Aula 22. Revisão I

22.1 Teorema Chinês do Resto

Seja dado o sistema das congruências:

$$\begin{cases} x \equiv c_1 \,(\mathrm{mod}\, n_1) \\ x \equiv c_2 \,(\mathrm{mod}\, n_2) \\ \vdots \\ x \equiv c_k \,(\mathrm{mod}\, n_k)\,, \end{cases}$$

Theorem 22.1: Chinês do Resto

Sejam $n_1, \ldots, n_k$ tais que $\mathrm{mdc}(n_i, n_j) = 1$, se $i \neq j$ e sejam $c_1, \ldots, c_k$ os inteiros dados. Assim o sistema acima admite a solução $t \in \mathbb{Z}$. Além disso, se $q \in \mathbb{Z}$ é qualquer outro solução do sistema, assim

$$q \equiv t \quad (\mathrm{mod}\, n_1 \cdot n_2 \cdot \ldots n_k)\,.$$

O Teorema Chinês de Resto fornece um algoritmo para procurar as soluções do sistema acima. Este algoritmo é chamado Algoritmo de Gauss.

Seja

$$N = n_1 \cdot \cdots \cdot n_k,$$

assim a geral solução desse sistema é dado por

$$x \equiv N_1 \cdot c_1 \cdot d_1 + N_2 \cdot c_2 \cdot d_2 + \ldots + N_k \cdot c_k \cdot d_k (\mathrm{mod}\, N)$$

onde $N_i = \frac{N}{n_i}$ e d_i tais que

$$N_i \cdot d_i \equiv 1 \,(\mathrm{mod}\, n_i)\,.$$

Exercício 22.1

Resolve $\begin{cases} 2x \equiv 1 \pmod 3 \\ x \equiv 1 \pmod 5 \\ 3x \equiv 4 \pmod 7 \end{cases}$

Solução 22.1

O inverso modular de 2 em $\mathbb{Z}_3$ é 2 e o inverso modular de 3 em $\mathbb{Z}_7$ é 5, assim

$$\begin{cases} 2x \equiv 1 (\text{mod } 3) \\ x \equiv 1 (\text{mod } 5) \\ 3x \equiv 4 (\text{mod } 7) \end{cases} \Rightarrow \begin{cases} 2 \cdot 2x \equiv 2 (\text{mod } 3) \\ x \equiv 1 \ (\text{mod } 5) \\ 5.3x \equiv 5.4 \ (\text{mod } 7) \end{cases}$$

Ou seja, o sistema é equivalente do

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 1 \pmod 5 \\ x \equiv 6 \pmod 7 \end{cases}$$

Como 3, 5 e 7 são primos entre si em pares assim existe único solução modulo $3 \cdot 5 \cdot 7 = 105$ pelo Teorema Chinês do Resto. Para encontrar a solução, podemos aplicar o algoritmo de Gauss temos

$$N = 3 \cdot 5 \cdot 7 = 105,$$

e $N_1 = 5 \cdot 7 = 35$, $N_1^{-1} = 2$ em $\mathbb{Z}_3$, $N_2 = 3 \cdot 7 = 21$, $N_2^{-1} = 1$ em Z_5, $N_3 = 3 \cdot 5 = 15$, $N_3^{-1} = 1$ em $\mathbb{Z}_7$. Assim

$$\begin{aligned} x &= N_1 \cdot c_1 \cdot N_1^{-1} + N_2 \cdot c_2 \cdot N_2^{-1} + N_3 \cdot c_3 \cdot N_3^{-1} \\ &= 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 1 + 15 \cdot 6 \cdot 1 = 140 + 21 + 50 = 251 \end{aligned}$$

Agora $x = 251 \equiv 41 \ (\text{mod } 105)$, assim

$$x \equiv 41 \ (\text{mod } 105)$$

é solução do sistema.

