NÚMEROS INTEIROS E CRIPTOGRAFIA – UFRJ

GABARITO LISTA 4: 0 TEOREMA DE FERMAT E APLICAÇÕES

1. Ver gabarito das questões do livro.

2. (a) Queremos determinar o menor inteiro positivo k tal que $\overline{5}^{96} = \overline{1}$ em $\mathbb{Z}_{97}$. Como é dito que existem 96 potências distintas de $\overline{5}$ em $\mathbb{Z}_{97}$, podemos concluir que a primeira repetição nas potências ocorre em $\overline{5}^{96}$. Por outro lado, $\overline{5}$ é inversível em $\mathbb{Z}_{97}$, de modo que a repetição ocorre quando a potência dá $\overline{1}$. Logo, a ordem de $\overline{5}$ em $\mathbb{Z}_{97}$ é 96.

   (b) Sabemos, pelo teorema de Fermat, que se $\overline{a} \in U(97)$, então $\overline{a}^{96} = \overline{1}$; donde, pelo lema chave, a ordem de $\overline{a}$ tem que dividir 96. Como 5 não divide 96, não temos nenhum elemento de ordem 5 em $\mathbb{Z}_{97}$.

   (c) Aplicando o resultado do item (a), temos
   $$5^{1185123} \equiv (5^{96})^{12345}.5^3 \equiv 5^3 \equiv 28 \pmod{97}$$
   Portanto, o resto da divisão de $5^{1185123}$ por 97 é 28.

3. (a) Novamente, pelo Teorema de Fermat, cada parcela da soma deixará resto 1 na divisão por p. Como temos $p-1$ parcelas, basta somá-las para concluir que $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv p-1 \pmod{p}$.

   (b) Se $p > 0$ for um primo ímpar, então $p+1$ é um número par maior que dois e, portanto, composto. Isto é, $p+1 = 2 \cdot b$, em que $2 \leq b \leq p$. Se $b > 2$, então $2b$ é fator de $p!$, pois 2 e b aparecem entre os números que multiplicamos para obter $p!$. Portanto,
   $$p! = 1 \cdot 2 \cdots b \cdots p = (p+1)q,$$
   para algum inteiro positivo q. Assim,
   $$2^{p!} \equiv (2^{p+1})^q \equiv 1^q \equiv 1 \pmod{2^{p+1}-1};$$
   donde
   $$2^{p!} - 1 \equiv 1 - 1 \equiv 0 \pmod{2^{p+1}-1}.$$
   Contudo, para fazer esta conta supusemos que p é ímpar e que $p+1 = sb$ com $b > 2$. Resta-nos analisar os casos em que $p = 2$ e em que $p+1 = 3$. Se $p = 2$, então $2^{p+1} - 1 = 7$, donde
   $$2^{2!} - 1 = 4 - 1 \equiv 3 \pmod{7}.$$

Por outro lado, se $p+1=4$, então $p=3$, de modo que $2^{p+1}-1=15$. Neste caso,

$$2^{p!}-1 \equiv 2^6-1 \equiv 63 \equiv 3 \pmod{15}.$$

Logo, o resto de $2^{p!}-1$ é zero quando o primo $p>3$ e é 3 quando $p=2$ ou $p=3$.

4. Como p é primo, utilizando o Teorema de Fermat, podemos reescrever $2x+x^p+x^{p!} \equiv 1 \pmod{p}$ da seguinte forma:

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

Isto é, $3x \equiv 0 \pmod{p}$. Conclui-se que 3 é o único primo para o qual temos $x \not\equiv 0 \pmod{p}$ solução da congruência. De fato, $3x \equiv 0 \pmod{3}$ para todo $x \in \mathbb{Z}$. Se p é um primo diferente de 3, $\text{mdc}(3,p)=1$, o que mostra que 3 possui inverso no módulo p. Logo, $3x \equiv x \equiv 0 \pmod{p}$, pois o inverso de 3 multiplicado por zero é zero. Esta última congruência nos mostra que se p é um primo diferente de 3, a solução da congruência será sempre $x \equiv 0 \pmod{p}$.

5. Como a ordem de 4 módulo 53 é 26 e $11236 = 432 \cdot 26 + 4$, temos que

$$4^{11236n}-2^{4n} \equiv 4^{432\cdot 26n+4n}-4^{4n} \equiv (4^{26})^{432n}\cdot 4^{4n}-4^{4n} \equiv 0 \pmod{53}.$$

6. Se $p>3$, então, por Fermat,

$$3^{2p}+2^{p-1}+1 \equiv (3^p)^2+2^{p-1}+1 \equiv 3^2+1+1 \equiv 11 \pmod{p}.$$

Como é dado que $3^{2p}+2^{p-1}+1 \equiv 0 \pmod{p}$, deveremos ter que $p=11$. Mas ainda falta testar o que acontece com $p=2$ e $p=3$. No primeiro caso,

$$3^{2p}+2^{p-1}+1 \equiv 3^4+0+1 \equiv 1^4+1 \equiv 0 \pmod{2}$$

e, no segundo caso,

$$3^{2p}+2^{p-1}+1 \equiv 0+2^2+1 \equiv 4+1 \equiv 2 \pmod{3}.$$

Logo, os primos desejados são $p=2$ e $p=11$.

