar Fermat ao primo 37, porque $15 < 36$. Por isso teremos que proceder diretamente. Contudo, $6^2 \equiv -1 \pmod{37}$, de modo que

$$6^{15} \equiv (6^2)^7 \cdot 6 \equiv -6 \equiv 31 \pmod{37}.$$

Reunindo tudo isto temos que

$$\begin{aligned} r &\equiv 8 \pmod{13} \\ r &\equiv 31 \pmod{37}. \end{aligned}$$

Para aplicar o algoritmo chinês do resto, explicitamos r da segunda congruência, o que nos dá

$$r = 31 + 37y,$$

e substituímos na primeira congruência, obtendo

$$r \equiv 31 + 37y \equiv 8 \pmod{13}.$$

Simplificando

$$11y \equiv -10 \pmod{13};$$

isto é,

$$-2y \equiv -10 \pmod{13};$$

e como 2 é inversível módulo 13,

$$y \equiv 5 \pmod{13}.$$

Logo, $y = 5 + 13k$, donde

$$r = 31 + 37y = 31 + 37(5 + 13k) = 216 + 481k.$$

Portanto, o resto desejado é 216.

Passando a (b), já sabemos que

$$6^{15} \equiv 216 \pmod{481}.$$

Elevando ao quadrado,

$$6^{30} \equiv 216^2 \equiv 480 \equiv -1 \pmod{481};$$

donde

$$6^{60} \equiv (-1)^2 \equiv 1 \pmod{481}.$$

Portanto, pelo lema chave, a ordem de 6 módulo 481 tem que dividir 60. Mas já vimos que a ordem não pode ser 15 nem 30. Com isto as únicas possibilidades que restam são 1, 2 e 4. Contudo, 6^1 e 6^2 são menores que 481, de modo que não podem ser congruentes a 1, ao passo que

$$6^4 \equiv 1296 \equiv 334 \pmod{481}.$$

Concluímos que a ordem de 6 módulo 481 é realmente 60.

3. Para resolver esta questão não há necessidade de fazer nenhuma conta adicional, podemos aproveitar o que já foi feito na questão anterior:

(a) 481 não pode ser número de Carmichael porque estes números não podem ter menos de três fatores primos;

(b) $481 - 1 = 480 = 2^5 \cdot 15$ e como $6^{30} \equiv 480 \pmod{481}$, concluímos que 481 terá saída inconclusivo no teste forte, de modo que é pseudoprimo forte para a base 6;

(c) como 481 é pseudoprimo forte para a base 6, então tem que ser pseudoprimo para a mesma base.

Quarta Prova–2009/2

1. Sejam p e q primos distintos.

   (a) Determine a maior ordem possível para um elemento de $U(p) \times U(q)$.

   (b) Use (a) para provar que $U(p) \times U(q)$ não pode ser um grupo cíclico.

   (c) Use (b) para provar que $U(pq)$ não pode ser um grupo cíclico.

   Justifique cuidadosamente suas explicações.

2. Considere a chave pública de RSA $n = 7171$ e $e = 4667$. Quebre este código usando o algoritmo de fatoração de Fermat e decodifique a mensagem 2196–3791.

3. Sabe-se que $p = 1109$ é um número primo e que

$$5^p \equiv 1552 \pmod{14p+1} \text{ e } 5^{2p} \equiv 2019 \pmod{14p+1}.$$

   Use isto para provar que $14p + 1$ é um número primo.

Resolução

1.(a) Seja $(\overline{a}, \overline{b}) \in U(p) \times U(q)$. Como

$$\overline{a}^{p-1} = \overline{1} \text{ em } U(p) \text{ e } \overline{b}^{q-1} = \overline{1} \text{ em } U(q),$$

então, escrevendo $m = \text{mmc}(p-1, q-1)$, temos

$$m = (p-1)k \text{ e } m = (q-1)\ell$$

de modo que,

$$(\overline{a}, \overline{b})^m = (\overline{a}^m, \overline{b}^m) = ((\overline{a}^{p-1})^k, (\overline{b}^{q-1})^\ell) = (\overline{1}, \overline{1}).$$

Portanto, pelo lema chave, a ordem de $(\overline{a}, \overline{b})$ não pode exceder m. Além disso, se escolhermos $\overline{a}$ como sendo um gerador de $U(p)$ e $\overline{b}$ como sendo um gerador de $U(q)$, então a ordem de $(\overline{a}, \overline{b})$ tem que ser exatamente igual a m. Logo, a ordem máxima possível é m.

(b) Como a a ordem de $U(p) \times U(q)$ é

$$\phi(pq) = \phi(p)\phi(q) = (p-1)(q-1) > m,$$

pois $p-1$ e $q-1$ são ambos pares, então nenhum elemento de $U(p) \times U(q)$ pode ter ordem igual à ordem do grupo. Portanto, este grupo não pode ser cíclico.

(c) Como p e q são primos entre si

$$U(p) \times U(q) \cong U(pq)$$

de modo que $U(pq)$ só poderia ser cíclico se $U(p) \times U(q)$ também fosse, que não é o caso.

2. Pelo algoritmo de fatoração de Fermat temos que $n = 7171 = 71 \cdot 101$. Daí $\phi(n) = 7000$ e, pelo algoritmo euclidiano estendido, o inverso de $e = 4667$ módulo 7000 é $d = 3$. Portanto, ao decodificar a mensagem, obtemos

$$\begin{aligned} 2196^3 &\equiv 301 \pmod{n} \\ 3791^3 &\equiv 510 \pmod{n}; \end{aligned}$$

que nos dá 301510 = UFA.

3. Seja $q = 14p + 1$. Fatorando $q - 1$, obtemos

$$q - 1 = 2 \cdot 7 \cdot p.$$

Portanto, para aplicar o teste de Lucas na base b devemos calcular

$$5^{14p},\ 5^{2p},\ 5^{7p} \text{ e } 5^{14} \text{ módulo } q = 14p + 1.$$

Levando em consideração os dados do problema, escolheremos $b = 5$. Com isto, já temos

$$5^{2p} \equiv 2019 \pmod{14p + 1},$$

que não é congruente a um módulo q, assim como

$$5^{14} \equiv 7195 \not\equiv 1 \pmod{q},$$

por um cálculo direto. Por outro lado,

$$5^{7p} = (5^{2p})^3 \cdot 5^p,$$

de modo que

$$5^{7p} \equiv (5^{2p})^3 \cdot 5^p \equiv 2019^3 \cdot 1552 \equiv 8874 \cdot 1552 \equiv 15526 \not\equiv 1 \pmod{q}$$

e, portanto,

$$5^{14p} \equiv (5^{7p})^2 \equiv 15526^2 \equiv 1 \pmod{q}.$$

Resumindo, temos que

$$\begin{aligned} 5^{q-1} &\equiv 5^{14p} \equiv 1 \pmod{q} \\ 5^{(q-1)/p} &\equiv 7195 \not\equiv 1 \pmod{q} \\ 5^{(q-1)/2} &\equiv 15526 \not\equiv 1 \pmod{q} \\ 5^{(q-1)/7} &\equiv 2019 \not\equiv 1 \pmod{q}; \end{aligned}$$

que, pelo teste de Lucas, garante que $14p + 1$ é primo.

Primeira Prova–2010/1

1. Sejam a e b números inteiros positivos. Prove que o seguinte algoritmo recursivo para calcular o máximo divisor comum de a e b funciona corretamente:

$$\texttt{mdc(a, b)} == \texttt{ se a} = \texttt{b então a, senão } \begin{cases} \texttt{mdc(b, a} - \texttt{b)} & \text{se } \texttt{a} > \texttt{b} \\ \texttt{mdc(a, b} - \texttt{a)} & \text{se } \texttt{a} < \texttt{b}. \end{cases}$$

   Sugestão: prove primeiramente que se $a > b$, então $\mathrm{mdc}(a - b, b) = \mathrm{mdc}(a, b)$, e não esqueça de explicar porque o algoritmo tem que parar.

2. Determine *infinitos* valores *inteiros* de x e y para os quais a equação

$$123467x + 17687y = 7$$

   é satisfeita.

3. O caixa automático de um banco só contém notas de 2 e de 5 reais. Prove, *por indução em* n, que para qualquer $n \geq 4$,

   > um cliente deste banco é capaz de sacar deste caixa automático qualquer valor de n reais, recebendo *no máximo* uma nota de 5 reais.

   Explique cada passo do processo de indução com cuidado.

Resolução

1. Devemos provar primeiramente que

$$\mathrm{mdc}(a, b) = \mathrm{mdc}(a - b, b).$$

Mas, segundo o resultado auxiliar usado para provar que o algoritmo euclidiano funciona, se

$$\alpha = \beta\gamma + \delta,$$

então

$$\mathrm{mdc}(\alpha, \beta) = \mathrm{mdc}(\beta, \gamma).$$

Como

$$a = b + (a - b),$$

podemos aplicar o resultado auxiliar com

$$\alpha = a,\ \beta = b, \gamma = 1 \text{ e } \delta = a - b$$

e concluir diretamente a igualdade desejada.

Se pusermos o algoritmo para rodar, a cada etapa a regra recursiva é aplicada a um par (a, b), criando assim um novo par que será $(b, a-b)$ ou $(a, b-a)$ dependendo se $a > b$ ou $b > a$. Começaremos analisando o que acontece em uma tal etapa. Para simplificar, digamos que $a > b$; o outro caso é análogo. Neste caso temos que

$$\text{mdc}(a, b) = \text{mdc}(b, a - b)$$

pela igualdade provada anteriormente. Além disso,

$$b > a - b$$

Assim,

- os pares de inteiros antes e depois de um passo recursivo têm o mesmo máximo divisor comum;
- o menor dos inteiros do par de entrada é sempre *estritamente maior* que menor dos inteiros do par de saída.

Portanto,

1. o máximo divisor comum de um par obtido em qualquer momento da aplicação do algoritmo é sempre igual ao máximo divisor comum do par inicial;
2. o menor dos inteiros dos vários pares calculados nos passos recursivos formam uma sequência estritamente decrescente de inteiros não negativos.

De (2) concluímos que o algoritmo não pode processar para sempre, porque entre dois inteiros dados (neste caso a ou b e 0) existe uma quantidade finita de inteiros. Em outras palavras o algoritmo *tem* que parar. Como o máximo divisor comum de qualquer par é sempre o mesmo, teremos que se o par inicial for (a, b), então $\text{mdc}(a, b)$ é igual ao máximo divisor comum do par final. Como o algoritmo só para quando o par final é da forma (c, c) para algum inteiro positivo c, devemos ter que $\text{mdc}(a, b) = \text{mdc}(c, c)$, que é evidentemente igual a c. Isto prova que o algoritmo para e que funciona corretamente.

2. Aplicando o algoritmo euclidiano estendido, obtemos

resto	quociente	x
123467	**	1
17687	**	0
17345	6	1
342	1	- 1
245	50	51
97	1	- 52
51	2	155
46	1	- 207
5	1	362
1	9	- 3465
0	**	**

Portanto, o máximo divisor comum desejado é 1, $x = -3465$ e

$$y = \frac{1 - x123467}{17687} = 24188.$$

Portanto, a solução desejada é

$$x = 7 \cdot (-3465) + k \cdot 17687 \text{ e } \quad y = 7 \cdot 24188 - k \cdot 123467,$$

qualquer que seja $k \in \mathbb{Z}$.

3. O conjunto verdade é

$$V = \{n \in \mathbb{N} \,|\, n = 2x + 5y \text{ com } \quad x \in \mathbb{N} \text{ e } \quad y = 0 \text{ ou } \quad 1\}.$$

Começamos provando a base, que corresponde a $n = 4$. Mas $4 = 2 \cdot 2 + 0 \cdot 5$, de modo que a máquina deve dar duas notas de dois reais e nenhuma de cinco reais.

Passando ao passo de indução, digamos que $k \in V$; isto é que

$$k = 2x + 5y \text{ em que } x \in \mathbb{N} \text{ e } y = 0 \text{ ou } 1.$$

Queremos mostrar que $k + 1 \in V$; isto é, que existem inteiros não negativos x' e y' tais que $k + 1 = 2x' + 5y'$ em que $y' = 0$ ou 1. Há dois casos a considerar. No primeiro caso, $y = 1$. Se isto acontecer, então

$$k = 2x + 5 \text{ donde } \quad k + 1 = 2x + 6 = 2(x + 3)$$

é da forma desejada; isto é, a máquina dará $x + 3$ notas de 2 reais para chegar a $k + 1$. Por outro lado, se $y = 0$, então

$$k = 2x \text{ donde } \quad k + 1 = 2x + 1 = 2(x - 2) + 5;$$

o que é possível pois $k \geq 4$ implique que $x \geq 2$, donde $x - 2 \geq 0$. Portanto, como desejávamos mostras, $k \in V$ implica que $k + 1 \in V$. O *princípio de indução finita* nos permite então concluir que $V = \mathbb{N}_{\geq 4}$. Em outras palavras, a máquina descrita na questào pode mesmo pagar qualquer quantia maior ou igual a 4 da maneira desejada.

Segunda Prova–2010/1

1. Prove, por indução em n, que

$$2^{4n+3} \geq 8(n+1), \text{ para todo } n \in \mathbb{N}.$$

   Explique cada passo do processo de indução com cuidado.

2. Ache dois fatores de $n = 93433$ pelo algoritmo de Fermat.

3. Seja $n = 13 \cdot 73$. Calcule:

   (a) a ordem de 3 módulo 13 e a ordem de 3 módulo 73;

   (b) o resto da divisão de 3^{n-1} por 13, o resto da divisão de 3^{n-1} por 73 e o resto da divisão de 3^{n-1} por n.

   Usando isto, determine se n é ou não um pseudoprimo para a base 3.

4. Seja $p > 2$ um número primo e q um fator de $2^p - 1$. Mostre o que se pede:

   (a) $2^p \equiv 1 \pmod{q}$;

   (b) 2 tem ordem p módulo q;

   (c) p divide $q - 1$;

   (d) $2p$ divide $q - 1$.

Sugestão para (c): teorema de Fermat.

Resolução

1. Considere

$$V = \{n \in \mathbb{N} \mid 2^{4n+3} \geq 8(n+1)\}.$$

Queremos provar por indução que $V = \mathbb{N}$. Para verificar a base calculamos

$$2^{4n+3}|_{n=0} = 2^3 = 8 \text{ e } 8(n+1)|_{n=0} = 8$$

de modo que a desigualdade é verdadeira neste caso. Portanto, $0 \in V$. Para efetuar o passo de indução, estabelecemos a hipótese de indução, segundo a qual $k \in V$; isto é,

$$2^{4k+3} \geq 8(k+1)$$

e queremos mostrar que $k+1 \in V$; isto é, que

$$2^{4(k+1)+3} \geq 8((k+1)+1) = 8(k+2)$$

Para isto, observamos que

$$2^{4(k+1)+3} = 2^{4k+7} = 2^{4k+3}2^4$$

de forma que, pela hipótese de indução,

$$2^{4(k+1)+3} = 2^{4k+3} \cdot 2^4 \geq 8(k+1) \cdot 16.$$

Contudo,

$$8(k+1) \cdot 16 = 16 \cdot 8k + 16 \cdot 8 > 8k + 16 = 8(k+2)$$

pois $16 < 16 \cdot 8$. Combinando as desigualdades anteriores,

$$2^{4(k+1)+3} \geq 8(k+1) \cdot 16 > 8(k+2),$$

donde segue a desigualdade desejada. Logo, $k+1 \in V$. O *princípio de indução finita* nos permite então concluir que $V = \mathbb{N}$. Em outras palavras, a desigualdade $2^{4n+3} \geq 8(n+1)$ vale para qualquer inteiro não-negativo.

2. O menor valor de x na tabela do algoritmo de Fermat é 306 e o primeiro para o qual $\sqrt{x^2 - n}$ é inteiro é 317, que corresponde a $\sqrt{317^2 - n} = 84$. Portanto, os fatores são 233 e 401.

3. (a) Como 13 e 73 são primos segue do teorema de Fermat que ordem de 3 módulo 13 tem que dividir 12 e que a ordem de 3 módulo 73 tem que dividir 72. Mas,

$$\begin{aligned} 3^2 &\equiv 9 \pmod{13} \\ 3^3 &\equiv 1 \pmod{13} \end{aligned}$$

logo 3 tem ordem 3 módulo 13. Por outro lado,

$$\begin{aligned} 3^2 &\equiv 9 \pmod{73} \\ 3^3 &\equiv 27 \pmod{73} \\ 3^4 &\equiv 8 \pmod{73} \\ 3^6 &\equiv 9 \cdot 8 \equiv 72 \equiv -1 \pmod{73}. \end{aligned}$$

Logo,

$$3^{12} \equiv (-1)^2 \equiv 1 \pmod{73}.$$

Portanto, a ordem de 3 divide 12. Como 3 não pode ordem 1, 2, 3, 4 ou 6 pelos cálculos anteriores, então 3 tem ordem 12 módulo 73.

(b) Como $n - 1 = 2^2 \cdot 3 \cdot 79$ temos que

$$\begin{aligned} 3^{n-1} &\equiv (3^3)^{2^2 \cdot 79} \equiv 1 \pmod{13} \\ 3^{n-1} &\equiv (3^{12})^{79} \equiv 1 \pmod{73}. \end{aligned}$$

Logo, $3^{n-1} - 1$ é divisível por 13 e por 73. Como $\text{mdc}(13, 73) = 1$, então $3^{n-1} - 1$ é divisível pelo produto de 13 por 73; isto é

$$3^{n-1} \equiv 1 \pmod{n}.$$

É pseudoprimo, porque é ímpar, composto e satisfaz a congruência anterior.

4. (a) Segue direto da definição de congruência pois q divide $2^p - 1$.

(b) Como $2^p \equiv 1 \pmod{q}$ o lema chave nos diz que a ordem de 2 módulo q tem que dividir p. Mas p é primo e $2^1 \equiv 1 \pmod{q}$ implicaria que q divide $2 - 1 = 1$, o que não é possível. Portanto, a ordem de 2 módulo q tem que ser p.

(c) e (d) Pelo teorema de Fermat, $2^{q-1} \equiv 1 \pmod{q}$. Logo, usando novamente o lema chave, temos que p divide $q - 1$. Por outro lado, como q é fator do número ímpar $2^p - 1$, o próprio q tem que se ímpar. Portanto, $q - 1$ tem que ser par. Como p é ímpar por hipótese, segue que $\text{mdc}(2, p) = 1$. Portanto, como 2 e p dividem $q - 1$, podemos concluir que $2p$ divide $q - 1$.

Terceira Prova–2010/1

1. Calcule 7^{51} módulo 817 usando o algoritmo chinês do resto e responda às seguintes perguntas:

   (a) 817 é pseudoprimo forte para a base 7?

   (b) 817 é pseudoprimo para a base 7?

   (c) 817 é número de Carmichael para a base 7?

2. Sejam m e n dois inteiros maiores que 2^{87654}. Mostre que o grupo $U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$ contém um subgrupo não cíclico de ordem 4.

3. A mensagem

   $$4324 - 40$$

   contém o nome de um dos primeiros computadores programáveis, projetado por Alan Turing e construído no National Physical Laboratory da Inglaterra na década de 1950. Esta mensagem foi codificada usando o RSA com chave pública

   $$n = 13261 \text{ e } \quad e = 9303.$$

   Quebre este código e decodifique a mensagem.

