

Lista 2 de MA14 — Aritmética (2017)

1. Ache o resto da divisão:
 - (a) de 7^{10} por 51
 - (b) de 2^{100} por 11
 - (c) de 14^{256} por 17
 - (d) de $13^{16} - 2^{25}5^{15}$ por 13.

2. Verifique se $0, 1, 2, 2^2, \dots, 2^9$ é sistema completo de restos módulo 11.

3. Verifique que para m ímpar o conjunto

$$\left\{ 0, \pm 1, \pm 2, \dots, \pm \frac{m-1}{2} \right\}$$

é um sistema completo de restos módulo m .

4. Verifique que para m par o conjunto

$$\left\{ 0, \pm 1, \pm 2, \dots, \pm \frac{m}{2} \right\}$$

é um sistema completo de restos módulo m .

5. Sejam m_1 e m_2 inteiros relativamente primos e a um inteiro. Prove que $a \equiv 0 \pmod{m_1 m_2}$ se e somente se $a \equiv 0 \pmod{m_1}$ e $a \equiv 0 \pmod{m_2}$. Mostre com um exemplo que a hipótese $(m_1, m_2) = 1$ é essencial neste problema.

6. Mostre que um inteiro na base 10 é divisível por 6 se e somente se a soma do algarismo das unidades com o quádruplo de cada um dos outros algarismos é divisível por 6.

7. Seja p um inteiro primo e sejam a e b inteiros. Prove que $(a+b)^p \equiv a^p + b^p \pmod{p}$

8. Seja a um inteiro. Mostre que a^5 e a têm o mesmo algarismo das unidades quando escritos na base 10.

9. Um palíndromo é um número que quando lido da esquerda para a direita é igual a quando lido da direita para esquerda, por exemplo, 121. Demonstre que todo palíndromo com um número par de algarismos é divisível por 11.

10. Demonstre que se $a_r \dots a_0$ é a representação decimal de n , então $7|n$ se, e só se, $7|(a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + a_6 + 3a_7 + 2a_8 - \dots)$.

11. Sejam m_1, m_2, \dots, m_k inteiros positivos e $a \equiv b \pmod{m_i}$ para todo i . Então $a \equiv b \pmod{\text{mmc}(m_1, m_2, \dots, m_k)}$.

12. Determine um número que dividido por 3,5,7 de restos 2,3,2

13. Prove que nenhum número natural deixa resto 5 quando dividido por 12 e resto 4 quando dividido por 15.

14. Determine todos os números naturais que quando divididos por 18 deixam resto 4 e que quando divididos por 14 deixam resto 6.

15. Mostre que o sistema de congruências lineares não tem solução:
$$\begin{cases} x \equiv 5 \pmod{6} \\ x \equiv 7 \pmod{15} \end{cases}$$

16. Um certo inteiro entre 1 e 1200 tem por resto 1, 2 e 6 quando dividido por 9, 11 e 13. Determine-o.

17. O protocolo de criptografia RSA funciona do seguinte modo:

- (a) Escolha dois números primos p e q e compute $n := p \cdot q$;
- (b) Compute $\varphi(n) = (p - 1) \cdot (q - 1)$;
- (c) Escolha $e \in \{2, 3, \dots, \varphi(n) - 1\}$ com $\text{mdc}(e, \varphi(n)) = 1$; disponibilize o par (e, n) , essa é a sua **chave pública**.
- (d) Compute d tal que $d \cdot e \equiv 1 \pmod{\varphi(n)}$ e mantenha-o em segredo, a sua **chave privada** é o par (d, n) .

Consideremos que uma mensagem é um natural $m \in \mathbb{Z}$ (por exemplo, m é o número representado em base 2 que o computador usa para gravar o arquivo com a mensagem no HD) tal que $m < n$ (isso não é uma restrição que põe tudo a perder, como foi explicado em sala, basta considerar o binário em blocos).

Para o Aécio mandar para você a mensagem m criptografada, ele busca pela sua chave pública, calcula $c := m^e \pmod{n}$ e envia c . Você, que é o único portador da chave privada, calcula a $c^d \pmod{n}$.

Demonstre que $m = c^d \pmod{n}$.