Gabarito Lista 4, Álgebra I

1a. Temos $\text{mdc}(3,5) = \text{mdc}(5,7) = \text{mdc}(3,7) = 1$ assim pelo Teorema Chinês do Resto existe um unico solução modulo $3 \cdot 5 \cdot 7 = 105$. Usamos o algorithmo de Gauss para encontrar o solução. Temos

$$N_1 = 5 \cdot 7 = 35, \quad N_2 = 3 \cdot 7 = 21, \quad N_3 = 3 \cdot 5 = 15;$$

$$c_1 = 1, \quad c_2 = 2, \quad N_3 = 3;$$

$$N_1^{-1} = 2, \quad N_2^{-1} = 1, \quad N_3^{-1} = 3 \cdot 5 = 1;$$

Assim temos

$$x = N_1 \cdot c_1 \cdot N_1^{-1} + N_2 \cdot c_2 \cdot N_2^{-1} + N_3 \cdot c_3 \cdot N_3^{-1} = 70 + 42 + 45 = 157 = 52(\text{mod } 105)$$

1b. Na mesma maneiro como o exercicio anterior temos

$$x \equiv 59(\text{mod } 462).$$

1c.

$$x \equiv 119(\text{mod } 210).$$

2. Temos $\begin{cases} a \equiv 0 \pmod 2 \\ a \equiv 2 \pmod 3 \\ a \equiv 2 \pmod 4 \\ a \equiv 2 \pmod 5 \\ a \equiv 2 \pmod 6 \end{cases}$. Resolvemos $\begin{cases} a \equiv 2 \pmod 3 \\ a \equiv 2 \pmod 4 \\ a \equiv 2 \pmod 5 \end{cases}$ Obtemos um unico solução $a \equiv 2(\text{mod } 60)$ que satisfaz $a \equiv 0 \pmod 2$ e $a \equiv 2 \pmod 6$.

3. Temos $\begin{cases} a \equiv 1 \pmod 2 \\ a \equiv 1 \pmod 3 \\ a \equiv 1 \pmod 4 \\ a \equiv 1 \pmod 5 \\ a \equiv 1 \pmod 6 \\ a \equiv 0 \pmod 7 \end{cases}$. Resolvemos $\begin{cases} a \equiv 1 \pmod 4 \\ a \equiv 1 \pmod 3 \\ a \equiv 1 \pmod 5 \\ a \equiv 0 \pmod 7 \end{cases}$ Obtemos $a \equiv 301(\text{mod } 410)$, é facil ver que $a \equiv 1 \pmod 2$ e $a \equiv 1 \pmod 6$

4a. Como $\text{mdc}(3,5) = 1$ é sufficiente mostrar que $a^{21} \equiv a(\text{mod } 3)$ e $a^{21} \equiv a(\text{mod } 5)$. Pelo T.de Fermat temos $a^3 \equiv a(\text{mod } 3)$, assim

$$\begin{aligned} a^{21} &= (a^3)^4 \\ &\equiv a^7(\text{mod } 3) \\ &\equiv (a^3)^2 \cdot a(\text{mod } 3) \\ &\equiv (a^2) \cdot a(\text{mod } 3) \\ &\equiv a(\text{mod } 3) \end{aligned}$$

Semelhante $a^5 \equiv a(\text{mod } 5)$, assim

$$\begin{aligned} a^{21} &= (a^5)^4 \cdot a \\ &\equiv a^4 \cdot a(\text{mod } 5) \\ &\equiv a(\text{mod } 5) \end{aligned}$$

4b. Na mesma maneira como o exercicio anterior Como mdc$(5, 7) = 1$ é sufficiente mostrar que $a^{12} \equiv 1(\text{mod } 5)$ e $a^{12} \equiv 1(\text{mod } 7)$. Pelo T.de Fermat temos $a^4 \equiv 1(\text{mod } 5)$, assim

$$\begin{aligned} a^{12} &= (a^4)^3 \\ &\equiv 1^3(\text{mod } 5) \\ &\equiv 1(\text{mod } 5) \end{aligned}$$

Semelhante $a^6 \equiv 1(\text{mod } 7)$, assim

$$\begin{aligned} a^{12} &= (a^6)^2 \\ &\equiv 1^2(\text{mod } 7) \\ &\equiv 1(\text{mod } 7) \end{aligned}$$

4c. Como mdc$(a, 42) = 1$ assim mdc$(a, 2) =$ mdc$(a, 3) =$ mdc$(a, 7) = 1$. Desde $42 = 2 \cdot 3 \cdot 7$, segue-se que $2, 3, 7$ não dividem a. Assim, pelo Teorema de Fermat, temos: $a^2 \equiv a(\text{mod } 2)$, $a^3 \equiv a(\text{mod } 3)$, e $a^7 \equiv a(\text{mod } 7)$, ou equivalentemente, $a \equiv 1(\text{mod } 2)$, $a^2 \equiv 1(\text{mod } 3)$, e $a^6 \equiv 1(\text{mod } 7)$. Temos: $a^6 \equiv 1^6(\text{mod } 2) \equiv 1(mmod 2)$ $a^6 \equiv (a^2)^3\ equiv 1^3(\text{mod } 3) \equiv 1(\text{mod } 3)$, e: $a^6 \equiv 1(\text{mod } 7)$. Nossa preocupação aqui é que 168 tem fatoração $23 \cdot 3 \cdot 7$. Assim, provavelmente não será suficiente para nós ter que $a^6 \equiv 1(\text{mod } 2)$. A gente precisa de mostrar que $a^6 \equiv 1(\text{mod } 2^3)$.