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

4. Sabe-se que $q = 1693$ e $p = 6q + 1$ são ambos primos. Ache um gerador de $U(\mathbb{Z}_p)$ sabendo-se que em $\mathbb{Z}_p$,

   $$\overline{6}^q = \overline{5566}.$$

Resolução

1. Fatorando $n = 817$, verificamos que é igual a $19 \cdot 43$. Portanto, devemos calcular

$$\begin{aligned} r &\equiv 7^{51} \pmod{19} \\ r &\equiv 7^{51} \pmod{43}. \end{aligned}$$

Aplicando o teorema de Fermat aos primos 19 e 43, obtemos

$$\begin{aligned} 7^{51} &\equiv 7^{15} \pmod{19} \\ 7^{51} &\equiv 7^{9} \pmod{43}; \end{aligned}$$

Como 7 tem ordem 3 módulo 19 e $7^3 \equiv 42 \pmod{43}$, obtemos

$$\begin{aligned} 7^{51} &\equiv 1 \pmod{19} \\ 7^{51} &\equiv 42 \pmod{43}; \end{aligned}$$

donde

$$\begin{aligned} r &\equiv 1 \pmod{19} \\ r &\equiv 42 \pmod{43}. \end{aligned}$$

Para aplicar o algoritmo chinês, tomamos

$$r = 42 + 43t$$

da segunda congruência e substituímos na primeira, obtendo:

$$42 + 43t \equiv 1 \pmod{19};$$

de modo que

$$5t \equiv 16 \pmod{19}.$$

Como 5 tem inverso 4 módulo 19, resta

$$t \equiv 4 \cdot 16 \equiv 7 \pmod{19};$$

isto é,

$$t = 7 + 19k.$$

Assim,

$$r = 42 + 43(7 + 19k) = 343 + 817k.$$

Logo, 7^{51} deixa resto 343 quando dividido por 817.

Para poder aplicar o *teste forte de composição*, fatoramos a maior potência de 2 de $n - 1 = 816$, obtendo

$$816 = 2^4 \cdot 51.$$

Em seguida calculamos a sequência

$$\begin{aligned} r_0 &\equiv 7^{51} \equiv 343 \not\equiv 1, 816 \pmod{817} \\ r_1 &\equiv r_0^2 \equiv 1 \not\equiv 816 \pmod{817}; \\ r_2 &\equiv r_1^2 \equiv 1 \not\equiv 816 \pmod{817}; \\ r_3 &\equiv r_2^2 \equiv 1 \not\equiv 816 \pmod{817}; \end{aligned}$$

de modo que 817 produz saída composto no teste forte. Portanto, 817 não é um pseudoprimo forte para a base 7. Por sua vez

$$7^{816} \equiv r_3^2 \equiv 1 \pmod{817}$$

implica que 817 é pseudoprimo para a base 7. Finalmente, este número não pode ser de Carmichael porque tem apenas dois fatores, ao passo que números de Carmichael não podem ter menos de três fatores.

2. Basta tomar o subgrupo formado pelos elementos

$$(\overline{1}, \overline{1}),\ (\overline{m-1}, \overline{1}),\ (\overline{1}, \overline{m-1}),\ (\overline{n-1}, \overline{m-1}).$$

Cada um destes elementos tem ordem dois, de modo que este subgrupo não pode ser cíclico.

3. Em quatro etapas o algoritmo de Fermat nos dá

$$n = 89 \cdot 149,$$

de modo que

$$\phi(n) = 88 \cdot 148 = 13024,$$

e, o algoritmo euclidiano estendido nos dá $d = 7$. Com isto podemos decodificar a mensagem, obtendo

$$\begin{aligned} 4324^7 &\equiv 101 \pmod{n} \\ 40^7 &\equiv 214 \pmod{n}. \end{aligned}$$

Portanto, a mensagem é 101214; isto é, ACE.

4. Sabe-se que $q = 1693$ e $p = 6q + 1$ são ambos primos. Como foi dito que p é primo, então

$$\#U(\mathbb{Z}_p) = p - 1 = 6q$$

e, para ser gerador, um elemento deve ter esta ordem. Mas

$$\overline{6}^q = \overline{5566};$$

implica que

$$\overline{6}^{2q} = \overline{5566}^2 = \overline{5565};$$

e que

$$\overline{6}^{3q} = \overline{5566}^3 = \overline{10158};$$

ao passo que

$$\overline{6}^6 = \overline{6020}.$$

Mostramos, portanto, que

$$\begin{aligned} \overline{6}^{(p-1)/2} &= \overline{10158} \neq \overline{1}; \\ \overline{6}^{(p-1)/3} &= \overline{5565} \neq \overline{1}; \\ \overline{6}^{(p-1)/q} &= \overline{6020} \neq \overline{1}; \end{aligned}$$

mas, pelo argumento do teste de primalidade, isto significa que $\overline{6}$ não pode ter ordem menor que $p - 1$ em $U(\mathbb{Z}_p)$, de modo que tem que ser um gerador deste grupo.

Prova Final–2010/1

Leia as instruções atentamente antes de prosseguir:

- justifique cuidadosamente todas as suas respostas;
- se está fazendo a final porque faltou a prova 1, então resolva as questões 1.1, 1.2 e uma outra questão qualquer de sua escolha;
- se está fazendo a final porque faltou a prova n, com $n = 2$ ou 3, então resolva as questões $n.1$, $n.2$, $n.3$ e uma outra questão qualquer de sua escolha;
- se está fazendo esta prova como final, resolva as questões 1.1, 2.1, 3.1, 3.2 e duas outras de sua escolha.

1.1 Seja $x > 0$ um número real. Prove, *por indução em* n, que

$$(1 + x)^n > 1 + nx.$$

Explicite claramente cada passo da indução.

1.2 Resolva a congruência $4547x + 35 \equiv 15 \pmod{9001}$.

2.1 Calcule:

(a) a ordem de 2 módulo 19;

(b) a ordem de 2 módulo 43;

(c) a ordem de $(\overline{2}, \overline{2})$ em $U(\mathbb{Z}_{19}) \times U(\mathbb{Z}_{43})$;

(d) a ordem de 2 módulo 817.

2.2 O objetivo desta questão é dar uma outra demonstração de que existem infinitos números primos. Para isso, suponha que exista um número finito de primos, que são todos menores que um número inteiro positivo $n \geq 3$.

(a) Mostre que, *sob a hipótese acima*, terímaos que ter que $\text{mdc}(n! - 1, n!)$ é diferente de 1.

(b) Mostre que (a) leva a uma contradição, e use isto para provar que existem infinitos números primos.

2.2 Seja $n > 2^{987654}$ um inteiro e p um fator primo de

$$F(n) = 2^{2^n} + 1.$$

(a) calcule a ordem de 2 módulo p;

(b) use o teorema de Fermat para mostrar que 2^{n+1} divide $p-1$.

3.1 Seja $n = 7 \cdot 13 \cdot 31 \cdot 61$. Calcule 3^{10755} módulo n pelo algoritmo chinês do resto e responda às seguintes perguntas:

(a) n é pseudoprimo forte para a base 3?

(b) n é pseudoprimo para a base 3?

(c) n é número de Carmichael?

3.2 Sejam m e n dois inteiros maiores que 2^{87654}. Mostre que o grupo $U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$ contém um subgrupo não cíclico de ordem 4.

3.3 Decodifique a mensagem $20506 - 3498$ que foi codificada usando o RSA com chave pública $n = 21971$ e $e = 8669$.

T1 A sequência de Fibonacci F_n é definida por

$$F_0 = F_1 = 1 \text{ e } \quad F_n = F_{n-1} + F_{n-2}.$$

Calcule o quociente e o resto da divisão de F_m por F_{m-2}, quando m for um inteiro maior do que $2^{3452552!}$.

T2 Calcule uma infinidade de múltiplos dos números 2459485 e de 87401 cuja soma seja 7.

T3 Seja $a > 2^{3452552!}$ um número inteiro e considere a soma

$$S_n = \frac{1}{a(a+1)} + \frac{1}{(a+1)(a+2)} + \cdots + \frac{1}{(a+n-1)(a+n)}.$$

Prove, *por indução em* n, que a soma acima é sempre igual a $n/a(a+n)$. Você deve identificar claramente a base da indução, a hipótese de indução e a recursão que vai ser utilizada.

L1 Sejam $b < a$ dois inteiros positivos.

(a) Mostre, por indução em n que, qualquer que seja o inteiro $n \geq 1$ vale a igualdade

$$\text{resto}(b^n, a) = \text{resto}(\text{resto}(b^{n-1}, a) * b, a)$$

(b) Descreva, na linguagem do Axiom, um algoritmo recursivo cuja entrada é formada pelos números inteiros positivos a, b e n (você pode supor que $b < a$) e que usa a identidade acima para calcular o resto da divisão de b^n por a.

Solução

T1. A partir de

$$F_m = F_{m-1} + F_{m-2} \text{ e } F_{m-1} = F_{m-2} + F_{m-3}$$

podemos concluir que

$$F_m = 2F_{m-2} + F_{m-3}.$$

Por outro lado

$$F_{m-2} = F_{m-3} + F_{m-4} \geq F_{m-3} + 0 \geq F_{m-3}$$

nos permite concluir que $0 \leq F_{m-3} < F_{m-2}$. Portanto, pela unicidade do quociente e do resto da divisão temos que o quociente desejado é 2 e o resto é F_{m-3}.

T2. Aplicando o algoritmo euclidiano estendido, temos que

restos	quocientes	x
2459485	**	1
87401	**	0
12257	28	1
1602	7	- 7
1043	7	50
559	1	- 57
484	1	107
75	1	- 164
34	6	1091
7	2	- 2346
6	4	10475
1	1	- 12821
0	-	-

donde podemos concluir que

$$y = \frac{1 + 2459485 \cdot 12821}{87401} = 360786.$$

Logo, a soma dos múltiplos

$$-7 \cdot 2459485 \cdot 12821 \text{ e } 7 \cdot 360786 \cdot 87401,$$

é igual a 7. Para obter infinitos múltiplos, tomamos

$$(-7 \cdot 2459485 \cdot +87401 \cdot k)12821 \text{ e } (7 \cdot 360786 \cdot 12821 \cdot k)87401,$$

em que k pode ser qualquer número inteiro.

T3. Como

$$S_{n+1} = \underbrace{\frac{1}{a(a+1)} + \frac{1}{(a+1)(a+2)} + \cdots + \frac{1}{(a+n-1)(a+n)}}_{S_n} + \frac{1}{(a+n)(a+n+1)}$$

a recursão é

$$S_{n+1} = S_n + \frac{1}{(a+n)(a+n+1)}$$

Considere, então, a seguinte afirmação:
$A(n)$: a soma S_n é igual a $n/a(a+n)$.
Nosso objetivo é provar, por indução em n, que este resultado vale para todo $n \geq 1$.

Começamos pela base, que corresponde ao caso $n = 1$. Por um lado, temos que

$$S_1 = \frac{1}{a(a+1)}$$

que é igual à expressão obtida substituindo $n = 1$ na fórmula $n/a(a+n)$, comprovando, assim, a validade da base. Já o passo de indução tem como hipótese

a soma S_k é igual a $k/a(a+k)$,

a partir da qual queremos mostrar que

a soma S_{k+1} é igual a $(k+1)/a(a+k+1)$.

Contudo, pela recursão

$$S_{k+1} = S_k + \frac{1}{(a+k)(a+k+1)}.$$

Substituindo a hipótese de indução

$$S_{k+1} = \frac{k}{a(a+k)} + \frac{1}{(a+k)(a+k+1)},$$

donde

$$\begin{aligned} S_{k+1} &= \frac{1}{(a+k)}\left[\frac{k}{a} + \frac{1}{(a+k+1)}\right] \\ &= \frac{1}{(a+k)}\left[\frac{k(a+k+1)+a}{a(a+k+1)}\right] \\ &= \frac{1}{(a+k)}\left[\frac{(k+1)(a+k)}{a(a+k+1)}\right] \end{aligned}$$

que, após os devidos cancelamentos, nos dá

$$S_{k+1} = \frac{(k+1)}{a(a+k+1)},$$

como desejávamos mostrar. Tendo provado a base e o passo de indução, o princípio de indução finita nos permite concluir que a afirmação $A(n)$ vale para todo inteiro $n \geq 1$; isto é

$$S_n = \frac{n}{a(a+n)} \text{ para todo } \quad n \geq 1.$$

L1. (a) Desejamos provar por indução que

$$\text{resto}(b^n, a) = \text{resto}(\text{resto}(b^{n-1}, a) \cdot b, a)$$

vale para todo $n \geq 1$. A base é simples, uma vez que, para $n = 1$,

$$\text{resto}(b^{n-1}, a) = \text{resto}(b^0, a) = \text{resto}(1, a) = 1$$

donde

$$\text{resto}(\text{resto}(b^{n-1}, a) \cdot b, a) = \text{resto}(1 \cdot b, a) = \text{resto}(b, a)$$

que é igual ao lado esquerdo da afirmação desejada quando $n = 1$. Quanto ao passo de indução, temos que partir da hipótese

$$\text{resto}(b^{k-1}, a) = \text{resto}(\text{resto}(b^{k-2}, a) \cdot b, a)$$

e chegar à conclusão que

$$\text{resto}(b^k, a) = \text{resto}(\text{resto}(b^{k-1}, a) \cdot b, a).$$

Para isto, observe que se r é o resto e q o quociente da divisão de b^{k-1} por a, então

$$b^{k-1} = aq + r \text{ e } 0 \leq r < a.$$

Multiplicando esta expressão por b, obtemos

$$b^k = b \cdot b^{k-1} = baq + br.$$

Mas se

$$br = aq_1 + r_1 \text{ com } 0 \leq r_1 < a,$$

então

$$b^k = baq + br = baq + (aq_1 + r_1) = a(bq + q_1) + r_1.$$

Como $0 \leq r_1 < a$ isto nos permite concluir que r_1 é o resto da divisão de b^k por a. Mas,

$$r_1 = \text{resto}(br, a) = \text{resto}(b \cdot \text{resto}(b^{k-1}, a), a),$$

comprovando, assim, que o passo de indução funciona corretamente. Portantp, o resultado desejado segue do o princípio de indução finita.

(b) Para programar no AXIOM um algoritmo recursivo que calcula o resto de b^n por a a partir da recursão

$$\text{resto}(b^n, a) = \text{resto}(\text{resto}(b^{n-1}, a) * b, a)$$

basta escrever

```
pow(b,n,a) == if n = 0 then 1 else resto(pow(b,n-1,a)*b,a).
```

T1 Calcule os dois fatores do número 655009 usando o algoritmo de Fermat.

T2 Calcule todas as potências distintas de 25 módulo 45 e use-as para determinar:

(a) a ordem de 25 módulo 45;

(b) o resto da divisão de $25^{2^{9879}}$ por 45.

Cuidado para não interpretar esta potência de maneira incorreta. No Axiom ela seria escrita na forma `25^(2^(9879))`.

T3 Seja $n > 17^{3452552}$ um número inteiro que satisfaz $(n-1)! \equiv -1 \pmod{n}$.

(a) Determine uma fórmula que, para cada $1 \leq d \leq n-1$, dá o inverso de d módulo n em função do fatorial de $n-1$ e do próprio d.

(b) Use (a) para mostrar que n tem que ser um número primo.

Dica para (b): mostre que nenhum $1 \leq d \leq n-1$ pode ser fator de n.

L2 Descreva, na linguagem do Axiom, uma função `ordem(b,p)` que, tendo como entrada um número primo $p > 1$ e um número inteiro $1 \leq b \leq p-1$ retorna a ordem de b módulo p. Seu programa deve usar as seguintes funções do Axiom:

- `powmod(b,k,n)` que calcula o resto da divisão de b^k por n;
- `divisors(n)` que calcula a lista de todos os divisores de n.

A função não precisa verificar se p é primo nem se b está no intervalo correto. Dica: teorema de Fermat.

Solução

T.1 Como $\sqrt{n} = 809,32$, precisaremos calcular a tabela, que é

x	$\sqrt{x^2 - n}$
810	33.030
811	52.076
812	65.840
813	77.201
814	87.103
815	96.0

Portanto,

$$x = 815 \text{ e } \quad y = 96,$$

de modo que os fatores desejados são

$$x - y = 719 \text{ e } \quad x + y = 911.$$

T.2 Um cálculo fácil mostra que as únicas potências de 25 que são distintas módulo 45 são

$$\begin{aligned} 25^1 &\equiv 25 \pmod{45} \\ 25^2 &\equiv 40 \pmod{45} \\ 25^3 &\equiv 10 \pmod{45} \end{aligned}$$

Em particular, 25 não tem ordem módulo 45, o que aliás já sabíamos porque $\text{mdc}(25, 45) = 5 \neq 1$, de modo que que 25 não pode ser inversível módulo 45, o que implica que não tem ordem para este módulo. Por outro lado, as potências de 25 módulo 45 aparecem em ciclos de comprimento 3. Assim, para saber quando vale $25^{2^{9879}}$ módulo 45, basta saber qual o resto de 2^{9879} por 3. Contudo,

$$2^{9879} \equiv (-1)^{9879} \equiv -1 \equiv 2 \pmod{3}$$

de modo que

$$25^{2^{9879}} \equiv 25^2 \equiv 40 \pmod{45}.$$

Logo o resto desejado é 40.

T.3 A fórmula para o inverso de d é

$$-\texttt{quo}((n-1)!, d) = -\frac{(n-1)!}{d}.$$

De fato,

$$d \cdot (-\texttt{quo}((n-1)!, d)) \equiv -(n-1)! \equiv 1 \pmod{n}.$$

Mas isto significa que todo inteiro d entre 1 e $n-1$ tem inverso módulo n. Contudo, d tem inverso módulo n se, e somente se, $\text{mdc}(d, n) = 1$. Em particular, podemos concluir que nenhum inteiro entre 1 e $n-1$ divide n. Logo, n não tem fatores próprios e tem que ser primo.

L.2 Combinando o teorema de Fermat com o lema chave podemos concluir que a ordem de qualquer inteiro que não é congruente a zero módulo p divide $p-1$. Portanto, basta procurar pela ordem de b entre os divisores de $p-1$. Uma solução possível é dada abaixo:

```
ordem(b,p) ==
   D:List(INT):= divisors((p-1)::PI)
   k:PI:= 1
   r:PI:= b
   while r ~= 1 and k <= #D repeat
       r:= powmod(b,D.k,p)
        k:= k+1
   return(D.(k-1))
```

Outra solução, mais curta, tirada da prova de Guilherme da Costa Sales:

```
ordem(b,p) ==
   L:List(INT):= [k for k in divisors(p-1)  | powmod(b,k,p) = 1 ]
   return(L.1)
```

T7 Sabe-se que $3^{1323} \equiv 8422 \pmod{10585}$ e que $10585 = 5 \cdot 29 \cdot 73$. Determine se 10585 é

(a) número de Carmichael;

(b) pseudoprimo para a base 3;

(c) pseudoprimo forte para a base 3.