7. Como 17 não divide 46, a única solução possível é $x \equiv 1 \pmod{47}$.

8. Os elementos são $\overline{3}, \overline{5}, \overline{6}, \overline{7}, \overline{10}, \overline{11}, \overline{12}$ e $\overline{14}$. Basta achar um deles. Por exemplo, como $\overline{3}$ tem ordem 16, então $\overline{3}^m$ também terá ordem 16 para todo m primo com 16. De fato, se k for a ordem de $\overline{3}^m$, então

$$\overline{3}^{km} = (\overline{3}^m)^k = \overline{1},$$

de modo que, pelo lema chave, 16 divide km. Como $\text{mdc}(m, 16) = 1$ por hipótese, então 16 divide k. Portanto, o menor valor de k para o qual vale a equação acima é $k = 16$. Logo,

$$\begin{aligned}
\overline{3}^3 &= \overline{10} \\
\overline{3}^5 &= \overline{5} \\
\overline{3}^7 &= \overline{11} \\
\overline{3}^9 &= \overline{14} \\
\overline{3}^{11} &= \overline{7} \\
\overline{3}^{13} &= \overline{12} \\
\overline{3}^{15} &= \overline{6}
\end{aligned}$$

têm todos ordem 16. Para resolver a congruência, note que, dos cálculos acima temos

$$\overline{7}^x = \overline{3}^{11x} = \overline{6} = \overline{3}^{15};$$

donde

$$\overline{3}^{11x-15} = \overline{1}.$$

Portanto, pelo lema chave, a ordem de $\overline{3}$ (que é 16) tem que dividir $11x - 15$. Em outras palavras,

$$11x \equiv 15 \pmod{16},$$

de modo que $x \equiv 6 \pmod{16}$.

9. Vou fazer o caso $M(29)$ e dar a resposta dos outros. Pelo método de Fermat, os fatores primos de $M(29)$ têm que ser da forma $2 \cdot 29 \cdot k + 1$, com $k \geq 1$. Vou verificar qual destes fatores efetivamente divide $M(29)$. Lembre-se que só adianta testar os que forem primos. Os três primeiros números da forma $2 \cdot 29 \cdot k + 1$ são 59, 117 e 175. O primeiro é primo mas não divide $M(29)$, os outros dois são compostos (múltiplos de 3 e de 5, respectivamente. O primeiro fator primo obtido é 233, que corresponde a $k = 4$.

   No caso de $M(83)$ o fator é 167 ($k = 1$). Para mostrar que $M(7)$ é primo é preciso verificar que não tem fatores menores que sua raiz. Como os fatores têm que ser da forma $2 \cdot 7 \cdot k + 1$, precisamos verificar que estes números não são fatores até

$$14 \cdot k + 1 \leq [2^{7/2}] = 11,$$

o que nos dá

$$k \leq \frac{10}{14} < 1,$$

o que prova que $M(7)$ não pode ter fatores próprios.

10. (a) Como $\overline{10}^p = \overline{1}$ em $U(q)$ e p é primo, temos, pelo lema chave, que a ordem de $\overline{10}$ é igual a p.
(b) Por Fermat, $\overline{10}^{q-1} = \overline{1}$ em $U(q)$. Logo, pelo lema chave, p tem que dividir $q-1$. Como $q-1$ é par e p é ímpar, o produto $2p$ deve dividir $q-1$. Logo, $q-1 = 2kp$.
(c) Tomando $p = 5$, a fórmula nos dá que os divisores de $10^p - 1$, maiores que 3, têm que ser da forma $q = 10k + 1$. Como

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

todos os divisores primos de $10^5 - 1$, maiores que 3, dividem 11111, podemos usar a fórmula para encontrar estes fatores. Dos três primeiros divisores, 11 e 31 são primos, mas não dividem 11111; o primeiro fator primo é 41. O cofator de 41 em 11111 é 271. Como qualquer fator primo de 271 divide 11111, seus fatores também podem ser encontrados usando a fórmula $10k + 1$. Note que já sabemos que k tem que ser maior que 4 ou o fator já teria sido encontrado na busca anterior. Como

$$10k + 1 \leq [\sqrt{271}] = 16,$$

segue-se que $k < 15/10 = 1.5$, de modo que 271 tem que ser primo.

Se você encontrar algum erro no gabarito, por favor comunique ao professor através do endereço `collier@dcc.ufrj.br`. Qualquer dúvida entre em contato com os monitores via Facebook. As aulas de monitoria serão nas segundas-feiras 13h-15h