NÚMEROS INTEIROS E CRIPTOGRAFIA – UFRJ

GABARITO LISTA 6: ALGORITMO CHINÊS DO RESTO

1. Ver gabarito das questões do livro.

2. Aplique o Algoritmo de Fermat para encontrar $999367 = 911 \cdot 1097$. Como 911 e 1097 são primos, pelo Teorema de Fermat:
$$5^{150154} \equiv (5^{910})^{165}.5^4 \equiv 625 \pmod{911}$$
e
$$5^{150154} \equiv (5^{1096})^{137}.5^2 \equiv 25 \pmod{1097}$$
Da primeira congruência, concluímos que $5^{150154} = 911q_1 + 625$, para algum $q_1 \in \mathbb{Z}$. Aplique o Algoritmo Euclidiano Extendido para encontar -289, o inverso modular de $\overline{911}$ em $\mathbb{Z}_{1097}$. Como $-289 \equiv 808 \pmod{1097}$, têm-se:
$$5^{150154} \equiv 911q_1 + 625 \equiv 25 \pmod{1097}$$
isto é,
$$911q_1 \equiv -600 \equiv 497 \pmod{1097}$$
Multiplique por 808 para encontrar $q_1 \equiv 401576 \equiv 74 \pmod{1097}$. Logo, $q_1 = 1097q_2 + 74$, para algum $q_2 \in \mathbb{Z}$. Substitua q_1 em nossa equação inicial:
$$5^{150154} = 911(1097q_2 + 74) + 625 = 999367q_2 + 68039$$
Portanto, o resto da divisão de 5^{150154} por 999367 é 68039.

3. Vamos mostrar que $n^3 - n \equiv 0 \pmod 2$ e $n^3 - n \equiv 0 \pmod 3$. Pelo Teorema Chinês dos Restos, vem imediatamente que $n^3 - n \equiv 0 \pmod 6$. Ao aplicarmos o Teorema de Fermat vemos que:
$$n^3 - n \equiv n^2 n - n \equiv n - n \equiv 0 \pmod 3,$$
sempre que $n \not\equiv 0 \pmod 3$. Contudo, se $n \equiv 0 \pmod 3$, então $n^3 \equiv 0 \pmod 3$, de modo que $n^3 - n \equiv 0 \pmod 3$ também é verdade quando $n \equiv 0 \pmod 3$. Portanto, $n^3 - n \equiv 0 \pmod 3$ para todo inteiro n. Por outro lado, como a diferença entre dois números ímpares ou dois números pares é sempre par, então $n^3 - n$ é par. Logo, $n^3 - n$ é divisível por 2 e por 3, qualquer que seja $n \in \mathbb{Z}$. Como 2 e 3 são primos entre si, podemos concluir que $6 = 2 \cdot 3$ divide $n^3 - n$, provando o que queríamos.

4. Seja X o número procurado. Sabe-se que $X \equiv 3 \pmod 9$, $X \equiv 4 \pmod{11}$ e $X \equiv 2 \pmod 5$. Os inteiros X que verificam a primeira congruência são da forma $X = 9q_1 + 3$, para algum $q_1 \in \mathbb{Z}$. Dentre estes, os que são solução da segunda congruência tem escrita na forma
$$X \equiv 9q_1 + 3 \equiv 4 \pmod{11}$$
isto é, $9q_1 \equiv 1 \pmod{11}$. Como 5 é o inverso multiplicativo de 9 no módulo 11, então $q_1 \equiv 5 \pmod{11}$. Logo, $q_1 = 11q_2 + 5$, para algum $q_2 \in \mathbb{Z}$. Substituindo na primeira equação, $X = 9(11q_2 + 5) + 3 = 99q_2 + 48$. Assim, da última congruência,
$$X \equiv 99q_2 + 48 \equiv 2 \pmod 5$$
vem que $99q_2 \equiv -46 \equiv 4 \pmod 5$ e, como 4 é o inverso de 99 módulo 5, $q_2 \equiv 16 \equiv 1 \pmod 5$. Portanto, $q_2 = 5q_3 + 1$, para algum $q_3 \in \mathbb{Z}$. Substitua na nossa última expressão para obter:
$$X = 99(5q_3 + 1) + 48 = 495q_3 + 147$$
Em particular, quando $q_3 = 0$, temos o menor número satisfazendo as condições do enunciado. Portanto, $X = 147$.