T8 Sabe-se que $n = 470857$ é o produto de dois números primos e que $\phi(n) = 469396$. Determine os fatores primos de n e use-os, juntamente com o algoritmo chinês do resto, para decodificar a mensagem 225265, encriptada com o RSA de chave pública $(470857, 312931)$. A correspondência entre letras e números é

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

T9 Sabe-se que $\overline{2}$ é gerador do grupo cíclico $U(3^5)$. Determine todos os elementos de ordem 3 de $U(3^5)$ e mostre que formam um subgrupo de $U(3^5)$.

L3 Crie uma função `gerador?` para o Axiom que, tendo como entrada um primo p e um inteiro $1 < b < 2p$ retorna `true` se a função conseguiu determinar pelo teste de Lucas, que $2p + 1$ é um número primo. Caso contrário a função retorna `false`. Explique como esta função pode ser usada para determinar um gerador do grupo $U(2p + 1)$, quando $2p + 1$ é primo.

T7. Como

$$10585 = 5 \cdot 29 \cdot 73,$$

cada fator tem multiplicidade um na fatoração de 10585. Por outro lado,

$$5 - 1 = 4, 29 - 1 = 28 \text{ e } 73 - 1 = 72 \text{ dividem } n - 1 = 10584$$

Portanto, pelo Teorema de Korselt podemos concluir que 10585 é número de Carmichael. Mas todo número de Carmichael é pseudoprimo para qualquer base que é prima com ele. Logo, 10585 é pseudoprimo para a base 3.

Para decidir se 10585 é pseudoprimo forte precisamos aplicar o *teste forte de composição* e verificar se a saída é inconclusiva. Mas,

$$10584 = 2^3 \cdot 1323.$$

Já sabemos que

$$3^{1323} \equiv 8422 \pmod{10585}$$

mas isto ainda não nos permite calcular nada. Passamos, então, ao elemento seguinte da sequência, que é

$$3^{2 \cdot 1323} \equiv 8422^2 \equiv 10584 \pmod{10585}.$$

Como este número é congruente a -1 módulo 10585, a saída do teste forte de composição será inconclusivo. Portanto, 10585 é pseudoprimo forte para a base 3.

T8. Sabemos que

$$n = p \cdot q = 470857 \text{ e que } \phi(n) = (p-1)(q-1) = 469396.$$

Logo,

$$n - (p+q) + 1 = pq - (p+q) + 1 = (p-1)(q-1) = 469396,$$

de modo que

$$p + q = 470857 - 469396 + 1 = 1462;$$

ou ainda,

$$p = 1462 - q.$$

Substituindo isto em $pq = 470857$, obtemos a equação

$$-q^2 + 1462q - 470857 = 0,$$

donde

$$q = \frac{-1462 \pm \sqrt{254016}}{2} = \frac{-1462 \pm 504}{2}$$

cujas soluções são os primos $q = 983$ e $p = 479$ desejados. Passando à decriptação, invertemos $e = 312931$ usando o algoritmo euclidiano estendido, construímos a tabela, que nos dá

$$d = \frac{1 - 469396 \cdot (-2)}{312931} = 3.$$

Restos	Quocientes	x
469396	**	1
312931	**	0
156465	1	1
1	2	- 2

Para usar o algoritmo chinês, calculamos

$$225265^3 \equiv 231 \pmod{479}$$
$$225265^3 \equiv 516 \pmod{983}.$$

Queremos achar $0 \leq r \leq 470856$ tal que

$$r \equiv 231 \pmod{479}$$
$$r \equiv 516 \pmod{983}.$$

Da segunda congruência, $r = 516 + 983t$,que, substituindo na primeira congruência dá $25t \equiv -285 \pmod{479}$ Como 5 é primo com 479, podemos cancelá-lo dos dois lados da congruência, obtendo

$$5t \equiv -57 \pmod{479}.$$

Para eliminar o 5 do lado esquerdo, teremos que invertê-lo módulo 479. Usando o algoritmo euclidiano estendido de novo

Restos	Quocientes	x
479	**	1
5	**	0
4	95	1
1	1	- 1

de modo que o inverso de 5 é

$$\frac{1 - 479 \cdot (-1)}{5} = 96.$$

Multiplicando a última congruência por 96, obtemos

$$t \equiv 96 \cdot (-57) \equiv 276 \pmod{479}.$$

Substituindo na expressão para r,

$$r = 516 + 983 \cdot (276) = 271824$$

que, pela tabela, vemos que corresponde a RIO.

T9. Sabemos que $U(3^5)$ é cíclico gerado por $\overline{2}$ e que sua ordem é

$$\phi(3^5) = 2 \cdot 3^4.$$

Como todo elemento de $U(3^5)$ é potência de $\overline{2}$, queremos encontrar aquelas potências de $\overline{2}$ que têm ordem 3 em $U(3^5)$. Mas se $\overline{2}^q$ tiver ordem 3, então $\overline{2}^{3q} = \overline{1}$, de modo que, pelo lema chave, a ordem de $\overline{2}$ (que é $2 \cdot 3^4$) tem que dividir $3q$. Isto é, $3q = 2 \cdot 3^4.c$, donde $q = 2 \cdot 3^3.c$. Como $q < 2 \cdot 3^4$, segue que $c = 1, 2$; donde

$$q = 2 \cdot 3^3 \text{ ou } \quad q = 2^2 \cdot 3^3.$$

Portanto, os únicos elementos de ordem 3 em $U(3^5)$ são

$$\overline{2}^{2 \cdot 3^3} \text{ e } \quad \overline{2}^{2^2 \cdot 3^3}.$$

O conjunto

$$\{\overline{1}, \overline{2}^{2\cdot 3^3}, \overline{2}^{2^2\cdot 3^3}\}$$

é um subgrupo porque coincide com o conjunto das potências de $\overline{2}^{2\cdot 3^3}$, e tais conjuntos sempre são subgrupos.

L3. Um possível algoritmo é

```
gerador?(b,p) ==
    p1:=powmod(b,2,2*p+1)
    p2:=powmod(b,p,2*p+1)
    p3:=powmod(p2,2,2*p+1)
    if p1 ~=1 and p2 ~=1 and p3=1 then
        return(true)
    else
        return(false)
```

No caso em questão, o que o teste de Lucas faz é tentar determinar se b tem ordem $2p$. Se isto acontece, então, b tem que ser gerador de $U(2p+1)$. Portanto, a saída `true` na verdade significa que $2p+1$ é primo e que b é um dos geradores de $U(2p+1)$.

Prova Final–2012/1

1.1 Prove, *por indução em* n, que

$$\left(1-\frac{1}{4}\right)\left(1-\frac{1}{9}\right)\cdots\left(1-\frac{1}{n^2}\right)=\frac{n+1}{2n}.$$

Explicite claramente cada passo da indução.

1.2 A sequência de Fibonacci F_n é definida por

$$F_0 = F_1 = 1 \text{ e } \quad F_n = F_{n-1} + F_{n-2}.$$

Calcule o quociente e o resto da divisão de F_m por F_{m-3}, quando m for um inteiro maior do que $2^{3452552!}$.

2.1 Calcule a ordem de 16 módulo 173 e use-a para determinar o resto da divisão de 2^{344003} por 173

2.2 Calcule o resto da divisão de $11^{n+2} + 12^{2n+1}$ por 133, quando $n > 7^{52436655454}$.

3.1 Seja $n = 781 = 11 \cdot 71$. Calcule 5^{195} módulo n pelo algoritmo chinês do resto e responda às seguintes perguntas:

(a) n é pseudoprimo para a base 5?

(b) n é número de Carmichael?

3.2 Decodifique a mensagem $38722 - 27554$ que foi codificada usando o RSA com chave pública $n = 47921$ e $e = 18989$. A enumeração das letras começa por $A = 10$.

4.0 Ache um subgrupo de ordem 3 em $U(5^4)$.

DCC-UFRJ–Números inteiros e criptografia–Primeira prova–2012/2

1. Determine *infinitos* múltiplos de 306244 e de 216146 cuja soma seja igual a 128.

2. Prove, por indução em n, que $4^n + 5$ é divisível por 3 para todo $n \geq 0$. Seu argumento deve explicitar claramente cada uma das etapas da indução: base, passo de indução, hipótese de indução e a recursão utilizada.

3. Seja $P = (x_0, y_0)$ uma solução de $x^2 - 2y^2 = 1$. Mostre como obter uma solução de $x^2 - 8y^2 = 1$ a partir de P^2 e escreva uma função `pell2to8`, na linguagem do Axiom, que, tendo como entrada inteiros x_0 e y_0 tais que $x_0^2 - 2y_0^2 = 1$, retorna um par de números que seja solução de $x^2 - 8y^2 = 1$. Sua função deve verificar que (x_0, y_0) de fato é solução de $x_0^2 - 2y_0^2 = 1$; caso contrário, a função deve retornar `[0,0]`.

4. **Oferta especial do dia:** ganhe $0,5$ extra na nota da prova explicando como generalizar a questão acima de modo a obter uma solução de $x^2 - 2^{2r+1}y^2 = 1$ a partir de uma solução (x_0, y_0) de $x^2 - 2y^2 = 1$. Você deve provar todas as afirmações que fizer em sua generalização, mas não é preciso descrever a função do Axiom correspondente a esta questão.

Gabarito

1. Aplicando o algoritmo euclidiano estendido aos números dados temos

Resto	Quociente	x
306244	**	1
216146	**	0
90098	1	1
35950	2	- 2
18198	2	5
17752	1	- 7
446	1	12
358	39	- 475
88	1	487
6	4	- 2423
4	14	34409
2	1	- 36832
0	*	*

de modo que

$$306244 \cdot (-36832) + 216146\beta = 2;$$

donde obtemos $\beta = 52185$. Como $128 = 2 \cdot 64$, multiplicamos

$$306244 \cdot (-36832) + 216146 \cdot 52185 = 2;$$

por 64, obtendo

$$306244 \cdot (-64 \cdot 36832) + 216146 \cdot (64 \cdot 52185) = 128.$$

Portanto,

$$306244 \cdot x + 216146 \cdot y = 128$$

tem as infinitas soluções da forma

$$\begin{aligned} x &= (-64 \cdot 36832) + k \cdot 216146 \\ y &= (64 \cdot 52185) - k \cdot 306244. \end{aligned}$$

Assim, os múltiplos desejados são

$$306244((-64 \cdot 36832) + k \cdot 216146) \text{ e } 216146((64 \cdot 52185) - k \cdot 306244).$$

2. A afirmação a ser provada para todo $n \geq 0$ é

$4^n + 5$ é divisível por 3.

Vamos proceder por indução. Para isto, começamos verificando a base, que corresponde ao caso $n = 0$. Mas, $4^0 + 5 = 1 + 5 = 6$, que é divisível por 3, comprovando que a base é verdadeira. Para fazer o passo de indução precisamos primeiro enunciar a *hipótese de indução*

$4^k + 5$ é divisível por 3;

a partir da qual queremos provar que

$4^{k+1} + 5$ é divisível por 3.

Contudo,

$$4^{k+1} + 5 = 4^k \cdot 4 + 5 = 4^k \cdot (3 + 1) + 5 = (4^k + 5) + 3 \cdot 4^k.$$

Como, pela hipótese de indução, $4^k + 5$ é divisível por 3, concluímos da equação acima que $4^{k+1} + 5$ é a soma de duas parcelas, ambas divisíveis por 3. Logo, $4^{k+1} + 5$ é, ele próprio, divisível por 3. Portanto, pelo Princípio de Indução Finita, podemos dizer que a afirmação "$4^n + 5$ é divisível por 3" vale para todo $n \geq 0$.

Para expressar a recursão de modo absolutamente transparente escreva $s_n = 4^n + 5$ e calcule

$$s_{k+1} - s_k = (4^{k+1} + 5) - (4^k + 5) = 4^{k+1} - 4^k = 3 \cdot 4^k;$$

de modo que a recursão usada é

$$s_{k+1} = s_k + 3 \cdot 4^k.$$

3. Calculando P^2, obtemos

$$P^2 = (x_0^2 + 2y_0^2, 2x_0y_0).$$

que, sendo solução de $x^2 + 2y^2 = 1$, deve satisfazer

$$(x_0^2 + 2y_0^2)^2 - 2(2x_0y_0)^2 = 1.$$

Mas isto nos dá

$$(x_0^2 + 2y_0^2)^2 - 2 \cdot 2^2(x_0y_0)^2 = 1;$$

donde

$$(x_0^2 + 2y_0^2)^2 - 8(x_0y_0)^2 = 1;$$

Portanto,

$$[x_0^2 + 2y_0^2, x_0y_0]$$

é solução de $x^2 - 8y^2 = 1$. A função correspondente no AXIOM é

```
pell2to8(x0,y0) ==
  S:List(INT)
  if one?(x0^2 -2y0^2) = false then
       S:= [0,0]
  else
```

```
        S:= [x0^2+2y0^2, x0y0]
    return(S)
```

4. Para generalizar o resultado da questão 3 basta mostrar, por indução em n que a ordenada de P^{2^n} é um múltiplo de 2^n (questão 10 da lista 3). Portanto, existem inteiros u e v tais que

$$P^{2^n} = (u, 2^n \cdot v).$$

Mas este ponto, sendo solução de $x^2 + 2y^2 = 1$, deve satisfazer

$$u^2 - 2(2^n v)^2 = 1,$$

que nos dá

$$u^2 - 2 \cdot 2^{2n} v^2 = 1,$$

isto é,

$$u^2 - 2^{2n+1} v^2 = 1.$$

Portanto, a solução correspondente de $x^2 - 2^{2n+1} y^2 = 1$ tem a mesma abscissa de P^{2^n}, mas sua ordenda é igual a ordenda de P^{2^n} dividida por 2^n.

4 Calcule os dois fatores primos do número 2925589 usando o algoritmo de Fermat.

5 Considere o número primo $p = 1913$. Determine:

(a) a ordem de 2 módulo p sabendo-se que é menor que $p/8$;

(b) o resto da divisão de 3^{65011} por p.

6 Sejam $P = [8, 2]$ e $Q = [7, 4]$ soluções da equação de Pell modular $x^2 - 3y^2 \equiv 1 \pmod{17}$. Determine as coordenadas da solução S desta mesma equação que satisfaz $P \otimes S \equiv Q^2 \pmod{17}$.

Oferta especial do dia Seja $p > 2^{128374564765775}$ um número primo e $d > 2^{17236465463}$ um inteiro. Determine quanto vale o produto de todas as soluções de $x^2 - dy^2 \equiv 1 \pmod{p}$ que não são congruentes a $[\pm 1, 0]$.

Solução

4. O número 2925589 não é um quadrado perfeito e sua raiz quadrada tem parte inteira igual a 1710. A tabela do algoritmo é:

x	$\sqrt{x^2 - n}$	Inteiro?
1711	$43,954$	não
1712	$73,177$	não
1713	$93,701$	não
1714	$110,485$	não
1715	$125,043$	não
1716	$138,083$	não
1717	150	sim

Portanto os fatores primos desejados são

$$1717 - 150 = 1567 \text{ e } \quad 1717 + 150 = 1867.$$

2. (a) Pelo teorema de Fermat e o lema chave sabemos que a ordem de 2 módulo p divide

$$p - 1 = 1912 = 8 * 239.$$

Sabemos também que a ordem de 2 é menor do que

$$\left[\frac{1913}{8}\right] = 239.$$

Como 239 é primo, as ordens possíveis são 2, 4, 8 e 239. Contudo,

$$2^8 \equiv 256 \not\equiv 1 \pmod{1913}$$

de modo que a ordem de 2 não pode ser 2, nem 4, nem 8. Portanto, 2 tem ordem 239 módulo 1913. Passando a (b), temos pelo teorema de Fermat que

$$3^{1912} \equiv 1 \pmod{1913}.$$

Como $65011 = 1912 \cdot 34 + 3$, a congruência acima nos dá

$$3^{65011} \equiv (3^1912)^34 \cdot 3^3 \equiv 1^{34} \cdot 3^3 \equiv 27 \pmod{1913}.$$

Portanto, o resto desejado é 27.

3. Multiplicando $P \otimes S \equiv Q^2 \pmod{17}$ por P' obtemos

$$P' \otimes (P \otimes S) \equiv P' \otimes Q^2 \pmod{17}$$

donde, pela associatividade de $\otimes$,

$$(P' \otimes P) \otimes S \equiv P' \otimes Q^2 \pmod{17},$$

que equivale a

$$[1, 0] \otimes S \equiv P' \otimes Q^2 \pmod{17}.$$

Portanto,

$$S \equiv P' \otimes Q \pmod{17}.$$

Mas sabemos que $P = [8, 2]$ tem inverso

$$P' \equiv [8, -2] \equiv [8, 15] \pmod{17}.$$

Como

$$Q^2 \equiv [7^2 + 3 \cdot 4^2, 7 \cdot 4 \cdot 2] \equiv [12, 5] \pmod{17},$$

obtemos

$$S \equiv [8, -2] \otimes [12, 5] \equiv [8 \cdot 12 - 3 \cdot 5 \cdot 2, 8 \cdot 5 - 2 \cdot 12] \equiv [66, 16] \equiv [15, 16] \pmod{17}.$$

Portanto,

$$S \equiv [15, 16] \pmod{17}.$$

Oferta do dia: cada solução $P \equiv [x_0, y_0] \pmod{p}$ tem um inverso $P' \equiv [x_0, -y_0] \pmod{p}$. Além disso, só podemos ter $P \equiv P' \pmod{p}$ se $x_0 \equiv -x_0 \pmod{p}$. Mas esta última equação equivale a $2x_0 \equiv 0 \pmod{p}$. Como p é um primo diferente de 2,

concluímos que $x_0 \equiv 0 \pmod{p}$. Mas se $[x_0, 0]$ é solução de $x^2 - dy^2 \equiv 1 \pmod{p}$ então $x_0^2 \equiv 1 \pmod{p}$, que equivale a

$$(x_0 - 1)(x_0 + 1) \equiv 0 \pmod{p};$$

isto é, a dizer que p divide o produto $(x_0 - 1)(x_0 + 1)$. Mas, pela propriedade fundamental dos primos isto implica que p divide $(x_0 - 1)$ ou p divide $(x_0 + 1)$. Em outras palavras, se

$$x_0 \equiv 1 \pmod{p} \text{ ou } x_0 \equiv -1 \pmod{p}.$$

Logo

$$P \equiv P' \pmod{p} \text{ se e somente se } P \equiv [\pm 1, 0] \pmod{p}.$$

Portanto, se multiplicarmos todas as soluções de $x^2 - dy^2 \equiv 1 \pmod{p}$ que não são congruentes a $[\pm 1, 0]$ teremos um produto em que cada solução pode ser pareada com seu inverso resultando em $[1, 0]$.

7 Sabe-se que 7 tem ordem 12 módulo 181.

(a) Calcule o resto da divisão de 7^{147} por $2353 = 13 \cdot 181$ usando algoritmo chinês do resto.

(b) Determine se 2353 é pseudoprimo forte para a base 7.

8 A mensagem $338 - 1500 - 2494$ foi codificada usando-se o RSA com chave pública $n = 7081$ e $e = 2765$.

(a) Fatore n e decodifique a mensagem.

(b) O que você faria se a chave pública fosse $n = 7081$ e $e = 2766$?

9 Sabe-se que $P = [\overline{11}, \overline{11}] \in \mathcal{P}(5, 97)$ tem ordem 49.

(a) Explique porque 5 não pode ser resíduo quadrático módulo 97.

(b) Determine um gerador para $\mathcal{P}(5, 97)$.