22.2 *Teoremas de Euler e Fermat*

Vamos lembrar as formulações dos teoremas de Fermat e Euler.

Theorem 22.2: Teorema de Fermat

Seja p um primo tal que $p \nmid a$, assim

$$a^{p-1} \equiv 1 \pmod p,$$

ou seja $p \mid (a^{p-1} - 1)$.

Definição: Função de Euler

Seia $n \in \mathbb{Z}, n \geqslant 1$. Define a **função de Euler** $\varphi(n)$ como sendo:

$$\varphi(n) := \text{numero dos inteiros a, tais que } 1 \leqslant a \leq n, \text{ e } \quad \text{mdc}(a, n) = 1.$$

Theorem 22.3: Teorema de Euler

Sejam a, n dois inteiros, com $n \geq 1$ e $\text{mdc}(a,n) = 1$, assim

$$a^{\varphi(n)} \equiv 1 \ (\text{mod}\, n).$$

Exercício 22.2

Mostre que se $\text{mdc}(a, 42) = 1$ assim

$$3 \cdot 7 \cdot 8 \mid a^6 - 1.$$

Solução 22.2

Pelo Teorema Chinese de Resto temos que se $\begin{cases} x \equiv 1 (\text{mod } n) \\ x \equiv 1 (\text{mod } m) \end{cases}$ assim $x \equiv 1 (\text{mod } n \cdot m)$.

Pelo Teorema de Fermat, temos que $a^2 \equiv 1 \ (\text{mod } 3)$ assim

$$a^6 \equiv 1 \ (\text{mod } 3).$$

Por outro lado $a^6 \equiv 1 \ (\text{mod } 7)$.

Agora, com $\text{mdc}(a, 42) = 1$ assim $a \equiv 1 \ (\text{mod} 2)$, portanto

$$a \equiv \pm 1, \text{ ou } a \equiv \pm 3 \ (\text{mod} 8).$$

Em ambos os casos temos que $a^2 \equiv 1 (\ \text{mod } 8)$ assim $a^6 \equiv 1 (\ \text{mod } 8)$. Assim temos que

$$\begin{aligned} a^6 &\equiv 1 \pmod 3 \\ a^6 &\equiv 1 \pmod 7 \\ a^6 &\equiv 1 \pmod 8 \end{aligned}$$

Agora pelo observação acima, temos que

$$a^6 \equiv 1 \pmod{3 \cdot 7 \cdot 8}.$$

Exercício 22.3

Encontre o resto da divição de 13^{26} por 10.

Solução 22.3

Temos que $13 \equiv 3 \ (\text{mod } 10)$, assim besta encontrar resto de divisão de 3^{26} por 10 Como $\text{mdc}(3, 10) = 1$, assim podemos aplicar Teorema de Euler. Temos que $\varphi(10) = 4$, portando $3^4 \equiv 1 \ (\text{mod}$

10)

$$3^{26} = \left(3^4\right)^6 \cdot 3^2 \equiv 3^2 = 9 \pmod{10}.$$

Assim $3^{26} \equiv 9 \pmod{10}$, e o resto é 9.

Exercício 22.4

Encontre o resto da divisão de 69^{903} por 31.

Solução 22.4

Temos que $69 \equiv 7 \pmod{31}$. Por outro lado 31 é primo, assim aplicando o Teorema de Fermat temos

$$7^{30} \equiv 1 \pmod{31},$$

Assim

$$7^{903} = \left(7^{30}\right)^{30} \cdot 7^3 \equiv 7^3 \pmod{31}.$$

Agora $7^3 = 343 \equiv 2 \pmod{31}$, portando o resto é 2.

Exercício 22.5

Sejam p, q primos distintos e impares tais que $(p-1) \mid (q-1)$. Mostre que se $\text{mdc}(a, pq) = 1$ então $a^{q-1} \equiv 1 \pmod{pq}$.