Primeiro temos que $a \equiv 1(\text{mod } 2)$ implica que $a-1 \equiv 0(\text{mod } 2)$ e $a+1 \equiv 0(\text{mod } 2)$. Temos que OU $(a-1) \equiv 0(\text{mod } 4)$ e $(a+1) \equiv 2(\text{mod } 4)$ OU $(a-1) \equiv 0(\text{mod } 4)$ e $(a+1) \equiv 0(\text{mod } 4)$. Assim isso implica que $(a^2 - 1) \equiv 0(\text{mod } 8)$. Agora, como $a^6 - 1 = (a^2 - 1)(a^4 + a^2 + 1)$ temos que

$$a^6 \equiv 1(\text{mod } 8).$$

E $a^6 \equiv 1(\text{mod } 168)$.

5,6. Veja notas das aulas (Revisão 1).

7. Temos $2^4 = 16 \equiv (-1)(\text{mod } 17)$ assim $2^8 = (2^4)^2 \equiv (-1)^2 = 1(\text{mod } 17)$. $2^{16} \equiv 1(\text{mod } 17)$ segue pelo T.de Fermat.

8a. Seja $a^{\frac{p-1}{2}} \equiv x(\text{mod } p)$. Assim

$$x^2 \equiv a^{p-1} \equiv 1(\text{mod } p).$$

Os unicos soluções da congruencia $x^2 \equiv 1(\text{mod } p)$ são $x \equiv 1(\text{mod } p)$ (assim $a^{\frac{p-1}{2}} \equiv 1(\text{mod } p)$) e $x \equiv p - 1(\text{mod } p)$ (assim $a^{\frac{p-1}{2}} \equiv p - 1 \equiv -1(\text{mod } p)$).

8b. Seja $e \nmid (p-1)$ assim $p - 1 = e \cdot q + r$ com $0 < r \leq e$, assim

$$1 \equiv a^{p-1} \equiv a^{eq+r} \equiv (a^e)^q \cdot a^r = a^r(\text{mod } p).$$

Contradição, com e é menor inteiro positivo tal que $a^e \equiv 1(\text{mod } p)$. Assim $e \mid p - 1$.

9,10. Veja notas das aulas (Revisão 1).

11. Pelo T.de Euler $m^{\varphi(n)} \equiv 1(\mod n)$ also temos que $n^{\varphi(m)} \equiv 0(\text{mod } n)$, assim

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1(\text{mod } n).$$

Semelhante $n^{\varphi(m)} \equiv 1(\mod m)$ also temos que $m^{\varphi(n)} \equiv 0(\text{mod } m)$, assim

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1(\text{mod } m).$$

Como mdc$(n, m) = 1$ assim temos

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1(\text{mod } nm).$$

12a. Pelo T. de Wilson temos

$$16! \equiv -1(\text{mod } 17).$$

Por outro lado $15!16 \equiv 15!(-1)(\text{mod } 17)$. Assim $15! \equiv 1(\text{mod } 17)$. Resto é 1.

12b. Temos $28! \equiv -1 \pmod{29}$.

$$26! \cdot 2 = 26! \cdot (-2) \cdot (-1) \equiv 26! \cdot 27 \cdot 28 = 28! \equiv -1 \pmod{29}.$$

13. Pares (a, b) são

$$(2,12),(3,8),(4,6),(5,14),(7,10),(9,18),(11,21),(13,16),(15,20),(17,19)$$

14. Temos $437 = 19 \cdot 23$. Pelo T. de Wilson temos

$$18! \equiv -1 \pmod{19}, \qquad 22! \equiv -1 \pmod{23}$$

Por outro lado

$$22! = 18! \cdot 19 \cdot 20 \cdot 21 \cdot 22 \equiv 18!(-1)(-2)(-3)(-4) \equiv 18! \cdot 24 \equiv 18! \pmod{23}.$$

Assim $18! \equiv -1 \pmod{19 \cdot 23}$.

15. Seja $5! \cdot 25! \equiv x \pmod{31}$. Pelo T. de Wilson temos

$$30! \equiv -1 \pmod{31}.$$

Assim

$$5!30! \equiv -(5!) \pmod{31}.$$

$$5!30! = 5! \cdot 25! \cdot 26 \dots 30.$$

Ou $26 \dots 30 \cdot x \equiv (-5) \dots (-1) \cdot x \equiv -(5!) \pmod{31}$ assim

$$120x \equiv 120 \pmod{31}$$

Como $\text{mdc}(120, 31) = 1$, cancelamos 120 assim $x \equiv 1 \pmod{31}$.