Oferta especial do dia Determine a quantidade de soluções módulo 1541 da equação de Pell modular $x^2 - 4y^2 \equiv 1 \pmod{1541}$.

Solução

7. (a) Usando o teorema de Fermat e o fato de 7 ter ordem 12 módulo 181, obtemos

$$7^{147} \equiv (7^{12})12 \cdot 7^3 \equiv 5 \pmod{13}$$
$$7^{147} \equiv (7^{12})12 \cdot 7^3 \equiv 162 \pmod{181}.$$

Portanto, se r for o resto da divisão de 7^{147} por $2353 = 13 \cdot 181$, teremos que

$$r \equiv 5 \pmod{13}$$
$$r \equiv 162 \pmod{181}.$$

Da segunda congruência obtemos que

$$r = 162 + 181t.$$

Substituindo isto na primeira congruência,

$$162 + 181t \equiv 6 + 12t \equiv 5 \pmod{13};$$

donde

$$t \equiv 1 \pmod{13}.$$

Logo, $t = 1 + 13k$, de modo que

$$r = 162 + 181(1 + 13t) = 343 + 2353t.$$

Portanto, o resto desejado é 343.
(b) Aplicando o teste de composição forte temos primeiramente que

$$n - 1 = 2353 = 16 \cdot 147 = 2^4 \cdot 147,$$

de modo que $k = 4$ e $q = 147$. Mas, como acabamos de ver,

$$r_0 \equiv 7^{343} \equiv 343 \pmod{2353}$$

que não é congruente a 1 nem a 2352 módulo 2353. Continuando o cálculo da sequência de restos,

$$r_1 \equiv 7^{2 \cdot 343} \equiv r_0^2 \equiv 343^2 \equiv 2352 \pmod{2353}$$

que é igual a $2353 - 1$. Portanto o teste forte terá como saída inconclusivo na base 7. Como 2353 é ímpar e composto, concluímos que é pseudoprimo forte para a base 7.

8. (a) Fatorando $n = 7081$ pelo algoritmo de Fermat, temos que seus fatores são $p = 73$ e $q = 97$. Logo,

$$\phi(n) = 72 \cdot 96 = 6912.$$

Aplicando o algoritmo euclidiano estendido a $e = 2665$ e $\phi(n) = 6912$, determinamos o inverso de $e = 2765$ como sendo $d = 5$. Decodificando a mensagem

$$\begin{aligned} 338^5 &\equiv \pmod{7081} \\ 1500^5 &\equiv \pmod{7081} \\ 2494^5 &\equiv \pmod{7081}. \end{aligned}$$

Logo, a mensagem original era

$$1214272924 = \text{CERTO}.$$

(b) Eu levantaria o braço e diria: "tem alguma coisa errada na letra (b) desta questão, por e não é primo com $\phi(n)$, como deveria ser o caso". De fato, $\text{mdc}(2766, 6912) = 6 \neq 1$.

9. (a) Pelo teorema de Lagrange a ordem de um elemento tem que dividir a ordem do grupo. Mas se 5 fosse resíduo quadrático módulo 97, teríamos que $\mathcal{P}(5, 97) = 96$ que não é divisível por 49, que é a ordem de $P = [\overline{11}, \overline{11}]$. Logo, 5 não pode ser resíduo quadrático módulo 97.

(b) Como 5 não é resíduo quadrático módulo 97, temos que $\mathcal{P}(5,97) = 98 = 2 \cdot 49$. Portanto, basta achar um elemento de ordem 2 em $\mathcal{P}(5,97)$ e multiplicar P por ele. Mas $[\overline{-1}, \overline{0}]$ tem ordem dois. Portanto, pela questão 2 da lista de revisão da terceira prova

$$[\overline{-1}, \overline{0}] \otimes [\overline{11}, \overline{11}] = [\overline{-11}, \overline{-11}]$$

tem ordem 98 e, consequentemente, é gerador de $\mathcal{P}(5,97)$.

Oferta: como 1541 não é primo, não podemos afirmar que $x^2 - 4y^2 \equiv 1 \pmod{1541}$ tem 1540 soluções. Mas podemos adaptar o mesmo método usado para contar as soluções usado no caso do módulo primo, porque 4 é obviamente um resíduo quadrático módulo 1541. Para isto, fatoramos $x^2 - 4y^2$, o que nos dá

$$(x - 2y)(x + 2y) \equiv x^2 - 4y^2 \equiv 1 \pmod{1541}.$$

Mas isto significa que $x - 2y$ tem que ser inversível módulo 1541 e $x + 2y$ tem que ser seu inverso. Portanto, devemos ter

$$x - 2y = \overline{a} \in U(1541)$$

donde

$$x + 2y = \overline{a}'$$

em que $\overline{a}'$ é o inverso de $\overline{a}$ em $U(1541)$. Mas o sistema

$$\begin{aligned} x - \overline{2}y &= \overline{a} \\ x + \overline{2}y &= \overline{a}' \end{aligned}$$

nos dá

$$\overline{2}x = \overline{a} + \overline{a}' \quad \text{e} \quad \overline{4}y = \overline{a}' - \overline{a}.$$

Como 2 e 4 são inversíveis módulo 1541, podemos concluir que o sistema acima *sempre tem uma única solução*. Logo, haverá uma solução da equação $x^2 - 4y^2 \equiv 1 \pmod{1541}$ para cada escolha

$$x - 2y = \overline{a} \in U(1541)$$

Mas $\#U(1541 = \phi(1541) = 1452$, de modo que o argumento acima mostra que $x^2 - 4y^2 \equiv 1 \pmod{1541}$ tem 1452 soluções. O mesmo argumento mostra que se n é ímpar então $x^2 - 4y^2 \equiv 1 \pmod{n}$ tem $\phi(n)$ soluções.

Primeira Prova–2013/1

1 Prove, por indução em n, que a soma Prove, por indução em n, que a soma

$$\sum_{i=1}^{n} \frac{i}{2^i}$$

é igual a

$$2 - \frac{n+2}{2^n}$$

para todo $n \geq 1$. Seu argumento deve explicitar claramente cada uma das etapas da indução.

2 Sabe-se que $b > 10^{675543321}$ é um número inteiro cujo resto na divisão por 7 é 5. Calcule o resto da divisão por 7 de $b^2 + 3b + 1$.
Dica: unicidade do resto.

3 Ache uma família infinita de soluções para a equação diofantina $2356293x + 26928y = 21$.

Oferta especial do dia Os *números de Fibonacci* são definidos pela recorrência $F_1 = F_2 = 1$ e $F_n = F_{n-1} + F_{n-2}$ para todo inteiro $n \geq 3$. Calcule $d(n) = \text{mdc}(F_{n+2}, F_n)$ para cada $n \geq 1$.

Gabarito

1. Para facilitar a resolução vamos escrever

$$S_n = \sum_{i=1}^{n} \frac{i}{2^i} \text{ e } F_n = 2 - \frac{n+2}{2^n}$$

Com esta notação o que queremos provar por indução em n é que $S_n = F_n$ para todo $n \geq 1$. Temos, então, que a base da indução consiste em verificar que $S_1 = F_1$. Como,

$$S_1 = \frac{1}{2} \text{ e } F_1 = 2 - \frac{3}{2} = \frac{1}{2},$$

a base é verdadeira. Para o passo de indução, supomos que $S_k = F_k$ para algum $k \geq 1$, que é a hipótese de indução, e mostramos que $S_{k+1} = F_{k+1}$. Contudo,

$$S_{k+1} = \underbrace{\frac{1}{2} + \frac{2}{4} + \frac{3}{8} \cdots + \frac{k}{2^k}}_{S_k} + \frac{k+1}{2^{k+1}},$$

de modo que

$$S_{k+1} = S_k + \frac{k+1}{2^{k+1}}.$$

Mas, pela hipótese de indução, $S_k = F_k$, donde

$$S_{k+1} = S_k + \frac{k+1}{2^{k+1}} = F_k + \frac{k+1}{2^{k+1}}.$$

Combinando

$$F_k = 2 - \frac{k+2}{2^k},$$

com a equação anterior, obtemos

$$S_{k+1} = 2 - \frac{k+2}{2^k} + \frac{k+1}{2^{k+1}}.$$

Pondo $1/2^k$ em evidência

$$S_{k+1} = 2 - \frac{1}{2^k}\left[(k+2) - \frac{k+1}{2}\right] = 2 - \frac{1}{2^k}\left[\frac{(2k+4)-(k+1)}{2}\right];$$

que equivale a

$$S_{k+1} = 2 - \frac{1}{2^k}\left[\frac{k+3}{2}\right] = F_{k+1};$$

como devíamos mostrar. Portanto, pelo Princípio de Indução Finita, a igualdade $S_n = F_n$ é verdadeira para todo $n \geq 1$.

2. Como b deixa resto 5 na divisão por 7, devemos ter que

$$b = 7q + 5$$

para algum inteiro positivo q. Note que 5 é um resto legítimo na divisão por 7 porque $0 \leq 5 < 7$. Substituindo $b = 7q + 5$ em $b^2 + 3b + 1$ obtemos

$$b^2 + 3b + 1 = (7q+5)^2 + 3(7q+5) + 1 = 49q^2 + 70q + 25 + 21q + 15 + 1.$$

Pondo 7 em evidência

$$b^2 + 3b + 1 = 7(7q^2 + 10q + 3q) + 25 + 15 + 1 = 7(7q^2 + 10q + 3q) + 41.$$

Contudo, 41 não é um resto admissível na divisão por 7 porque não é menor que 7. Por isso, devemos dividir 41 por 7, obtendo $41 = 5 \cdot 7 + 6$. Assim,

$$b^2 + 3b + 1 = 7(7q^2 + 10q + 3q) + 5 \cdot 7 + 6 = 7(7q^2 + 10q + 3q + 5) + 6.$$

Levando em conta esta última equação e $0 \leq 6 < 7$, podemos concluir da unicidade do quociente e do resto que o resto da divisão de $b^2 + 3b + 1$ por 7 é 6.

3. Para resolver $2356293x + 26928y = 21$ começamos aplicando o algoritmo euclidiano estendido a 785431 e 8976:

de modo que

$$2356293 \cdot 1303 + 26928\beta = 3;$$

Resto	Quociente	x
2356293	**	1
26928	**	0
13557	87	1
13371	1	- 1
186	1	2
165	71	- 143
21	1	145
18	7	- 1158
3	1	1303
0	*	*

donde obtemos $\beta = -114017$. Como $21 = 3 \cdot 7$, multiplicamos a equação anterior por 7, obtendo:

$$2356293 \cdot (1303 \cdot 7) + 26928 \cdot (-114017 \cdot 7) = 21.$$

por 7, obtendo 9121,- 342051

$$2356293 \cdot 1303 + 26928 \cdot (-114017) = 3.$$

Portanto, uma família infinita de soluções

$$2356293x + 26928y = 21,$$

é dada por

$$\begin{aligned} x &= (1303 \cdot 7) + k \cdot 26928 \\ y &= (-114017 \cdot 7) - k \cdot 2356293, \end{aligned}$$

qualquer que seja o inteiro k.

Oferta especial do dia: Como recorrência

$$F_1 = F_2 = 1 \text{ e } \quad F_n = F_{n-1} + F_{n-2} \text{ para todo inteiro } \quad n \geq 3,$$

temos que

$$F_{n+2} = F_{n+1} + F_n = (F_n + F_{n-1}) + F_n = 2F_n + F_{n-1}.$$

Portanto pelo lema utilizado na demonstração do algoritmo euclidiano,

$$\text{mdc}(F_{n+2}, F_n) = \text{mdc}(F_{n-1}, F_n).$$

Mas, aplicando o mesmo lema à recorrência que define os números de fibonacci, obtemos

$$\text{mdc}(F_n, F_{n-1}) = \text{mdc}(F_{n-1}, F_{n-2}) = \cdots = \text{mdc}(F_3, F_2).$$

Como $F_2 = 1$ divide $F_3 = 2$, concluímos que

$$\text{mdc}(F_n, F_{n-1}) = \text{mdc}(F_3, F_2) = 1.$$

Logo,

$$d(n) = \text{mdc}(F_{n+2}, F_n) = \text{mdc}(F_{n-1}, F_n) = 1,$$

para todo $n \geq 1$.

4 Calcule os dois fatores primos do número 758603 usando o algoritmo de Fermat.

5 Sabendo-se que 97 é um número primo e que todos os elementos diferentes de $\overline{0}$ de $\mathbb{Z}_{97}$ são potências de $\overline{5}$, determine:

(a) a ordem de $\overline{5}$ em $\mathbb{Z}_{97}$;

(b) um elemento de ordem 5 em $\mathbb{Z}_{97}$;

(c) o resto da divisão de $5^{1185123}$ por 97.

6 Seja $P = [\overline{253}, \overline{176}]$ uma solução da equação de Pell $x^2 - \overline{2}y^2 = \overline{1}$ em $\mathbb{Z}_{257}$. Sabendo-se que $P^{64} = [\overline{0}, \overline{34}]$, e que $\overline{2} = \overline{60}^2$, determine:

(a) a ordem de P em $\mathcal{P}(3, 97)$;

(b) inteiros a e b tais que $Q = [\overline{a}, \overline{b}]$ é um elemento de ordem 8 em $\mathcal{P}(3, 97)$.

Dica para (b): calcule b a partir do fato de que Q^2 é conhecido.

Oferta especial do dia Descreva, na linguagem do Axiom, uma função `resolvePell` que, tendo como entrada um inteiro positivo d retorna uma solução diferente de $[\pm 1, 0]$ da equação de Pell $x^2 - dy^2 = 1$. Lembre-se que se d é um quadrado perfeito, a equação de Pell correspondente não tem soluções diferentes de $[\pm 1, 0]$. A sua função deve testar isto e retornar a mensagem `apenas soluções triviais` quando isto ocorrer.

4. Como $n = 758603$ não tem raiz quadrada, construímos a tabela:

x	$\sqrt{x^2 - n}$	status
871	6.165	não é inteiro
872	42.2	não é inteiro
873	59.38	não é inteiro
874	72.62	não é inteiro
875	83.8	não é inteiro
876	93.66	não é inteiro
877	102.6	não é inteiro
878	110.8	não é inteiro
879	118.5	não é inteiro
880	125.7	não é inteiro
881	132.5	não é inteiro
882	139	é inteiro

Portanto, os fatores desejados são

$$x - y = 882 - 139 = 743 \text{ e } \quad x + y = 882 + 139 = 1021.$$

5. Como é dito que cada elemento não nulo de $\mathbb{Z}_{97}$ é uma potência de $\overline{5}$, têm que existir 96 potências distintas deste elemento, o que só é possível se $\overline{5}$ tiver ordem 96 em $\mathbb{Z}_{97}$. Como todo a ordem de um elemento de um grupo tem que dividir o número de elementos do grupo, então não pode existir elemento de ordem 5 em $\mathbb{Z}_{97}$. De fato, $U(97)$ tem ordem $96 = 2^5 \cdot 3$, que não é divisível por 5. Como $\overline{5}$ tem ordem 96 e dividindo 1185123 por 96 obtemos quociente 12345 e resto 3, teremos que

$$\overline{5}^{1185123} = (\overline{5}^{96})^{12345} \cdot \overline{5}^3 = \overline{125} = \overline{28}$$

concluímos que $5^{1185123}$ tem resto 28 na divisão por 97.

6. Como $\overline{2} = \overline{60}^2$, temos que 2 é resíduo quadrático módulo 257, de modo que $\mathcal{P}(2, 97)$ tem $257 - 1 = 256 = 2^8$ elementos. Logo, pelo teorema de Lagrange combinado com o lema chave, a ordem de P tem que dividir 2^8. Em particular, a ordem de P tem que ser uma potência de 2. Como foi dado no problema que $P^{64} = [\overline{0}, \overline{34}]$, sabemos que a ordem de P não pode ser uma potência de 2 menor ou igual a que 2^6. Mas,

$$P^{128} = (P^{64})^2 = [\overline{256}, \overline{0}] = [\overline{-1}, \overline{0}]$$

cujo quadrado é o elemento neutro. Portanto, P tem ordem 2^8, já que nenhuma potência de P com expoente da forma 2^k e $k < 8$ é igual a $[\overline{1}, \overline{0}]$. Para fazer o item (b), basta notar que, como P tem ordem $256 = 8 \cdot 32$ então P^{32} tem que ter ordem 8. De fato, se r for a ordem de P^{32}, então

$$(P^{32})^r = P^{32r} = [\overline{1}, \overline{0}];$$

de modo que, pelo lema chave, a ordem de P tem que dividir $32r$. Mas o menor r para o qual 256 divide $32r$ é $r = 8$. Portanto, para completar a questão, basta achar as coordenadas de P^{32}. Mas, Em vez de calcular P^{32} diretamente, prefiro usar o fato de que

$$P^{64} = (P^{32})^2.$$

Supondo que $P^{32} = [\overline{a}, \overline{b}]$, teremos que

$$[\overline{0}, \overline{34}] = P^{64} = (P^{32})^2 = [\overline{a^2 + 2b^2}, \overline{2ab}],$$

donde

$$\overline{a^2 + 2b^2} = \overline{0} \text{ e } \overline{2ab} = \overline{34}.$$

Mas P^32 é solução de $x^2 - \overline{2}y^2 = \overline{1}$, de modo que

$$\overline{a^2 - 2b^2} = \overline{1}.$$

Subtraindo esta última igualdade de $\overline{a^2 + 2b^2} = \overline{1}$, obtemos

$$\overline{4b^2} = \overline{-1} = \overline{256};$$

donde $\overline{b^2} = \overline{64}$, que nos dá $\overline{b} = \overline{8}$. Logo, de $\overline{2ab} = \overline{34}$ obtemos $\overline{16a} = \overline{34}$; isto é, $\overline{8a} = \overline{17}$. Mas $\overline{8}$ tem inverso $\overline{225}$ de modo que

$$a = \overline{225} \cdot \overline{17} = \overline{227}.$$

Assim, $Q = [\overline{227}, \overline{8}]$.

Como $P^2 = [\overline{31}, \overline{134}]$, efetuando o cálculo acima obtemos

$$P^{32} = [\overline{253}, \overline{176}] \otimes [\overline{31}, \overline{134}] = [\overline{140}, \overline{26}]$$

Oferta Especial do dia: Uma possibilidade é o código abaixo:

```
resolvePell(d:PI):Union(String,List(NNI)) ==
    r:PI:= wholePart(sqrt(d::FLOAT))::INT
    if d = r^2 then
           "apenas solucoes triviais"
    else
           x:= 1 - pois não quero soluções triviais
           while integer?(sqrt(1+d*y^2)) repeat
                   y := y+1
           [sqrt(1+d*y^2)::INT,y]
```

7 Seja $n = 7813 = 13 \cdot 601$. Sabendo-se que 5 tem ordem 12 módulo 601, determine:

(a) o resto da divisão de 5^{1953} por 7813 usando o algoritmo chinês do resto;

(b) se n é pseudoprimo forte na base 5;

(c) se n é pseudoprimo na base 5.

8 A mensagem $5917-57117$ foi codificada usando-se o RSA com chave pública $n = 59623$ e $e = 35381$. Sabendo-se que $\phi(n) = 58968$:

(a) ache os fatores primos de n;

(b) decodifique a mensagem.