Solução 22.5

Como p e q são primos, então $\text{mdc}(p, q) = 1$. Como $p - 1 \mid q - 1$, então $q - 1 = k(p-1), k \in \mathbb{Z}$. Logo, pelo Teorema de Euler, temos:

$$a^{(p-1)} \equiv 1 \pmod{p}$$
$$\left(a^{(p-1)}\right)^k \equiv 1^k \pmod{p}$$
$$a^{(q-1)} \equiv 1 \pmod{p}$$

Novamente, pelo Teorema de Fermat, temos:

$$a^{(q-1)} \equiv 1 \pmod{q}.$$

Assim:

$$\begin{cases} a^{(q-1)} \equiv 1 \pmod{p} \\ a^{(q-1)} \equiv 1 \pmod{q} \end{cases} \Rightarrow a^{(q-1)} \equiv 1 \pmod{pq}\ .$$

Exercício 22.6

Sejam a inteiro, e $n > 0$ com $\text{mdc}(a,n) = 1 = \text{mdc}(a-1,n)$. Mostre que

$$1 + a + \ldots + a^{\varphi(n)-1} \equiv 0 \pmod{n}.$$

Solução 22.6

Temos que $a^{\varphi(n)} \equiv 1 \pmod{n}$ (pois $\text{mdc}(a,n) = 1$), assim $a^{\varphi(n)} - 1 \equiv 0$, portando

$$(a-1)\left(1 + a + a^2 + \ldots + a^{\varphi(n)-1}\right) \equiv 0 \pmod{n}$$

Como $\text{mdc}(a-1,n) = 1$, assim

$$1 + a + a^2 + \ldots + a^{\varphi(n)-1} \equiv 0 \pmod{n}.$$

Exercício 22.7

Mostre que $a^{37} \equiv a \pmod{1729}$.

Solução 22.7

Note que $1725 = 7 \cdot 13 \cdot 19$, aplicando o Teorema de Fermat, temos:

$$\begin{aligned} a^{37} &= \left(a^7\right)^5 \cdot a^2 \equiv a^5 \cdot a^2 = a^7 \equiv a \pmod{7} \\ a^{37} &= \left(a^{13}\right)^2 \cdot a^{11} \equiv a^2 \cdot a^{11} = a^{13} \equiv a \pmod{13} \\ a^{37} &= a^{15} \cdot a^{18} \equiv a \cdot a^{18} = a^{15} \equiv a \pmod{19} \end{aligned}$$

Assim

$$a^{37} \equiv a \pmod{7 \cdot 13 \cdot 19}.$$

22.3 *Teorema de Wilson*

Theorem 22.4: Wilson

Se p é um primo, assim P divide $(p-1)! + 1$

Exercício 22.8

Encontre o resto da divição de 85! por 89.

Solução 22.8

89 é primo assim pelo Teorema de Wilson, temos que

$$88! \equiv -1 \pmod{89}$$

Assim

$$-1 \equiv 85! \cdot 86 \cdot 87.88 \pmod{89}$$
$$-1 \equiv 85!(-3) \cdot (-2) \cdot (-1) \pmod{85}$$
$$\Rightarrow 85! \cdot 6 \equiv 1 \pmod{85}.$$

Fácil ver que $6.15 \equiv 1 \pmod{89}$, ou seja 15 é inverso modular de 6, assim

$$85! \cdot 6 \cdot 15 \equiv 85! \equiv 15 \pmod{89}$$

Portanto o resto é 15.

Exercício 22.9

Suponha que $p > 3$ um primo. Mostre que

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

Solução 22.9

Pelo Teorema de Wilson, temos que

$$(p-1)! \equiv -1 \pmod{p},$$

assim

$$(p-3)!(p-2) \cdot (p-1) \equiv -1 \pmod{p}$$

$$\Rightarrow (p-3)!(-2) \cdot (-1) \equiv -1 \pmod{p}$$

Mas

$$-2 \cdot \left(-\frac{p+1}{2}\right) = p+1 \equiv 1 \pmod{p},$$

Portanto

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

22.4 *Função de Euler*

Na aula passada vimos as seguinte regras quais ajudam calcular os valores da função $\varphi(n)$.