5. Inicialmente, repare que $30 = 2 \cdot 3 \cdot 5$. Para simplificar a notação, defina $Q = 2^{450!} + 3^{890!} + 15^{900!}$. Como $2^{450!} \equiv 0 \pmod 2$ (pois $2^{450!}$ é múltiplo de 2), $3^{890!} \equiv 1 \pmod 2$ (pelo Teorema de Fermat) e $15^{900!} \equiv 1 \pmod 2$ (também pelo Teorema de Fermat), então $Q \equiv 2 \equiv 0 \pmod 2$. Além disso, $2^{450!} \equiv 1 \pmod 3$ (pelo Teorema de Fermat), $3^{890!} \equiv 0 \pmod 3$ (pois $3^{890!}$ é múltiplo de 3) e $15^{900!} \equiv 0 \pmod 3$ (já que $15^{900!}$ é múltiplo de 3). Portanto, $Q \equiv 1 \pmod 3$. Note que $2^{450!} \equiv 1 \pmod 5$ (pelo Teorema de Fermat), $3^{890!} \equiv 1 \pmod 5$ (segue do Teorema de Fermat) e $15^{900!} \equiv 0 \pmod 5$ (pois $15^{900!}$ é múltiplo de 5). Logo, $Q \equiv 2 \pmod 5$. Desta forma, obtemos o seguinte sistema de congruências:
$$\begin{cases} Q = 2^{450!} + 3^{890!} + 15^{900!} \equiv 0 \pmod 2 \\ Q = 2^{450!} + 3^{890!} + 15^{900!} \equiv 1 \pmod 3 \\ Q = 2^{450!} + 3^{890!} + 15^{900!} \equiv 2 \pmod 5 \end{cases}$$
Isto mostra que $Q = 2k_1$, para algum $k_1 \in \mathbb{Z}$. Da segunda congruência, vem que $Q \equiv 2k_1 \equiv 1 \pmod 3$. Como 2 é o inverso multiplicativo de 2 módulo 3, segue-se que $k_1 \equiv 2 \pmod 3$, isto é, $k_1 = 3k_2 + 2$, para algum $k_2 \in \mathbb{Z}$. Substituindo na primeira equação:
$$Q = 2k_1 = 2(3k_2 + 2) = 6k_2 + 4$$
Desta última equação e da terceira congruência concluímos que $Q \equiv 6k_2 + 4 \equiv 2 \pmod 5$. Ou seja, $6k_2 \equiv k_2 \equiv -2 \equiv 3 \pmod 5$. Logo, $k_2 = 5k_3 + 3$, para algum $k_3 \in \mathbb{Z}$. Finalmente, substitua a expressão de k_3 na última equação:
$$Q = 6k_2 + 4 = 6(5k_3 + 3) + 4 = 30k_3 + 22$$

Portanto, o resto da divisão de $2^{450!} + 3^{890!} + 15^{900!}$ por 30 é 22.

6. (a) Inicialmente, repare que $55 = 5 \cdot 11$. Além disso, $\overline{7}$ tem ordem 4 em $\mathbb{Z}_5$ e 10 em $\mathbb{Z}_{11}$. Queremos determinar o menor inteiro positivo k tal que

$$7^k \equiv 1 \pmod 5$$
$$7^k \equiv 1 \pmod{11}$$

Logo, $k = \text{mmc}(4, 10) = 20$.

(b) Temos que $143 = 11 \cdot 13$. Como $\overline{4}$ tem ordem 5 em $\mathbb{Z}_{11}$ e ordem 6 em $\mathbb{Z}_{13}$, a ordem de $\overline{4}$ em $\mathbb{Z}_{143}$ é $\text{mmc}(5, 6) = 30$.

(c) Como $45 = 3^2.5$ e $\overline{2}$ tem ordem 1 e 4 em $\mathbb{Z}_3$ e $\mathbb{Z}_5$, respectivamente, a ordem de $\overline{2}$ em $\mathbb{Z}_{45}$ é $\text{mmc}(1, 4) = 4$.

7. 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:

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

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

$$r \equiv 5 \pmod{13}$$
$$r \equiv 1 \pmod{217}.$$

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.

Para determinar se 2821 é pseudoprimo forte para a base 2 precisamos aplicar o teste de composição forte 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:

$$r_1 \equiv 2^{705} \equiv 2605 \pmod{2821}$$
$$r_2 \equiv 2^{2\cdot 705} \equiv 2605^2 \equiv 1520 \pmod{2821}$$

Como $r_1 \neq 1, 2820$ e $r_2 \neq 2820$ então o teste de composição forte 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.

8. 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

$$r_0 \equiv 6^{27} \pmod{7}$$
$$r_0 \equiv 6^{27} \pmod{31}.$$

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

$$r_0 \equiv 6 \pmod{7}$$
$$r_0 \equiv 30 \pmod{31},$$

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

$$r_0 \equiv 6 \equiv -1 \pmod 7$$
$$r_0 \equiv 30 \equiv -1 \pmod{31},$$

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.

9. (a) Usando o teorema de Fermat, temos que:

$$11^{77} \equiv 11 \equiv 1 \pmod 5$$
$$11^{77} \equiv 11^1 3 \equiv 2^6 \cdot 11 \equiv 7 \pmod{17}$$
$$11^{77} \equiv 11^{21} \equiv (11^6)^3 \cdot 11^3 \equiv 9^3 \cdot 11^3 \equiv 17 \pmod{29}.$$

Isto nos dá o sistema de congruências

$$r \equiv 1 \pmod 5$$
$$r \equiv 7 \pmod{17}$$
$$r \equiv 17 \pmod{29}.$$

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.
(b) Precisamos aplicar o teste forte de composição 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.
(c) Como $n - 1 = 2^5 \cdot 77$ e

$$11^{77\cdot 2^4} \equiv 1 \pmod n$$

temos que

$$11^{77\cdot 2^5} \equiv (11^{77\cdot 2^4})^2 \equiv 1^2 \equiv 1 \pmod n;$$

de modo que 2465 é pseudoprimo para a base 11.

10. 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.