9 Sejam $P = [\overline{56}, \overline{48}]$ e $Q = [\overline{6}, \overline{17}]$ duas soluções da equação de Pell modular $x^2 - \overline{7}y^2 = \overline{1}$ em $\mathbb{Z}_{71}$. Sabendo-se que P tem ordem 9 e Q tem ordem 8, determine:

- a ordem do grupo $\mathcal{P}(7, 71)$;
- um gerador para $\mathcal{P}(7, 71)$;
- o gerador de um subgrupo cíclico de ordem 24 em $\mathcal{P}(7, 71)$.

Você deve indicar quais são as coordenadas dos pontos obtidos em (b) e (c).

Oferta especial do dia Sejam $q > p > 10^{200}$ dois números primos, $n = p \cdot q$ o produto destes primos e e um inteiro positivo tal que $\text{mdc}(\phi(n), e) = 1$. Portanto, (n, e) é uma chave pública do RSA.

(a) Mostre que se $0 \leq b \leq n - 1$ é primo com n então existe um inteiro positivo k tal que $b^{e^k} \equiv b \pmod{n}$.

(b) Explique como seria possível usar isto para quebrar o RSA.

DICA: k é a ordem de $\overline{e}$ em $U(\phi(n))$. Note que $\overline{e}$ é a classe da chave pública e do RSA no grupo $U(\phi(n))$ e *não* o elemento neutro de $U(\phi(n))$, que é igual a $\overline{1}$.

(a) Seja $n = 7813 = 13 \cdot 601$. Seja $0 \leq r \leq n-1$ um número tal que $r \equiv 5^{1953} \pmod{n}$. Então, pelo Teorema de Fermat e pelos dados do problema:

$$r \equiv 5^{1953} \equiv 5^9 \equiv (5^2)^4 \cdot 5 \equiv (-1)^4 \cdot 5 \equiv 5 \pmod{13}$$
$$r \equiv 5^{1953} \equiv (5^{12})^{162} \cdot 5^9 \equiv 476 \pmod{601}.$$

Portanto, devemos resolver o sistema

$$r \equiv\equiv 5 \pmod{13}$$
$$r \equiv\equiv 476 \pmod{601},$$

pelo Algoritmo Chinês do Resto. Tomando $r = 476 + 601t$ na segunda equação e substituindo na primeira, obtemos

$$476 + 601t \equiv 5 \pmod{13}.$$

Reduzindo o lado esquerdo módulo 13, resta:

$$8 + 3t \equiv 5 \pmod{13} \text{ donde } 3t \equiv -3 \pmod{13}.$$

Como 3 é inversível módulo 13, concluímos que

$$t \equiv -1 \equiv 12 \pmod{13}.$$

Assim, $t = 12 + 13k$ nos dá

$$r = 476 + 601t = 476 + 601(12 + 13k) = 7688 + 7813k;$$

(b) Já sabemos que n é ímpar de modo que o resto desejado é 7688. e composto. Para determinar se é ou não pseudoprimo forte na base 5 basta aplicar o teste forte de composição e verificar se retorna inconclusivo. Para isto começamos determinando a maior potência de de 2 que divide $n-1$:

$$n - 1 = 7812 = 2^2 \cdot 153,$$

donde $k = 2$ e $q = 153$. Como já sabemos que

$$5^{153} \equiv 7688 \pmod{7813},$$

precisamos apenas calcular o quadrado deste número:

$$5^{2 \cdot 153} \equiv 7688^2 \equiv 7812 \pmod{7813}.$$

Como obtivemos um resíduo igual a $n-1$, a saída do teste será `inconcluisivo`, de forma que 7813 é realmente um pseudoprimo forte para a base 5. Finalmente, como todo pseudoprimo forte é igualmente pseudoprimo para a mesma base, segue-se que 7813 é pseudoprimo na base 5.

8. Sabemos que

$$n = pq = 59623 \text{ e que } \phi(n) = (p-1)(q-1) = 58968.$$

Portanto,

$$58968 = pq - (p+q) + 1 = 59623 - (p+q) + 1 \text{ donde } \quad p+q = 656.$$

Substituindo $q = 59623/p$ em $p + q = 656$, obtemos a equação do segundo grau

$$p^2 - 656p + 59623 = 0,$$

cujas soluções são 109 e 547, que são os fatores primos de 59623. Logo, $p = 109$ e $q = 547$. Para fazer (b) precisamos apenas de calcular o inverso de $e = 35381$ módulo $\phi(n) = 58968$ pelo algoritmo euclidiano estendido, que dá $d = 5$. Portanto, para decodificar a mensagem basta calcular:

$$\begin{aligned} 5917^5 &\equiv 192 \pmod{59623} \\ 57117^5 &\equiv 219 \pmod{59623}. \end{aligned}$$

Olhando na tabela vemos que a mensagem é JMJ.

9. A maneira mais fácil de fazer é usar o exercício 2 da lista de revisão para a terceira prova. Como P tem ordem 9 e Q tem ordem 8 e 9 e 8 são primos entre si, então $P \otimes Q$ tem ordem $8 \cdot 9 = 72$. Como estamos trabalhando sob módulo 71, concluímos que

- 7 não é resíduo quadrático módulo 71;
- o grupo $\mathcal{P}(7, 71)$ tem ordem 72;
- $P \otimes Q = [\overline{13}, \overline{33}]$ gera $\mathcal{P}(7, 71)$.

Finalmente, para obter um elemento de ordem 24 basta notar que $72 = 24 \cdot 3$, de modo que

$$(P \otimes Q)^3 = [\overline{13}, \overline{33}]^3 = [16, 52]$$

tem ordem 24 e, portanto, gera um subgrupo cíclico de ordem 24 em $\mathcal{P}(7, 71)$.

Oferta especial do dia: como $0 \leq b \leq n-1$ é primo com n por hipótese, temos que $\overline{b} \in U(n)$, que é o conjunto de elementos inversíveis módulo n. De maneira semelhante, $\overline{e} \in U(\phi(n))$. Como $U(\phi(n))$ é um grupo finito, o subgrupo cíclico de $U(\phi(n))$ gerador por $\overline{e}$ também é finito. Digamos que este subgrupo tenha ordem k. Então,

$$\overline{e}^{k-1} \cdot \overline{e} = \overline{e}^m = \overline{1};$$

de modo que $\overline{d} = \overline{e}^{k-1}$ em $U(\phi(n))$. Por outro lado, como o RSA decodifica corretamente qualquer bloco $0 \leq b \leq n-1$, temos que

$$b \equiv (b^e)^d \pmod{n}.$$

Levando em conta que $d \equiv e^{m-1} \pmod{\phi(n)}$:

$$b \equiv (b^e)^{e^{k-1}} \equiv b^{e^k} \pmod{n},$$

como desejávamos mostrar. Outra maneira, ainda mais óbvia é usar que $e^k \equiv 1 \pmod{\phi(n)}$, de modo que $e^k = 1 + c\phi(n)$, para algum inteiro positivo c. Isto nos dá

$$b^{e^k} \equiv b^{1+c\phi(n)} \equiv b \cdot b^{\phi(n)} \equiv b \pmod{\phi(n)},$$

pelo Teorema de Lagrange, pois $\phi(n)$ é a ordem de $U(n)$. A razão pela qual isto leva a um ataque do RSA é que o resíduo r de b^e módulo n é conhecido, pois é a codificação do bloco b, que pode ser interceptada quando a mensagem codificada é transmitida. Mas, calculando e-ésimas potências sucessivas de r, acabamos obtendo

$$r^{e^{k-1}} \equiv b^{e^k} \equiv b \pmod{n},$$

decodificando assim a mensagem. A razão pela qual isto não representa um ataque qua ameaça o RSA é que k é geralmente muito grande e, portanto, levará um tempo muito grande para chegar a b^{e^k}. Este ataque ao RSA é conhecido como o *ataque cíclico*.

Questão 1 (2 points)

Sejam a e b números inteiros maiores que $10^{100!}$. Se a deixa resto 5 e b deixa resto 7 na divisão por 13, qual o resto de ab na divisão por 13?

Solução:

Como a deixa resto 5 na divisão por 13, existe um inteiro q tal que

$$a = 13q + 5.$$

Analogamente, como b deixa resto 7 na divisão por 13, existe um inteiro q' tal que

$$b = 13q' + 7.$$

Logo,

$$ab = (13q + 5)(13q' + 7) = 13(13qq' + 7q + 5q') + 35.$$

Note que 35 não pode ser o resto de ab na divisão por 13 porque $35 > 13$. Mas, dividindo 35 por 13 obtemos

$$35 = 13 \cdot 2 + 9.$$

Substituindo isto na equação para ab,

$$ab = 13(13qq' + 7q + 5q') + 35 = 13(13qq' + 7q + 5q' + 2) + 9.$$

Portanto, o resto da divisão de ab por 13 é 9 (e o quociente é $13qq' + 7q + 5q' + 2$).

Questão 2 (2 points)

Dois fazendeiros cultivavam juntos todo o seu arroz e o dividiam igualmente entre si no tempo da colheita. Num certo ano cada um deles foi a um mercado diferente vender o seu arroz. Cada um destes mercados só comprava arroz em múltiplos de um peso padrão, que diferia em cada um dos mercados. O primeiro fazendeiro vendeu o seu arroz em um mercado onde o peso padrão era 87 Kg. Ele vendeu tudo o que podia e voltou para casa com 18 Kg de arroz. O segundo fazendeiro vendeu todo o arroz que podia em um mercado cujo peso padrão era de 170 Kg e voltou para casa com 58 Kg. Use o algoritmo euclidiano estendido para determinar a quantidade total de arroz que eles cultivaram?

Solução:

Seja t a quantidade de arroz que coube a cada um dos fazendeiros naquele ano. Como o primeiro fazendeiro vendeu seu arroz em um mercado com peso padrão $87Kg$ e lhe restaram $18Kg$, temos que

$$t = 87q + 18;$$

de maneira semelhante, os dados correspondentes ao segundo fazendeiro nos permitem afirmar que

$$t = 170q' + 58.$$

Subtraindo uma equação da outra, obtemos

$$87q - 170q' = 40.$$

Aplicando o algoritmo euclidiano estendido a 160 e 87 temos:

restos	quocientes	x
170	$**$	1
87	$**$	0
83	1	1
4	1	-1
3	20	21
1	1	-22

de modo que

$$y = \frac{1 - 31 \cdot 160}{87} = 43$$

Logo,

$$-170 \cdot 22 + 87 \cdot 43 = 1.$$

Multiplicando esta equação por 40, obtemos

$$-170 \cdot 880 + 87 \cdot 1720 = 40.$$

Portanto, a solução geral da equação diofantina $87q - 170q' = 40$ é dada por

$$q = 1720 - 170k \quad \text{e} \quad q' = 880 - 87k.$$

Portanto, a quantidade total de arroz que coube ao primeiro fazendeiro é

$$t = 87q + 18 = 87(1720 - 160k) + 18 = -14790k + 149658$$

e ao segundo fazendeiro

$$t = 170q' + 58 = 160(880 - 87k) + 58 = -14790k + 149658.$$

de modo que o total tem que satisfazer $2t = 299316 - 29580 \cdot k$. Os valores de k para os quais a solução é positiva ocorrem quando

$$k < \frac{299316}{29580} = 10,11886...$$

Portanto, o menor valor possível que resolve o problema é $k = 10$, que corresponde a 3516 Kg de arroz.

Questão 3 (2 points)

No conjunto $\mathcal{R}$ dos *números racionais diferentes de* 1, definimos a operação

$$a \star b = a + b - ab.$$

em que $a \neq 1$ e $b \neq 1$ são frações.

(a) Determine o elemento neutro desta operação.

(b) Quais propriedades de um grupo (abeliano) esta operação satisfaz?

(c) Determine se $\mathcal{R}$ com a operação $\star$ é um grupo (abeliano).

Solução:

(a) Precisamos descobrir um número racional e tal que $a \star e = a$ para todo número racional $a \neq 1$. Mas, por definição $a \star e = a + e - ae$ para que isto seja igual a a devemos ter que $e - ea = 0$; isto é, que $e(1 - a) = 0$, que só vale para todo $a \in \mathbb{Q}$ se $e = 0$. Portanto, o elemento neutro de $\star$ é 0.

(b) Como a soma e a multiplicação de frações é uma fração, é claro da definição de $\star$ que se $a, b \in \mathcal{R}$, então $a \star b = a + b - ab$ é uma fração. Resta saber se $a, b \neq 1$ implicam que $a + b - ab \neq 1$. Contudo, $a + b - ab = 1$ equivale a dizer que $b - ab = 1 - a$. Pondo b em evidência do lado esquerdo,

$$b(1 - a) = 1 - a.$$

Como $a \in \mathcal{R}$, então $a \neq 1$, de modo que $1 - a \neq 0$ pode ser cancelado dos dois lados da igualdade, o que nos dá $b = 1$. Mas isto é falso, pois $b \in \mathcal{R}$. Logo, se $a, b \in \mathcal{R}$, então $a \star b = a + b - ab \in \mathcal{R}$, de modo que a operação é fechada em $\mathcal{R}$. Além disso, já sabemos que $\star$ admite 0 como elemento netro. A operação é comutativa porque

$$a \star b = a + b - ab = b + a - ba = b \star a,$$

e é associatividade porque

$$a \star (b \star c) = a \star (b + c - bc) = a + (b + c - bc) - a(b + c - bc) = a + b + c - bc - ab - ac + abc$$

que é igual a

$$(a \star b) \star c = (a + b - ab) \star c = a + b - ab + c - (a + b - ab)c.$$

Finalmente, precisamos verificar se cada elemento de $\mathbb{Q}$ tem inverso relativamente a $\star$. Para isso, dado $a \in \mathbb{Q}$, precisamos resolver a equação $a \star a' = 0$. Mas, pela definição de $\star$,

$$0 = a \star a' = a + a' - aa' = a + a'(1 - a).$$

Como $a \neq 1$, podemos resolver a equação obtendo

$$a' = \frac{-a}{1 - a} = \frac{a}{a - 1},$$

para o inverso de $a \in \mathcal{R}$ relativamente à operação $\star$.

Questão 4 (2 points)

Ache uma solução da equação de Pell $x^2-18y^2=1$ usando o método cíclico (algoritmo de Brouncker) e calcule o quadrado do inverso deste elemento.

Solução:

Seja $F_0(x_0,y_0)=x_0^2-18y_0^2$ e $P=(x_0,y_0)$. A raiz quadrada positiva de $F_0(t,1)=t^2-18$ é $t=4.21875...$ e sua parte inteira é $q_0=4$. Portanto, devemos aplicar a F_0 e P a substituição definida por

$$x_0=y_1+4x_1 \quad \text{e} \quad y_0=x_1$$

obtendo, ao final do primeiro passo,

$$F_1(x_1,y_1)=2x_1^2-8x_1y_1-y_1^2 \quad \text{e} \quad P=(4x_1+y_1,x_1).$$

Passando ao segundo passo, a raiz positiva de $F_1(t,1)=2t^2-8t-1$ é $t=4.09375$, cuja parte inteira é $q_1=4$. Logo, devemos aplicar a F_1 e P a substituição

$$x_1=y_2+4x_2 \quad \text{e} \quad y_1=x_2$$

que nos dá

$$F_2(x_2,y_2)=x_2^2-8x_2y_2-2y_2^2 \quad \text{e} \quad P=(17x_1+4y_1,4x_1+y_1).$$

Como o coeficiente de x_2^2 em F_2 é 1 e a equação resultante de $F_1=1$ ao cabo destas duas etapas é $F_2=(-1)^2=1$, temos que $F_2(1,0)=0$. Portanto, para obter a solução desejada basta tomar $x_2=1$ e $y_2=0$ em P, o que nos dá $P=(17,4)$.

Como o inverso de $(17,4)$ é $(17,-4)$, então o quadrado do inverso de P é

$$(17,-4)^2=(17,-4)\otimes(17,-4)=(17^2+4^2\cdot 18,2\cdot 17\cdot(-4))=[577,-136].$$

Questão 1 (2 points)
Ache os fatores de 46259 usando o algoritmo de fatoração de Fermat.

Solução:

Como a raiz quadrada de 46259 é $215,079$, devemos executar a tabela

x	$\sqrt{x^2-n}$	inteiro?
216	$19,92$	não
217	$28,81$	não
218	$35,57$	não
219	$41,26$	não
220	$46,27$	não
221	$50,81$	não
222	55	sim

Portanto, os fatores desejados são

$$x-y=167 \quad \text{e} \quad x+y=277.$$

Questão 2 (2 points)
Sabe-se que um dos seguintes primos 7, 11, 23, 29 e 41 é fator de $30!+1$. Determine este primo.

Solução:

Como $\text{mdc}(30!, 30!+1)=1$, nenhum fator de $30!$ pode dividir $30!+1$. Mas 7, 11 e 29 dividem $30!$. Logo, o único primo da lista dada que pode dividir $30!+1$ é 41

Questão 3 (2 points)
Sabe-se que $3^{13} \equiv 53 \pmod{131}$.

(a) Calcule a ordem de $\overline{3}$ em $\mathbb{Z}_{131}$.

(b) Calcule o resto da divisão de $97^{3336712}$ por 131.

Solução:

Pelo teorema de Fermat

$$3^{130} \equiv 1 \pmod{131};$$

de modo que, pelo lema chave, a ordem de $\overline{3}$ tem que dividir 130. Como

$$\begin{aligned} 3^5 &\equiv 112 \pmod{131} \\ 3^{13} &\equiv 53 \pmod{131} \\ 3^{65} &\equiv 53^5 \equiv 1 \pmod{131}, \end{aligned}$$

podemos concluir que $\overline{3}$ tem ordem 65 módulo 131. Por outro lado

$$3336712 = 25667 \cdot 130 + 2$$

de modo que, pelo teorema de Fermat,

$$97^{3336712} \equiv (97^{130})^{25667} \cdot 97^2 \equiv 97^2 \equiv 108 \pmod{131}.$$

Portanto, o resto da divisão de $97^{3336712}$ por 131 é 108.

Questão 4 (2 points)

Seja $1891 = 31 \cdot 61$. Use o teorema de Fermat para determinar se 1891 é pseudoprimo

(a) para a base 3;

(b) para a base 11.

Solução:

Como $1891 = 31 \cdot 61$, vamos calcular 5^{1891} módulo cada um destes primos. Usando o Teorema de Fermat para o primo 31, obtemos

$$\begin{aligned} 3^{1890} &\equiv 1 \pmod{31} \\ 11^{1890} &\equiv 1 \pmod{31} \end{aligned}$$

pois 30 divide 1890. Por outro lado, calculando as potências de $\overline{3}$ em $\mathbb{Z}_{61}$ temos

$$\begin{aligned} \overline{3}^4 &= \overline{81} = \overline{20} \\ \overline{3}^5 &= \overline{3} \cdot \overline{20} = -\overline{1}. \end{aligned}$$

Logo,

$$\overline{3}^{10} = \overline{1}$$

de modo que

$$\overline{3}^{1890} = \overline{1}$$

em $\mathbb{Z}_{61}$. Mostramos, assim, que $3^{1890} - 1$ é divisível por 31 e por 61; e, portanto, também pelo produto $31 \cdot 61 = 1891$. Logo 1891 é um pseudoprimo para a base 3. Passando à base 11, temos que em $\mathbb{Z}_{61}$:

$$\begin{aligned} \overline{11}^2 &= \overline{60} \\ \overline{11}^3 &= \overline{11} \cdot \overline{60} = \overline{50} \\ \overline{11}^4 &= \overline{60}^2 = \overline{1}. \end{aligned}$$

Assim,

$$\overline{11}^{1890} = (\overline{11}^4)^{472} \cdot \overline{11}^2 = \overline{11}^2 = \overline{60}$$

em $\mathbb{Z}_{61}$, Em particular,

$$11^{1890} \not\equiv 1 \pmod{1891};$$

de modo que 1891 não é pseudoprimo para a base 11.

