NÚMEROS INTEIROS E CRIPTOGRAFIA – UFRJ

GABARITO LISTA 3: ARITMÉTICA MODULAR

1. Ver gabarito das questões do livro.

2. Basta calcular o resto de $3^{227}+1$ pelas potências de 2 até achar uma para a qual o resto é não nulo. Faremos isto usando congruência módulo a potência de 2. Assim,
   - $3^{227}+1 \equiv 1^{227}+1 \equiv 2 \equiv 0 \pmod 2$, pois $3 \equiv 1 \pmod 2$;
   - $3^{227}+1 \equiv (-1)^{227}+1 \equiv -1+1 \equiv 0 \pmod 2$, pois $4 \equiv -1 \pmod 4$ e 227 é ímpar;
   - $3^{227}+1 \equiv 3 \cdot 9^{113}+1 \equiv 3+2 \equiv 5 \pmod 2$, pois $9 \equiv 1 \pmod 8$.

   Como $3^{227}+1$ seria divisível por 8 se fosse divisível por qualquer potência de 2 maior que 8, podemos concluir que a maior potência de 2 que divide $3^{227}+1$ é $2^2 = 4$.

3. (a) As potências distintas de 97 módulo 233 são:

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

   já que $\overline{97}^8 = \overline{1}$.

   (b) Como $97^8 \equiv \overline{1} \pmod{233}$, precisamos calcular o resto da divisão de 234111 por 8, que dá 7 (e quociente 29263). Logo

$$97^{234111} \equiv (97^8)^{29263} \cdot 97^7 \equiv 1^{29263} \cdot 97^7 \equiv 221 \pmod{233}.$$

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

4. (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.

   (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,

$$7^{25^{100}} \equiv 7^{11} \equiv 85 \pmod{113}.$$

5. (a) Como

$$2^{16} \equiv 2^{2^4} \equiv -1 \pmod{F(4)}$$

e como 2^4 divide $2^{67!}$, temos que

$$2^{2^{67!}} \equiv (2^{2^4})^{2^{67!}-16} \equiv (-1)^{2^{67!}-16} \equiv 1 \pmod{F(4)}.$$

Sabemos, pelo teorema de Fermat, que $3^{30} \equiv 1 \pmod{31}$. Como $2^5 \equiv 2 \pmod{30}$ e 1024 deixa resto 4 na divisão por 2, temos que

$$2^{1024} \equiv 2^4 \equiv 16 \pmod{30};$$

isto é $2^{1024} = 30q + 16$, em que q é o quociente desta divisão. Logo,

$$3^{2^{1024}} \equiv (3^{30})^q \cdot 3^{16} \equiv 3^{16} \equiv 43046721 \equiv 28 \pmod{31}.$$

6. Como $12 = 2^2 \cdot 3$, as ordens de 4 e 3 módulo 13 só podem ser iguais a 2, 3, 4, 6 ou 12. Mas,

$$3^3 \equiv 27 \equiv 1 \pmod{13},$$

donde

$$4^2 \equiv 16 \equiv 3 \pmod{13}$$

implies that

$$4^6 \equiv 3^3 \equiv 1 \pmod{13}.$$

Portanto, 3 tem ordem 3 e 4 tem ordem 6 módulo 13. Como

$$4^{24n+1} + 3^{2(18n^2+1)} \equiv 4^{24})^n \cdot 4 + (3^{18})^{2n^2) \cdot 3} \pmod{13},$$

e como 24 é divisível por 4 e 18 é divisível por 3, concluímos, usando as ordens que calculamos para 4 e 3 módulo 13, que:

$$4^{24n+1} + 3^{2(18n^2+1)} \equiv 4 + 3^2 \equiv 13 \equiv 0 \pmod{13}.$$

Logo, $4^{24n+1} + 3^{2(18n^2+1)}$ é divisível por 13 qualquer que seja o inteiro $n \geq 0$.

7. Por tentativa temos que 2 tem ordem 3 módulo 7, o que nos permite concluir que -2 tem ordem 6 módulo 7, pois

$$-2^2 \equiv 4 \pmod 7 \quad \text{ao passo que} \quad -2^3 \equiv -1 \pmod 7.$$

Por tentativa 3 tem ordem 16 módulo 17, porque

$$3^2 \equiv -8 \pmod{17}$$
$$3^4 \equiv 8^2 \equiv 13 \pmod{17}$$
$$3^8 \equiv 13^2 \equiv 16 \pmod{17}.$$

Note que, embora 2 tenha ordem 8 módulo 17, não segue disto que -2 tenha ordem 16 módulo 17, porque

$$-2^{16} \equiv 2^{16} \equiv (2^8)^2 \equiv 1 \pmod{17}.$$

Qualquer inteiro cuja ordem módulo 32 existe tem ordem menor ou igual a 8, logo o elemento pedido não existe. Como 2 tem ordem 5 módulo 31, -2 terá ordem 10, porque

$$(-2)^{10} \equiv (-2^5)^2 \equiv (-1)^2 \equiv 1 \pmod{31},$$

de modo que, pelo lema chave, a ordem de -2 terá que ser 2, 5 ou 10. Como $(-2)^5 \equiv -1 \pmod{31}$ e $(-2)^2 \equiv 4 \pmod{31}$, a ordem terá que ser 10. Finalmente, como 31 é primo, segue do teorema de Fermat que

$$b^{30} \equiv \quad \pmod{31}$$

qualquer que seja $b \not\equiv 0 \pmod{31}$. Portanto, pelo lema chave, a ordem de todo inteiro que não é divisível por 31 tem que dividir $30 \equiv 2 \cdot 3 \cdot 5$. Como 7 não divide 30, o elemento desejado não existe.

8. Um cálculo fácil mostra que as únicas potências de 25 que são distintas módulo 45 são

$$25^1 \equiv 25 \pmod{45}$$
$$25^2 \equiv 40 \pmod{45}$$
$$25^3 \equiv 10 \pmod{45}$$

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.

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