Regra 1:

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

se p é um primo. **Regra 2**:

$$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$$

se $\text{mdc}(n, m) = 1$.

Sabendo essas regras, temo como calcular $\varphi(n)$ para qualquer valor n, na seguinte maneira. Pelo Teorema fundamendal da Aritmetica, temos que qualquer inteiro positivo n pode ser escrito como

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k},$$

onde $p_1, \ldots, p_k$ são primos distintos e $\alpha_1, \ldots, \alpha_k$ inteiros positivos. Assim

$$\begin{aligned} \varphi(n) = \varphi(p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}) &\overset{Regra2}{=} \varphi(p_1^{\alpha_1}) \cdot \ldots \varphi(p_k^{\alpha_k}) \\ &\overset{Regra1}{=} \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdot \ldots \cdot \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right) \end{aligned}$$

Ou seja

$$\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdot \ldots \cdot \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right)$$

Exercício 22.10

Resolve $\varphi(x) = 140$.

Solução 22.10

Suponha que

$$x = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k},$$

Assim $\varphi(x) = 140$, implique

$$p_1^{\alpha_1 - 1} \cdot (p_1 - 1) \cdot \ldots p_k^{2_k - 1} (p_k - 1) = 2^2 \cdot 5 \cdot 7.$$

Primeiramente, se 2 não é fator primo do x, assim como $140 = 2^2 \cdot 5 \cdot 7$ tem exatamente 2 fatores primos (pois todo $p_i - 1$ é par). Neste caso $n = 3 \cdot 71 = 213$ e

$$\varphi(213) = (3 - 1) \cdot (71 - 1) = 2 \cdot 70 = 140.$$

Agora, obviamente $2 \cdot 213$ é solução também, pois

$$\varphi(2 \cdot 213) = (2 - 1) \cdot (3 - 1) \cdot (71 - 1) = 140.$$

Suponha que 2^d é fator de n, com $d > 1$, assim

$$2^{\alpha - 1} \cdot p^{\alpha - 1} \cdot \underbrace{(p - 1)}_{\text{par}} = 2^2 \cdot 5 \cdot 7$$

e $d = 2$, temos que $p = 71$ de novo. Neste caso $x = 4 \cdot 71 = 284$. Assim 213, 284 e 426 todas soluções possíveis.

Exercício 22.11

Mostre que para todo n temos
a) $\varphi(4n) = 2\varphi(2n)$;
b) $\varphi(4n+2) = \varphi(2n+1)$;

Solução 22.11

a) Seja $n = 2^\alpha \cdot m$ com $\text{mdc}(2, m) = 1$. Assim, para $\alpha \geqslant 0$, temos:

$$\varphi(4n) = \varphi\left(2^2 \cdot 2^\alpha \cdot m\right) = \varphi\left(2^{\alpha+2} \cdot m\right) = \varphi\left(2^{\alpha+2}\right)\varphi(m) = 2^{\alpha+1} \cdot \varphi(m)$$

Por outro lado

$$\varphi(2n) = \varphi\left(2^1 \cdot 2^\alpha \cdot m\right) = \varphi\left(2^{\alpha+1} \cdot m\right) = \varphi\left(2^{\alpha+1}\right)\varphi(m) = 2^\alpha \cdot \varphi(m)$$

Logo, $\varphi(4n) = \varphi(2n)$.

b) Como $\varphi(4n+2) = \varphi(2 \cdot (2n+1))$ e $\text{mdc}(2, 2n+1) = 1$, então

$$\varphi(2 \cdot (2n+1)) = \varphi(2) \cdot \varphi(2n+1) = \varphi(2n+1).$$