Questão 5 (2 points)

Sejam p e q números primos distintos.

(a) Prove que há um único elemento de ordem dois em $U(p)$.

(b) Use o teorema chinês do resto para determinar quantos elementos de ordem dois existem em $U(pq)$.

Solução:

Se $\overline{a} \neq \overline{1}$ tem ordem dois em $U(p)$, então $\overline{a}^2 = \overline{1}$; isto é, p divide

$$\overline{a}^2 - \overline{1} = (\overline{a} - \overline{1})(\overline{a} + \overline{1}) = \overline{0}.$$

Em outras palavras, p divide $(a-1)(a+1)$. Como p é primo, isto implica que p divide $a-1$ ou p divide $a+1$; que equivale a dizer que

$$\overline{a} = \overline{1} \quad \text{ou} \quad \overline{a} = -\overline{1}.$$

Como $\overline{a} \neq \overline{1}$, por hipótese, mostramos o único elemento de ordem dois em $U(p)$ é $-\overline{1}$. Passando, agora, à letra (b), suponhamos que $\overline{\alpha} \neq \overline{1}$ tem ordem dois em $U(pq)$. Como no caso anterior, isto implica que

$$(a-1)(a+1) \equiv 0 \pmod{pq};$$

mas, desta vez, há quatro possibilidades:

1. pq divide $a-1$;
2. pq divide $a+1$;
3. p divide $a-1$ e q divide $a+1$;
4. q divide $a-1$ e p divide $a+1$.

O caso (1) está excluído pois $\overline{\alpha} \neq \overline{1}$ e o caso (2) corresponde a $\overline{\alpha} = -\overline{1}$. Os casos (3) e (4) correspondem aos sistemas de congruências

$$\begin{aligned} a &\equiv 1 \pmod{p} & \qquad a &\equiv -1 \pmod{p} \\ a &\equiv -1 \pmod{q} & \qquad a &\equiv 1 \pmod{q}. \end{aligned}$$

Como p e q são primos distintos, temos que $\text{mdc}(p,q) = 1$, de modo que, pelo teorema chinês do resto, ambos os sistemas têm exatamente uma solução cada um. Temos, assim, três elementos de ordem dois em $U(pq)$: $\overline{pq-1}$ e as soluções dos dois sistemas de congruência apresentados acima. Note que estes três elementos têm que ser diferentes, pois são soluções de sistemas de congruências distintos.

Questão 1 (2 points)

Sabendo que 2101 tem dois fatores primos distintos, determine:

(a) o resto da divisão de 7^{525} por 2101, pelo algoritmo chinês do resto;

(b) se 2101 é ou não pseudoprimo forte para a base 7.

Solução:

Como $2101 = 11 \cdot 191$, vou calcular 3^{525} módulo cada um deste números. Usando o teorema de Fermat e o fato de $\overline{7}$ ter ordem 10 em $\mathbb{Z}_{191}$, temos então que

$$7^{525} \equiv 7^5 \equiv 10 \equiv -1 \pmod{11}$$
$$7^{525} \equiv 7^5 \equiv 190 \equiv -1 \pmod{191}.$$

Logo, pelo teorema chinês do resto,

$$7^{525} \equiv -1 \equiv 2100 \pmod{2101}.$$

Como $2100 = 2^2 \cdot 525$ a congruência acima mostra que 2101 é pseudoprimo forte para a base 7.

Questão 2 (2 points)

Use o teorema de Lagrange para mostrar que $\mathcal{P}(3, 17)$ não contém nenhum elemento de ordem cinco.

Solução:

Para poder usar Lagrange precisamos descobrir quantos elementos tem o grupo $\mathcal{P}(3, 17)$, mas isto depende de 3 ser ou não resíduo quadrático módulo 17. Para determinar isto calculamos os quadrados dos elementos de $\mathbb{Z}_{17}$ representados por inteiros menores que 8, porque $(17 - a)^2 \equiv a^2 \pmod{17}$. Os resultados estão tabelados abaixo:

classe	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$
quadrado	$\overline{1}$	$\overline{4}$	$\overline{9}$	$\overline{16}$	$\overline{8}$	$\overline{2}$	$\overline{15}$	$\overline{13}$

Verificamos a partir da tabela que 3 *não* é resíduo quadrático módulo 3, de modo

$$\#\mathcal{P}(3, 17) = 17 + 1 = 18.$$

Mas, pelo teorema de Lagrange, a ordem de um elemento tem que dividir a ordem do grupo. Como 5 não divide 18, o grupo $\mathcal{P}(3, 17)$ não pode ter elementos de ordem cinco.

Questão 3 ()

Determine um subgrupo *não cíclico* de ordem 4 no grupo $\mathcal{U}(3, 11)$.

Solução:

Um subgrupo *não cíclico* de ordem 4 de um grupo só pode ter, além do elemento neutro, elementos de ordem dois. Portanto, precisamos apenas achar os elementos de ordem dois em $\mathcal{U}(3, 11)$. Seja $[\overline{a}, \overline{b}]$ um tal elemento. Então

$$[\overline{a}, \overline{b}]^2 = [\overline{a}^2 + \overline{3}\overline{b}^2, \overline{2}\overline{a}\overline{b}] = [\overline{1}, \overline{0}].$$

Mas isto significa que

$$\overline{2}\overline{a}\overline{b} = \overline{0},$$

que, como $\overline{2}$ é inversível módulo 11, implica que

$$\overline{a} = \overline{0} \quad \text{ou} \quad \overline{b} = \overline{0}.$$

Quando $\overline{b} = \overline{0}$, obtemos os elementos

$$[\pm\overline{1}, \overline{0}].$$

Já $\overline{a} = \overline{0}$, nos dá

$$\overline{3}\overline{b}^2 = (\overline{5}\overline{b})^2 = \overline{1};$$

donde podemos concluir que

$$\overline{5}\overline{b} = \pm\overline{1}.$$

Levando em conta que o inverso de $\overline{5}$ em $\mathbb{Z}_{11}$ é $\overline{9}$, temos que

$$[\overline{0}, \pm\overline{9}]$$

também têm ordem dois em $U(3, 11)$. Logo, o subgrupo desejado é

$$\{[\overline{1}, \overline{0}], [\overline{10}, \overline{0}], [\overline{0}, \overline{9}], [\overline{0}, \overline{2}]\}$$

e este é o único subgrupo cíclico de ordem 4 em $\mathcal{U}(3, 11)$.

Questão 4 ()

A base rebelde no planeta Aargonar 3 interceptou a mensagem $[1553, 3997]$ enviada pelo Império Galático, indicando o membro da Aliança Rebelde que eles pretendem raptar. Surpreendentemente a mensagem foi encriptada usando o RSA com chave pública $n = 4387$ e $e = 2827$, o que permitiu que fosse facilmente decriptada. Fatore a chave e decodifique a mensagem.

Solução:

Aplicando o algoritmo de Fermat a 4387 e levando em conta que não é um quadrado perfeito, obtemos a tabela

x	$\sqrt{x^2-4387}$
67	10.1
68	15.4
69	19.34
70	22.65
71	25.57
72	28.23
73	30.69
74	33

Portanto, os fatores primos de 4387 são

$$74-33=41 \quad \text{e} \quad 74+33=107.$$

Logo,

$$\phi(4387)=40\cdot 106=4240.$$

Aplicando o algoritmo euclidiano estendido descobrimos que o inverso de 2827 módulo 4240 é 3. Decodificando obtemos

$$\begin{aligned} 1553^3 &\equiv 2130 \pmod{4387} \\ 3997^3 &\equiv 2014 \pmod{4387}. \end{aligned}$$

Mas $21-30-20-14$, que corresponde às letras LUKE.

Questão 5 ()

Sabe-se que $3^{947}\equiv 5103 \pmod{7577}$.

(a) Mostre que 7577 é primo usando o teste de Lucas.

(b) A classe $\overline{9}$ gera $U(7577)$?

Solução:

Temos que

$$7577-1=7576=2^3\cdot 947$$

e que 947 é primo. Por outro lado, de $3^{947}\equiv 5103 \pmod{7577}$ podemos concluir que

$$\begin{aligned} 3^{7576/2} &\equiv 3^{4\cdot 947}\equiv 5103^4\equiv 7576\equiv -1 && \pmod{7577} \\ 3^{7576/947} &\equiv 3^4\equiv 81 && \pmod{7577} \end{aligned}$$

Da primeira destas congruências segue imediatamente que

$$3^{7576} \equiv (3^{4\cdot 947})^2 \equiv (-1)^2 \equiv 1 \pmod{7577}.$$

Logo, pelo teste de Lucas, 7577 é primo. Os mesmos cálculos mostram que

$$9^{4\cdot 947} \equiv 3^{8\cdot 947} \equiv 3^{7576} \equiv 1 \pmod{7577};$$

de modo que $\overline{9}$ tem ordem

$$4 \cdot 947 = 3738 < 7576$$

e não pode ser gerador de $U(7577)$.

Questão 1 ()

Quando tiramos ovos de uma cesta 7 de cada vez e 27 de cada vez, restam 2 ovos e 5 ovos respectivamente. Qual a quantidade mínima de ovos que a cesta pode conter?

Solução:

Se a quantidade de ovos na cesta for x, temos o sistema de congruências

$$\begin{aligned} x &\equiv 2 \pmod 7 \\ x &\equiv 5 \pmod{27}. \end{aligned}$$

Tirando o valor de x da segunda equação, obtemos $x = 5 + 87y$. Substituindo na primeira equação:

$$5 + 27y \equiv 2 \pmod 7,$$

que equivale a

$$-y \equiv -3 \pmod 7;$$

que nos dá $y \equiv 3 \pmod 7$. Logo, $y = 3 + 7z$, donde

$$x = 5 + 27(3 + 7z) = 86 + 189z.$$

Portanto, a quantidade mínima de ovos que a cesta poderia conter é 86.

Questão 2 ()

Sabe-se que 1249 é primo e que $599^{32} \equiv 1 \pmod{1249}$.

(a) Calcule a ordem de $\overline{599}$ em $U(1249)$.

(b) Calcule o resto da divisão de $599^{15243529}$ por 1249.

Solução:

De $599^{32} \equiv 1 \pmod{1249}$ sabemos, pelo lema chave, que a ordem de $\overline{599}$ divide 16. Mas

$$\begin{aligned} 599^2 &\equiv 338 \pmod{1249} \\ 599^4 &\equiv 585 \pmod{1249} \\ 599^8 &\equiv 1248 \pmod{1249} \\ 599^{16} &\equiv 1 \pmod{1249}. \end{aligned}$$

Logo a ordem de $\overline{599}$ é 16. Dividindo 15243529 por 16, obtemos resto 9, logo

$$599^{15243529} \equiv 599^9 \equiv 599^8 \cdot 599 \equiv -599 \equiv 650 \pmod{1249};$$

de modo que o resto desejado é 650.

Questão 3 ()

Sabe-se que $7^{57} \equiv 1032 \pmod{1825}$. Determine se:

(a) 1825 é um pseudoprimo forte para a base 7;

(b) 1825 é um pseudoprimo para a base 7.

Solução:

Para começar, 1825 é composto (múltiplo de 5) e ímpar. Como $1824 = 2^5 \cdot 57$, e

$$7^{57} \equiv 1032 \neq 1,1824 \pmod{1825}$$

precisamos apenas calcular

$$\begin{aligned} 7^{2\cdot 57} &\equiv 1032^2 \equiv 1049 \neq 1824 \pmod{1825} \\ 7^{4\cdot 57} &\equiv 1049^2 \equiv 1751 \neq 1824 \pmod{1825} \\ 7^{8\cdot 57} &\equiv 1751^2 \equiv 1 \neq 1824 \pmod{1825} \\ 7^{16\cdot 57} &\equiv 1^2 \equiv 1 \neq 1824 \pmod{1825}, \end{aligned}$$

de modo que o teste forte de composição retorna *composto*. Logo, 1825 não é um pseudoprimo forte para a base 7. Contudo, segue dos cálculos acima que

$$7^{1824} \equiv 7^{32\cdot 57} \equiv 1^2 \equiv 1 \pmod{1825}.$$

Portanto, 1825 é um pseudoprimo para a base 7.

Questão 4 ()

Considere $n = 4504139$.

(a) Fatore n usando o algoritmo de Fermat.

(b) Determine o menor valor de e para o qual o par $[n, e]$ pode ser uma chave pública do RSA.

Solução:

Como $\sqrt{4504139} = 2122.295$ não é inteiro, usamos a tabela

x	$\sqrt{x^2 - n}$	Inteiro?
2123.0	54.681	não
2124.0	85.071	não
2125.0	107.17	não
2126.0	125.45	não
2127.0	141.39	não
2128.0	155.71	não
2129.0	168.83	não
2130.0	181.0	sim!

Logo os fatores são

$$x - y = 2130 - 181 = 1949 \quad \text{e} \quad x + y = 2130 - 181 = 2311.$$

Portanto,

$$\phi(n) = 1948 \cdot 2310 = 4499880,$$

que é divisível por 2, 3, 5, 7 e 11, de modo que o menor valor possível para e é 13.

Questão 5 ()

Seja $P = [\overline{a}, \overline{0}] \in \mathcal{U}(3, 17)$.

(a) Determine a de modo que P gere um subgrupo cíclico de ordem 8.

(b) Determine a de modo que P gere um subgrupo cíclico de ordem 18.

Solução:

Como

$$P^k = [\overline{a}^k, \overline{0}],$$

basta achar elementos de ordem 8 e de ordem 16 em $U(17)$. Como $U(17)$ tem ordem 16, não pode haver nenhum elemento de ordem 18 da forma especificada em $\mathcal{U}(3, 17)$. Por outro lado,

$$2^4 \equiv 16 \equiv -1 \pmod{17},$$

de modo que

$$2^8 \equiv (-1)^2 \equiv 1 \pmod{17},$$

e $\overline{2}$ tem ordem 8 em $U(17)$. Logo, se $a = 2$,

$$P = [\overline{2}, \overline{0}]$$

tem ordem 8 em $\mathcal{U}(3, 17)$.

Questão 1 (2 points)

Jullyana precisava usar seu celular pré-pago para entrar em contato com seu amigo Gabriel que está participando do programa Ciência sem Fronteiras no Canadá. Se o contato fosse feito através de mensagens de texto, cada uma das quais custaria 3 reais e cinquenta centavos, sobraria 1 real e 32 centavos em sua conta. Jullyana decidiu-se por uma ligação telefônica, cada minuto da qual custou 13 reais e 53 centavos, e sobrou-lhe 1 real e 17 centavos na conta do celular. Use o algoritmo euclidiano estendido para determinar a quantia mínima (em reais) que Jullyana podia ter na conta do seu celular.

Solução:

Seja v o valor *em centavos* que Jullyana tinha na conta do seu celular. Sabemos que, se a comunicação fosse feita por mensagens de texto, então sobraria 1 real e 32 centavos reais ao custo de 3 reais e cinquenta centavos por mensagem, de modo que

$$v = 350q + 132$$

em que q é a quantidade de mensagens de texto que trocaram entre si. Como ela optou por uma chamada telefônica, sobrou-lhe 1 real e 17 centavos ao custo de 13 reais e 53 centavos por minuto, de modo que

$$v = 1353m + 117$$

em que m representa a quantidade de minutos durante os quais Jullyana e Gabriel se falaram. Igualando as duas equações

$$350q + 132 = 1353m + 117$$

donde

$$1353m - 350q = 132 - 117 = 15.$$

Aplicando o algoritmo euclidiano estendido a 1353 e 350 temos:

restos	quocientes	x
1353	**	1
350	**	0
303	3	1
47	1	-1
21	6	7
5	2	-15
1	4	67

de modo que

$$y = \frac{1 - 67 \cdot 1353}{350} = -259$$

Logo,

$$1353 \cdot 67 - 350 \cdot 259 = 1.$$

Multiplicando esta equação por 15, obtemos

$$1353 \cdot 1005 - 350 \cdot 3885 = 15.$$

Portanto, a solução geral da equação diofantina $1353m - 350q = 15$ é dada por

$$m = 1005 - 350k \quad \text{e} \quad q = 3885 - 1353k.$$

Como a quantidade de mensagens de texto trocadas entre Jullyana e Gabriel, assim como a quantidade de minutos que eles falaram, têm que ser números positivos, devemos ter:

$$1005 - 350k > 0 \quad \text{e} \quad 3885 - 1353k > 0;$$

donde

$$k < 2,871...$$

Como k é inteiro, o maior valor possível para k é $k = 2$. Logo a quantia mínima que Jullyana poderia ter em sua conta de celular é

$$v = 1353m + 117 = 1353 * (1005 - 350 * 2) + 117 = 412782$$

isto é, impressionantes 4.127 reais e 82 centavos!

Questão 2 (2 points)
Sabe-se que $(9, 4) \in \mathcal{P}(5)$. Calcule as coordenadas de $(9, 4)^4 \otimes (-9, 4)^3$.

Solução:

Como

$$(-9, 4) = (-1, 0) \otimes (9, -4)$$

temos que

$$(9, 4)^4 \otimes (-9, 4)^3 = (9, 4)^4 \otimes (-1, 0)^3 \otimes (9, -4)^3$$

donde

$$(9, 4)^4 \otimes (-9, 4)^3 = ((9, 4) \otimes (9, -4))^3 \otimes (-1, 0)^3 \otimes (9, 4).$$

Mas $(9, -4)$ é o inverso de $(9, 4)$ em $\mathcal{P}(5)$ e $(-1, 0)^2 = (1, 0)$, de modo que

$$(9, 4)^4 \otimes (-9, 4)^3 = (-1, 0)^3 \otimes (9, 4) = (-1, 0) \otimes (9, 4) = (-9, -4).$$

Questão 3 (2 points)
No conjunto $\mathcal{G}$ dos pares de números racionais (x, y) *cuja segunda coordenada não é nula* definimos uma operação $\star$ pela regra $(x_1, y_1) \star (x_2, y_2) = (x_1 + x_2, y_1 y_2)$.

(a) Determine o elemento neutro desta operação.

(b) Quais propriedades de um grupo (abeliano) esta operação satisfaz? $\mathcal{G}$ com a operação $\star$ é um grupo (abeliano)?

Solução:

(a) Precisamos determinar um par $(x_0, y_0) \in \mathcal{G}$ tal que

$$(x_0, y_0) \star (x_1, y_1) = (x_1, y_1),$$

qualquer que seja $(x_1, y_1) \in \mathcal{G}$. Mas, pela definição de $\star$:

$$(x_0, y_0) \star (x_1, y_1) = (x_0 + x_1, y_0 y_1).$$

Para que este último par seja igual a (x_1, y_1) devemos ter que

$$x_0 + x_1 = x_1 \quad \text{e que} \quad y_0 y_1 = y_1;$$

o que só ocorre se $x_0 = 0$ e $y_0 = 1$. Portanto, o elemneto neutro desejado é $(0, 1)$.

(b) Como a soma e a multiplicação de frações é uma fração, é claro da definição de $\star$ que se

$$u_1 = (x_1, y_1) \quad \text{e} \quad u_2 = (x_2, y_2),$$

então as coordenadas de

$$u_1 \star u_2 = (x_1 + x_2, y_1 y_2)$$

são frações. Além disso, como $y_1 \neq 0$ e $y_2 \neq 0$, temos que $y_1 y_2 \neq 0$, o que nos permite concluir que $u_1 \star u_2 \in \mathcal{G}$. Em outras palavras, a operação $\star$ é fechada em $\mathcal{G}$. A comutatividade de $\star$ é consequência imediata da comutatividade das operações de soma e multiplicação de frações. Para provar a associatividade, sejam u_1 e u_2 como acima e $u_3 = (x_3, y_3)$. Então,

$$(u_1 \star u_2) \star u_3 = (x_1 + x_2, y_1 y_2) \star (x_3, y_3) = ((x_1 + x_2) + x_3, (y_1 y_2) y_3),$$

ao passo que

$$u_1 \star (u_2 \star u_3) = (x_1, y_1) \star (x_2 + x_3, y_2 y_3) \star = (x_1 + (x_2 + x_3), y_1 (y_2 y_3)).$$

Logo a igualdade entre $(u_1 \star u_2) \star u_3$ e $u_1 \star (u_2 \star u_3)$ é consequência da associatividade das operações de adição e multiplicação de frações. Finalmente, precisamos determinar se cada elemento de $\mathcal{G}$ tem inverso relativamente à operação $\star$. Para isso devemos descobrir se, para um dado $u_1 \in \mathcal{G}$, existe $u_2 \in \mathcal{G}$ tal que $u_1 \star u_2$ é igual ao elemento neutro de $\mathcal{G}$. Mas isto equivale a resolver a equação

$$(x_1 + x_2, y_1 y_2) = (0, 1);$$

da qual obtemos

$$x_2 = -x_1 \quad \text{e} \quad y_2 = 1/y_1.$$

Note que a fração $1/y_1$ sempre está bem determinada porque $y_1 \neq 0$.

(c) Do que fizemos em (b) podemos concluir que a operação $\star$, definida em $\mathcal{G}$ satisfaz todas as propriedades necessárias para garantir que $\mathcal{G}$ seja um grupo abeliano.

Note que

$$\mathcal{G} = \mathbb{Z} \times (\mathbb{Q} \setminus \{0\})$$

é um caso particular da construção de produto que estudamos na folha de Estudo Dirigido de grupos.

Questão 4 (2 points)

(a) Ache dois fatores de 1009427 pelo algoritmo de Fermat.

(b) Qual o menor número inteiro positivo n para o qual $n!$ é divisível por 253000?

Solução:

(a) Como $\sqrt{1009427} = 1004.702$ não é inteiro, precisamos construir a tabela começando da parte inteira $\sqrt{1009427}$ mais um:

x	$\sqrt{x^2 - n}$	inteiro?
1005	$24,454$	não
1006	$51,078$	não
1007	$67,985$	não
1008	$81,468$	não
1009	$93,027$	não
1010	$103,31$	não
1011	$112,67$	não
1012	$121,31$	não
1013	$129,39$	não
1014	137	sim

de modo que os fatores são

$$1014 - 137 = 877 \quad \text{e} \quad 1014 + 137 = 1151.$$

(b) Fatorando 253000 temos

$$253000 = 2^3 \cdot 5^3 \cdot 11 \cdot 23.$$

Como 23 é primo, n não pode ser menor que 23. Por outro lado, como $8 = 2^3$ e 11 são menores que 23 e 5, 10 e 15, que são múltiplos de 5, também são menores que 23, temos que

$$23! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdots 8 \cdot 9 \cdot 10 \cdot 11 \cdots 15 \cdots 23$$

é divisível por 253000.

Questão 5 (2 points)

Dado um número primo $p > 2$, defina $p^{\triangle}$ como sendo o produto de todos os primos *ímpares* positivos menores ou iguais a p. Considere a sequência de primos gerada pela seguinte regra recursiva:

$$p_1 = 5 \text{ e } p_n \text{ é o menor fator primo de } \quad p_{n-1}^{\triangle} - 2.$$

Mostre que os primos $p_1, p_2, \ldots$ gerados por esta regra são todos distintos; isto é, se $i \neq j$ então $p_i \neq p_j$.

Solução:

Suponhamos, por contradição, que existem dois primos iguais na sequência; digamos $p_i = p_k$, mas $i < k$. Neste caso caso, $p_k = p_i$ divide $p_{k-1}^{\triangle}$. Como, pela definição da sequência, p_k é o menor fator primo de $p_{k-1}^{\triangle} - 2$, então p_k tem que dividir

$$p_{k-1}^{\triangle} - (p_{k-1}^{\triangle} - 2) = 2.$$

Contudo, $p_{k-1}^{\triangle}$ é um número ímpar, de modo que $p_{k-1}^{\triangle} - 2$ também é ímpar. Mas p_k é fator deste último número, logo tem que ser ímpar também. Portanto, p_k não pode dividir 2, contradizendo o que havíamos determinado acima. A contradição ocorreu porque supusemos que existem dois primos iguais na sequência, logo isto é falso, concluindo a demonstração.

Questão 1 (2 points)
A mensagem encriptada

$$[3946, \quad 1249, \quad 3718]$$

foi interceptada pelo Templo Jedi e contém uma ameaça de morte a um de seus membros. Sabendo que a mensagem foi codificada usando o RSA com chave pública $n = 7081$ e $e = 2765$, decodifique-a e revele quem é o jedi cuja vida foi ameaçada.

Solução:

Aplicando o algoritmo de Fermat $n = 7081$ descobrimos em uma etapa que seus fatores são $p = 73$ e $q = 97$. Portanto,

$$f = (p-1)(q-1) = 6912.$$

Invertendo $e = 2765$ módulo f descobrimos que $e = 5$. Decodificando:

$$3946^5 \equiv 2630$$
$$1249^5 \equiv 1816$$
$$3718^5 \equiv 2423$$

Logo, o jedi ameaçado é QUIGON.

Questão 2 (2 points)
Calcule:

(a) a ordem de $\overline{10}$ em $\mathbb{Z}_{53}$;

(b) o resto da divisão de $31^{7449366}$ por 53.

Solução:

(a) Como 53 é primo e $52 = 2^2 \cdot 13$, segue do teorema de Fermat e do Lema Chave que a ordem de $\overline{10}$ em $\mathbb{Z}_{53}$ tem que dividir 52. Portanto, a ordem de $\overline{10}$ em $\mathbb{Z}_{53}$ tem que ser 1, 2, 4, 13, 26 ou 52. Contudo, em $\mathbb{Z}_{53}$:

$$\overline{10} \neq \overline{1};$$
$$\overline{10}^2 = \overline{100} \neq \overline{1};$$
$$\overline{10}^4 = \overline{36} \neq \overline{1};$$
$$\overline{10}^{13} = \overline{36}^3 \cdot 10 = \overline{16} \cdot 10 = \overline{1};$$

de modo que a ordem de $\overline{10}$ em $\mathbb{Z}_{53}$ é 13.

(b) Por Fermat $\overline{31}^{52} = \overline{1}$ em $\mathbb{Z}_{53}$. Como $7449366 = 143257 \cdot 52 + 2$, temos que

$$31^{7449366} \equiv (31^{52})^1 43257 \cdot 31^2 \equiv 7 \pmod{53}.$$

Portanto, o resto desejado é 7.

Questão 3 (2 points)

Sabe-se que 809 é primo e que $\overline{3}^{809} = \overline{1}$ em $\mathbb{Z}_{1619}$. Determine quais das seguintes afirmações são verdadeiras e quais são falsas, justificando cuidadosamente suas respostas.

(a) $\overline{3}$ tem ordem 809 em $U(1619)$;

(b) todos os elementos de $U(1619)$ são potências de $-\overline{3}$;

(c) $\#U(1619) < 1618$.

Solução:

(a) Verdadeiro. Pelo Lema Chave, se $\overline{a}^m = \overline{1}$ em $U(n)$, então a ordem de $\overline{a}$ divide m. Como $\overline{3}^{809} = \overline{1}$ e 809 é primo, segue-se que $\overline{3}$ tem ordem igual a um ou 809. Entretanto, $\overline{3}^1 \neq \overline{1}$ implica que $\overline{3}$ não tem ordem um em $U(1619)$; portanto, a ordem deve ser 809.

(b) Verdadeiro. Como

$$(-\overline{3})^{1618} = ((-\overline{3})^{809})^2 = (-\overline{1})^2 = \overline{1},$$

segue-se, do Lema Chave, que a ordem de $-\overline{3}$ em $U(1619)$ divide 1618. Por outro lado, $1618 = 2 \cdot 809$ e

$$(-\overline{3})^{809} = -\overline{1} \neq \overline{1}$$
$$(-\overline{3})^2 = \overline{9} \neq \overline{1},$$

de modo que resta apenas a possibilidade de que a ordem de $-\overline{3}$ seja 1618.

(c) Falso. Como vimos em (b), $-\overline{3}$ tem 1618 potências distintas em $U(1619)$, de modo que $\#U(1619) \geq 1618$.

Questão 4 (2 points)

Sabe-se que $3281 = 17 \cdot 193$ e que $3^{205} \equiv 3038 \pmod{3281}$.

(a) Determine se 3281 é um pseudoprimo forte para a base 3.

(b) Ache dois inteiros positivos entre 2 e 3280 relativamente aos quais 3281 não é pseudoprimo forte.

Solução:

(a) como 3281 é ímpar e composto, resta-nos, apenas, aplicar o teste forte de composição a 3281 na base 3. Começamos calculando

$$3281 - 1 = 3280 = 2^4 \cdot 205.$$

Como

$$r \equiv 3^{205} \equiv 3038 \not\equiv 1, 3280 \pmod{3281},$$

prosseguimos inicializando $i = 1$ e calculando o quadrado de r módulo 3281:

$$r \equiv r^2 \equiv 3038^2 \equiv 3272 \not\equiv 3280 \pmod{3281};$$

continuando, temos $i = 2$ e

$$r \equiv r^2 \equiv 3272^2 \equiv 81 \not\equiv 3280 \pmod{3281};$$

e, finalmente, $i = 3$ e

$$r \equiv r^2 \equiv 81^2 \equiv 3280 \pmod{3281};$$

donde podemos concluir que o teste forte tem como saída `inconclusivo`. Portanto, 3281 é um pseudoprimo forte para a base 3.

(b) Como todo *pseudoprimo forte* para uma base tem que ser *pseudoprimo* para aquela mesma base, basta achar duas bases b para as quais $b^{n-1} \not\equiv 1 \pmod{3281}$. Mas $b^{n-1} \equiv 1 \pmod{3281}$ implica que b é inversível módulo 3281, basta escolher b tal que $\text{mdc}(b, 3281) \neq 1$. Contudo $3281 = 17 \cdot 193$, de modo que podemos tomar $b = 17$ e $b = 193$.

Questão 5 (2 points)

Determine quantas são as bases $1 \leq b \leq 104$ para as quais 105 é um pseudoprimo.

Solução:

Como b é composto e ímpar, precisamos apenas verificar para quais valores de $2 \leq b \leq 104$ a congruência

$$b^{104} \equiv 1 \pmod{105}$$

é verificada. Mas, $105 = 3 \cdot 5 \cdot 7$, de modo que podemos reduzir o problema ao de encontrar os valores de b para os quais:

$$\begin{aligned} b^{104} &\equiv 1 \pmod{3} \\ b^{104} &\equiv 1 \pmod{5} \\ b^{104} &\equiv 1 \pmod{7}. \end{aligned}$$

Aplicando o teorema de Fermat ao primeiro primo, obtemos

$$b^{104} \equiv (b^2)^{52} \equiv 1 \pmod 3,$$

para todo inteiro b que não é divisível por 3. Fazendo o mesmo para o segundo

$$b^{104} \equiv (b^4)^{13} \equiv 1 \pmod 5,$$

para todo inteiro b que não é divisível por 5. Finalmente,

$$b^{104} \equiv (b^2) \pmod 7,$$

para todo inteiro b que não é divisível por 7. Portanto, se b não por divisível por 3, 5, nem 7, teremos

$$\begin{aligned} b^{104} &\equiv 1 \pmod 3 \\ b^{104} &\equiv 1 \pmod 5 \\ b^{104} &\equiv b^2 \pmod 7. \end{aligned}$$

Logo, 105 será um pseudoprimo para a base b sempre que:

- $b \not\equiv 0 \pmod 3$;
- $b \not\equiv 0 \pmod 5$;
- $b^2 \equiv 1 \pmod 7$.

A primeira destas congruências tem 2 soluções, a segunda 4 e a terceira apenas 2. Como 3, 5 e 7 são primos entre si, todos os sistemas da forma

$$\begin{aligned} b &\equiv \alpha \pmod 3 \\ b &\equiv \beta \pmod 5 \\ b &\equiv \gamma \pmod 7, \end{aligned}$$

com

- $\alpha = 1$ ou 2;
- $\beta = 1$, 2, 3 ou 4;
- $\gamma = 1$ ou 6

têm solução. Temos, então, $2 \cdot 4 \cdot 2 = 16$ sistemas diferentes, o que nos dá 16 bases diferentes.

Questão 1 (2 points)
Sabe-se que $\overline{2}$ tem ordem 140 em $U(355)$.

(a) Determine a quantidade de elementos de $U(355)$.

(b) Determine elementos de ordem 14 e de ordem 16 em $U(355)$.

Solução:

(a) Como a fatoração de 355 em primos é dada por $355 = 5 \cdot 71$, temos que

$$\#U(355) = \phi(355) = \phi(5 \cdot 71) = \phi(5)\phi(71) = 4 \cdot 70 = 280.$$

(b) Como $\overline{2}$ tem ordem 140 em $U(355)$, então

$$\overline{2}^{140/14} = \overline{2}^{10} = \overline{314},$$

tem ordem 14 em $U(355)$. Contudo $U(355)$ não tem nenhum elemento de ordem 16 porque, pelo teorema de Lagrange, a ordem de um elemento tem que dividir a quantidade de elementos do grupo, mas 16 não divide 280.

Questão 2 (2 points)
Sabe-se que $(\overline{0}, \overline{9})$ tem ordem dois em $\mathcal{U}(5, 101)$.

(a) Use isto para achar $\overline{a} \in \mathbb{Z}_{101}$ tal que $\overline{a}^2 = \overline{5}$.

(b) Determine um subgrupo de ordem quatro em $\mathcal{U}(5, 101)$.

Solução:

(a) Como $(\overline{0}, \overline{9})$ tem ordem dois,

$$(\overline{0}, \overline{9})^2 = (\overline{59}^2, \overline{0})$$

deve ser igual a $(\overline{1}, \overline{0})$. Logo, $\overline{5} \cdot \overline{9}^2 = \overline{1}$ em $U(101)$. Mas isto implica que $\overline{5} = \overline{a}^2$ em que $\overline{a}$ é o inverso de $\overline{9}$ em $U(101)$. Aplicando o algoritmo euclidiano estendido, obtemos $\overline{a} = \overline{45}$.

Além de $(\overline{0}, \overline{9})$, sabemos que $(\overline{-1}, \overline{0})$ tem ordem dois em $\mathcal{U}(5, 101)$. Mas,

$$(\overline{0}, \overline{9}) \otimes (\overline{-1}, \overline{0}) = (\overline{0}, \overline{-9})$$

de modo que o subgrupo desejado será

$$\{(\overline{1}, \overline{0}), (\overline{-1}, \overline{0}), (\overline{0}, \overline{9}), (\overline{0}, \overline{-9})\}.$$

Questão 3 (2 points)

Considere o primo $p = 1091$ e seja $n = 6p + 1$. Sabe-se que $2^p \equiv 4215 \pmod{n}$.

(a) Mostre que n é primo, usando o teste de Lucas.

(b) Ache um gerador para $U(n)$.

Solução:

De $2^p \equiv 4215 \pmod{n}$ obtemos

$$2^{(n-1)/3} \equiv 2^{2p} \equiv 4215^2 \equiv 4214 \pmod{n}$$
$$2^{(n-1)/2} \equiv 2^{3p} \equiv 4215^3 \equiv 6546 \pmod{n}$$
$$2^{(n-1)} \equiv (2^{3p})^2 \equiv 6546^2 \equiv 1 \pmod{n}.$$

Como

$$2^{(n-1)/p} \equiv 2^6 \equiv 264 \pmod{n},$$

podemos concluir, pelo teste de Lucas, que n é primo e que $\overline{2}$ é gerador de $U(n)$.

Questão 4 (2 points)

Uma loja pretende usar em seu site de compras online uma chave pública de RSA em que n é um número com 200 algarismos e $e = 3$. Explique porque seria fácil decifrar qualquer número de cartão de crédito encriptado com esta chave.
DICA: quantos algarismos tem um número de cartão de crédito encriptado com esta chave?

Solução:

Um número de cartão de crédito tem 16 algarismos; elevando-o ao cubo obtemos um número com, no máximo, 49 algarimos. Como n tem 200 algarimos, a encriptação do número de cartão de crédito será igual ao seu cubo e poderá ser obtida extraindo-se uma raiz cúbica.

Questão 5 (2 points)

Sabe-se que as únicas soluções das equações $u^3 = \overline{1}$ e $v^3 = \overline{18}$ em $\mathbb{Z}_{29}$ são, respectivamente, $u = \overline{1}$ e $v = \overline{14}$. Use isto para determinar todos os elementos de ordem 3 do grupo $\mathcal{P}(2, 29)$.

Solução:

Como 2 não é um resíduo quadrático módulo 29, segue-se que $\#\mathcal{P}(2, 29) = 30$, que é divisível por 3, de modo que o elemento desejado pode mesmo existir. Digamos, então, que $P = [\overline{x}, \overline{y}]$ seja um elemento de ordem 3 em $\mathcal{P}(2, 29)$. Como

$$(\overline{1}, \overline{0}) = P^3 = [\overline{6}\overline{x}\overline{y}^2 + \overline{x}^3, \overline{2}\overline{y}^3 + \overline{3}\overline{x}^2\overline{y}),$$

devemos ter que

$$\overline{6}\overline{x} \cdot \overline{y}^2 + \overline{x}^3 = \overline{1} \tag{7}$$
$$\overline{2}\overline{y}^3 + \overline{3}\overline{x}^2 \cdot \overline{y} = \overline{0}. \tag{8}$$

Da segunda equação, obtemos

$$\overline{y}(\overline{2}\overline{y}^2 + \overline{3}\overline{x}^2) = \overline{0};$$

de modo que $\overline{y} = \overline{0}$ ou

$$\overline{2}\overline{y}^2 + \overline{3}\overline{x}^2 = \overline{0}.$$

Mas, substituindo $\overline{y} = \overline{0}$ na primeira equação obtemos $\overline{x}^3 = \overline{1}$, cuja única solução é $\overline{1}$. Logo, neste caso, obtemos apenas o par $(\overline{1}, \overline{0})$, cuja ordem é um e não três. Passando ao outro caso, temos que

$$\overline{2}\overline{y}^2 = -\overline{3}\overline{x}^2. \tag{9}$$

Mas (7) pode ser escrita na forma

$$(\overline{2}\overline{y}^2)(\overline{3}\overline{x}) + \overline{x}^3 = \overline{1}.$$

Substituindo (9) nesta última equação e fazendo os devidos cancelamentos, obtemos

$$-\overline{8}\overline{x}^3 = \overline{1}.$$

Como $\overline{8}$ tem inverso $\overline{11}$ em $\mathbb{Z}_{29}$, podemos concluir que

$$\overline{x}^3 = \overline{-11} = \overline{18};$$

de modo que $\overline{x} = \overline{14}$. Substituindo isto em (9),

$$\overline{2}\overline{y}^2 = -\overline{314}^2 = -\overline{8},$$

donde $\overline{y}^2 = \overline{25}$, que equivale a dizer que

$$\overline{y} = \overline{5} \quad \text{ou} \quad \overline{y} = -\overline{5} = -\overline{24}.$$

Portanto, os elementos de ordem 3 em $\mathcal{P}(2, 29)$ são $(\overline{14}, \overline{5})$ e $(\overline{14}, \overline{24})$.

Questão 1 (2 points)
Determine todas as soluções da equação diofantina linear $9867x + 674y = 230311$ para as quais $x > 0$ e $y > 0$.

Solução:

Vamos começar aplicando o algoritmo euclidiano estendido a 986747 e 67451. Obtemos a tabela

restos	quocientes	x
9867	**	1
674	**	0
431	14	1
243	1	-1
188	1	2
55	1	-3
23	3	11
9	2	-25
5	2	61
4	1	-86
1	1	147

Portanto, $\alpha = 147$ e

$$\beta = \frac{1 - 147 \cdot 9867}{674} = -2152.$$

Logo, a solução geral da equação dada é

$$x = 230311 \cdot 147 + k \cdot 674 = 33855717 + k \cdot 674$$
$$y = -230311 \cdot 2152 - k \cdot 9867 = -495629272 - k \cdot 9867.$$

Para que $x > 0$ e $y > 0$, devemos ter que

$$33855717 + k \cdot 674 > 0 \quad \text{e} \quad -495629272 - k \cdot 9867 > 0.$$

Da primeira desigualdade obtemos $k > -50231.034$ e da segunda $k < -50230.99$. Como k tem que ser inteiro, $k = -50231$. Logo, há apenas uma solução com x e y positivo, que é obtida substituindo $k = -50231$ na solução geral, o que nos dá:

$$x = 23 \quad \text{e} \quad y = 5.$$

Questão 2 (2 points)
Ache os dois fatores primos de 166493 pelo algoritmo de Fermat.

Solução:

Como a parte inteira da raiz quadrada de 166493 é igual a 408 e $408^2 \neq 166493$, precisaremos calcular a tabela

x	$\sqrt{x^2 - n}$	$x^2 - y^2 - n$
409	28	4
410	40	7
411	49	27
412	57	2
413	63	107
414	70	3
415	75	107
416	81	2
417	86	0

Logo, $x = 417$ e $y = 86$, de modo que os fatores são

$$x - y = 417 - 86 = 331 \quad \text{e} \quad x + y = 503.$$

Questão 3 (3 points)

Determine:

(a) a ordem de 2 módulo 331;

(b) o resto da divisão de 2^{162635} por 331;

(c) um elemento de ordem 5 módulo 331.

Solução:

Como $[\sqrt{331}] = 18$, se 331 for composto, tem que ter um fator menor primo que 18. Mas os primos menores que 18 são 2, 3, 5, 7, 11, 13 e 17 e nenhum deles divide 331. Logo, 331 é primo. Portanto, pelo teorema de Fermat,

$$2^{330} \equiv 1 \pmod{331}$$

e, pelo lema chave, a ordem de 2 tem que dividir

$$330 = 2 \cdot 3 \cdot 5 \cdot 11.$$

Começando pelos divisores menores, temos que

$$\begin{aligned} 2^2 &\equiv 4 \pmod{331} \\ 2^3 &\equiv 8 \pmod{331} \\ 2^5 &\equiv 32 \pmod{331} \\ 2^6 &\equiv 64 \pmod{331} \\ 2^{10} &\equiv 31 \pmod{331} \\ 2^{11} &\equiv 62 \pmod{331} \\ 2^{15} &\equiv 330 \pmod{331}. \end{aligned}$$

Mas desta última potência segue que

$$2^{30} \equiv 330^2 \equiv (-1)^2 \equiv 1 \pmod{331}.$$

Portanto, pelo lema chave, a ordem de 2 divide 30. Como as potências acima também mostram que a ordem de 2 não é igual a nenhum divisor de 30, temos que 2 tem ordem 30 módulo 331. Como

$$162635 = 5421 \cdot 30 + 5,$$

teremos

$$2^{162635} \equiv (2^{30})^{5421} \cdot 2^5 \equiv 2^5 \equiv 32 \pmod{331}.$$

Portanto, o resto desejado é 32. Finalmente, como 2 tem ordem 30 módulo 331, então

$$(2^6)^5 \equiv 1 \pmod{331}.$$

Logo, pelo lema chave, a ordem de $2^6 \equiv 64 \pmod{331}$ divide 5. Como, 5 é primo e $64 \not\equiv 1 \pmod{331}$, temos que 64 tem ordem 5 módulo 331.

Questão 4 (3 points)

Seja $p > 1$ um primo e n um número inteiro, de modo que $3p + 1 = n^2$.

(a) Mostre que $n < 2\sqrt{p}$.

(b) Mostre que p tem que dividir $n + 1$ ou $n - 1$.

(c) Mostre que não é possível que p divida $n - 1$.

(d) Determine todos os p's que dividem $n + 1$.

Solução:

Como $p > 1$, temod que

$$n^2 = 3p + 1 < 3p + p = 4p,$$

donde $n \leq 2\sqrt{2}$. Se p dividir $n+1$, então

$$2\sqrt{p}+1 > n+1 > p,$$

de modo que

$$\sqrt{p} > \frac{p-1}{2}.$$

Mas isto implica que

$$p > \frac{(p-1)^2}{4}$$

que equivale a dizer que

$$p^2 - 6p + 1 < 0.$$

Como as raízes da equação são $3 \pm 2\sqrt{2}$ e os valores negativos de p têm que cair entre as raízes, devemos ter que

$$2 \leq p \leq 3 + 2\sqrt{2} = 5.8284...$$

Portanto, $p = 2$, 3 ou 5, donde $3p+1 = 7$, 10 ou 16, e este último é o único para o qual obtemos um quadrado perfeito. Argumentando, de maneira semelhante, quando p divide $n-1$, temos que

$$2\sqrt{p} - 1 > n - 1 > p,$$

donde

$$\sqrt{p} > \frac{p+1}{2},$$

que equivale a

$$0 > p^2 - 2p + 1 = (p-1)^2,$$

que não tem solução.

Justifique cuidadosamente todas as suas respostas.

Questão 1 (4 points)

Sabe-se que $p = 491$ e $q = 8 \cdot p + 1 = 3929$ são ambos primos e que $2^p \equiv 226 \pmod{q}$.

(a) Calcule a ordem de $\overline{2}$ em $\mathbb{Z}_q$.

(b) Dê exemplos de elementos de ordens 4 e p em $\mathbb{Z}_q$.

(c) Calcule o inverso de $\overline{2}^p$ em $\mathbb{Z}_q$.

(d) Determine um elemento $\overline{a} \neq \pm\overline{1}$ em $\mathbb{Z}_p$, que seja solução da equação $\overline{a}^{15!} = \overline{1}$.

Solução:

Como q é primo e $q-1 = 8 \cdot p$, a ordem de $\overline{2}$ em $\mathbb{Z}_q$ só pode ser 2, 4, 8, p, $2p$, $4p$ ou $8p$. Já sabemos, por $2^p \equiv 226 \pmod{q}$, que não pode ser p. Como $2^8 = 256 < q$, a ordem de $\overline{2}$ n ao pode ser nenhum divisor de 8. Por outro lado,

$$2^{2p} \equiv 226^2 \equiv 3928 \equiv -1 \pmod{q},$$

donde

$$2^{4p} \equiv (2^{2p})^2 \equiv (-1)^2 \equiv 1 \pmod{q}.$$

Logo, a ordem de $\overline{2}$ divide $4p$. Como já vimos que não é igual a 2, 4, p e $2p$, a ordem de $\overline{2}$ tem que ser $4p$. Portanto, $\overline{2}^p = \overline{226}$ tem ordem 4 e $\overline{2^4} = \overline{16}$ tem ordem p. Além disso, temos de

$$(\overline{2^p})^3 \cdot \overline{2^p} = (\overline{2^p})^4 = \overline{1}$$

que

$$(\overline{2^p})^3 = \overline{226}^3 = \overline{3703}$$

é o inverso de $\overline{2}^p$. Finalmente, como os únicos divisores de 15! que dividem $q - 1 = 8 \cdot p$ são 2, 4 e 8, então as únicas soluções possíveis para a equação dada são elementos com estas ordens em $\mathbb{Z}_q$. Mas já sabemos que $\overline{2}^p = \overline{226}$ tem ordem 4, logo é uma solução diferente de $\pm\overline{1}$ para a equação dada.

Questão 2 (3 points)

Determine:

(a) o resíduo de 13^{21} módulo 85, pelo teorema chinês do resto;

(b) se 85 é pseudoprimo forte na base 13;

(c) se 85 é pseudoprimo na base 13.

Solução:

Fatorando 85 obtemos $85 = 5 \cdot 17$. Como $13 \equiv 3 \pmod 5$ e, pelo teorema de Fermat, $3^4 \equiv 1 \pmod 5$, temos que

$$13^{21} \equiv 3^{21} \equiv (3^4)^5 \cdot 3 \equiv 3 \pmod 5.$$

Por outro lado, o teorema de Fermat também nos dá $13^{16} \equiv 1 \pmod{17}$, donde

$$13^{21} \equiv 13^{16} \cdot 13^5 \equiv 13^5 \equiv (-4)^5 \equiv -32^2 \equiv -(-2)^2 \equiv -4 \equiv 13 \pmod{17}.$$

Portanto, se r for o resíduo de 13^{21} módulo 85, então $0 \leq r \leq 84$ satisfaz o sistema

$$\begin{aligned} r &\equiv 3 \pmod 5 \\ r &\equiv 13 \pmod{17}. \end{aligned}$$

Aplicando o algoritmo chinês, temos da segunda congruência que

$$r = 13 + 17k.$$

Substituindo isto na primeira congruência:

$$13 + 17k \equiv 3 \pmod 5,$$

que equivale a

$$17k \equiv 0 \pmod 5;$$

donde $k \equiv 0 \pmod 5$. Portanto,

$$r = 13 + 17k = 13 + 85\ell$$

de modo que $r = 13$. Como já sabemos que 85 é ímpar e composto, falta apenas aplicar o teste forte para descobrir se é pseudoprimo forte na base 13. Mas,

$$85 - 1 = 84 = 2^2 \cdot 21.$$

Como já sabemos que $13^{21} \equiv 13 \pmod{85}$, falta apenas determinar

$$13^{2 \cdot 21} \equiv 13^2 \equiv 84 \pmod{85},$$

de modo que 85 é mesmo pseudoprimo forte na base 13. Como todo pseudoprimo forte é pseudoprimo para a mesma base, 85 também é pseudoprimo na base 13.

Questão 3 (3 points)

Determine:

(a) todos os elementos de $\mathcal{P}(3, 13)$;

(b) um gerador de $\mathcal{P}(3, 13)$;

(c) um elemento de ordem dois em $\mathcal{P}(3, 13)$.

Solução:

Os quadrados módulo 13 são

$$\begin{array}{cccccccc} x & \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} & \overline{6} \\ x^2 & \overline{0} & \overline{1} & \overline{4} & \overline{9} & \overline{3} & \overline{12} & \overline{10} \end{array}$$

e as classes da forma $\overline{1} + \overline{3}y^2$ são

$$\begin{array}{cccccccc} y & \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} & \overline{6} \\ \overline{1} + \overline{3}y^2 & \overline{1} & \overline{4} & \overline{0} & \overline{2} & \overline{10} & \overline{11} & \overline{5} \end{array}$$

Comparando as duas tabelas e levando em conta que se $[\overline{a}, \overline{b}]$ é solução de $x^2 - \overline{3}y^2 = \overline{1}$, então o mesmo vale para $[\pm\overline{a}, \pm\overline{b}]$, chegamos aos seguintes pares

$$[\overline{1}, \overline{0}], [\overline{12}, \overline{0}], [\overline{0}, \overline{2}], [\overline{0}, \overline{11}], [\overline{2}, \overline{1}], [\overline{11}, \overline{1}], [\overline{2}, \overline{12}], [\overline{11}, \overline{12}], [\overline{6}, \overline{4}], [\overline{6}, \overline{9}], [\overline{7}, \overline{4}], [\overline{7}, \overline{9}].$$

Destes elementos,

$$[\overline{11}, \overline{1}], \quad [\overline{11}, \overline{12}], \quad [\overline{2}, \overline{1}], \quad \text{e} \quad [\overline{2}, \overline{12}]$$

têm ordem 12 e, portanto, são geradores. Vou verificar isto para um deles, por exemplo:

$$\begin{aligned} [\overline{2}, \overline{1}]^2 &= [\overline{7}, \overline{4}] \\ [\overline{2}, \overline{1}]^3 &= [\overline{0}, \overline{2}] \\ [\overline{2}, \overline{1}]^6 &= [\overline{12}, \overline{0}] \\ [\overline{2}, \overline{1}]^{12} &= [\overline{1}, \overline{0}], \end{aligned}$$

para ter certeza que a ordem é mesmo 12 precisamos ainda calcular

$$[\overline{2}, \overline{1}]^4 = [\overline{6}, \overline{4}]$$

para ter certeza que a ordem não pode ser 4. Finalmente, o elemento de ordem dois é $[\overline{12}, \overline{0}]$.

Justifique cuidadosamente todas as suas respostas.

Questão 1 (4 points)
Considere o grupo $\mathcal{U}(2,7)$.

(a) Determine o subconjunto S de $\mathcal{U}(2,7)$ formado por todos os elementos cuja segunda coordenada é $\overline{0}$.

(b) Mostre que S é um subgrupo de $\mathcal{U}(2,7)$.

(c) Este subgrupo é cíclico? Se for, ache um gerador.

(d) Ache um elemento de ordem 8 em $\mathcal{U}(2,7)$, sabendo-se que existe um conjunto T, cujos elementos têm todos ordem seis, tal que

$$\mathcal{U}(2,7) = \{P \otimes Q \,|\, P \in S \text{ e } \ Q \in T\}.$$

Solução:

Pela definição de $\mathcal{U}(2,7)$, um par $[\overline{a},\overline{0}]$ pertença a este grupo desde que

$$\overline{a}^2 - 2\overline{0}^2 = \overline{a}^2$$

seja inversível módulo 7. Portanto, os elementos desejados são

$$[\overline{1},\overline{0}],\ [\overline{2},\overline{0}],\ [\overline{3},\overline{0}],\ [\overline{4},\overline{0}],\ [\overline{5},\overline{0}],\ [\overline{6},\overline{0}].$$

Como

$$[\overline{a},\overline{0}] \otimes [\overline{b},\overline{0}] = [\overline{ab},\overline{0}]$$

o produto de quaisquer dois elementos de S pertence a S. Além disso, S contem o elemento neutro $[\overline{1},\overline{0}]$ e o inverso de $[\overline{a},\overline{0}]$ é $[\overline{a'},\overline{0}]$, em que $\overline{a'}$ é o inverso de $\overline{a}$ em $\mathbb{Z}_7$. Portanto, S é um subgrupo de $\mathcal{U}(2,7)$. Este subrupo é cíclico, porque $[\overline{3},\overline{0}]$ e $[\overline{5},\overline{0}]$ têm ordem seis. Finalmente, se $P \in \mathcal{U}(2,7)$, então existe um elemento $Q_1 \in S$ e um elemento $Q_2 \in T$, tal que $P = Q_1 \otimes Q_2$. Como S tem ordem 6, então a ordem de qualquer elemento de S divide 6. Logo,

$$P^6 = (Q_1 \otimes Q_2)^6 = Q_1^6 \otimes Q_2^6 = [\overline{1},\overline{0}] \otimes [\overline{1},\overline{0}] = [\overline{1},\overline{0}],$$

pois $Q_2 \in T$ e todos os elementos de T têm ordem seis. Logo, pelo lema chave, a ordem de todo elemento de $\mathcal{U}(2,7)$ divide 6, de modo que não pode haver elementos de ordem 8 neste grupo.

Questão 2 (3 points)

Sabe-se que a mensagem $6963 - 690$ foi encriptada usando o sistema RSA com chave pública $n = 14803$ e $d = 9707$.

(a) fatore n usando o algoritmo de Fermat;

(b) calcule $\phi(n)$ e e;

(c) decodifique a mensagem.

Solução:

Em um passo o algoritmo de Fermat descobre que os fatores de n são 131 e 113. Logo,

$$f = \phi(n) = (p-1)(q-1) = 112 \cdot 130 = 1560.$$

Aplicando o algoritmo euclidiano estendido a f e e, obtemos

restos	quocientes	x
14560	**	1
9707	**	0
4853	1	1
1	2	-2.

Logo,

$$d = \frac{1 - (-2) \cdot 14560}{9707} = 3.$$

Finalmente, decodificando, temos

$$6963^3 \equiv 271 \pmod{14803}$$
$$690^3 \equiv 824 \pmod{14803},$$

que corresponde à palavra `RIO`.

Questão 3 (3 points)

Seja $n = 8 \cdot 479 + 1$. Sabendo-se que $\overline{3}^{479} = \overline{19}$ em $\mathbb{Z}_n$, determine:

(a) se n é primo, pelo teste de Lucas;

(b) a ordem de $\overline{3}$ em $U(n)$;

(c) dois geradores de $U(n)$.

Solução:

Fazendo os cálculos em $\mathbb{Z}_n$, verificamos que

$$\overline{3}^{2 \cdot 479} = \overline{19}^2 = \overline{361}$$
$$\overline{3}^{4 \cdot 479} = \overline{61}^2 = \overline{3832}$$
$$\overline{3}^{8 \cdot 479} = \overline{61}^2 = \overline{1}.$$

Logo,

$$\overline{3}^{8\cdot 479} = \overline{3}^{8\cdot 479} = \overline{1}.$$

Por outro lado,

$$\overline{3}^{(n-1)/2} = \overline{3}^{4\cdot 479} = \overline{3832} \neq \overline{1}$$
$$\overline{3}^{(n-1)/479} = \overline{3}^{8} = \overline{2728} \neq \overline{1}.$$

Portanto, n é primo pelo teste de Lucas. Mas o teste de Lucas consiste em mostrar que $\overline{3}$ tem ordem $8 \cdot 479$. Finalmente, como n é primo,

$$\#U(n) = n - 1 = 8 \cdot 479.$$

Logo, $\overline{3}$ e qualquer potência de $\overline{3}$ de expoente primo com $8 \cdot 479$ gera $U(n)$; em particular, $\overline{3}^3$, $\overline{3}^5$, $\overline{3}^7$ são geradores de $U(n)$.