Aula 17. Teorema de Wilson. Função de Euler

17.1 Lembrete

Vamos lembrar que na aula passada a gente viu dois Teoremas fundamenntais

Teorema de Fermat. Sejam p um primo e a um inteiro com $p \nmid a$. Assim:

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

Como corolário isso implique que para todo inteiro a, temos que

$$a^{p} \equiv a \pmod{p}.$$

Teorema de Euler. Sejam a, n dois inteiros com $n > 0$ e $\text{mdc}(a, n) = 1$. Assim:

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

onde

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

Exemplo 17.1

Suponha que $a = 2, n = 9$. Temos $\text{mdc}(2, 9) = 1$, calculando $\varphi(9)$ temos

$$\{1, 2, \cancel{3}, 4, 5, \cancel{6}, 7, 8, \cancel{9}\}.$$

Assim temos $\varphi(9) = 6$ e

$$2^{6} \equiv 1 \pmod{9},$$

Exemplo 17.2

Suponha que $a = 31, n = 20$. Temos $\text{mdc}(31, 20) = 1$, calculando $\varphi(20)$ temos

$$\{1, \cancel{2}, 3, \cancel{4}, \cancel{5}, \cancel{6}, 7, \cancel{8}, 9, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \cancel{15}, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}\}.$$

Assim temos $\varphi(20) = 8$ e

$$31^{8} \equiv 1 \pmod{20},$$

Exemplo 17.3

Vamos encontrar o resto de divisão de 5^{100} por 7. Pelo Teorema de Fermat temos que

$$5^6 \equiv 1 (\mathrm{mod} 7)$$

assim

$$(5^6)^{16} \equiv 1 (\mathrm{mod} 7),$$

ou seja $5^{96} \equiv 1 (\mathrm{mod} 7)$. Por outro lado $5^2 \equiv 4 (\mathrm{mod} 7)$, assim $5^4 \equiv 16 \equiv 2 (\mathrm{mod} 7)$. Portanto

$$5^{100} \equiv 2 (\mathrm{mod} 7).$$

17.2 *Teorema de Wilson*

Theorem 17.1: Wilson

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

Vamos ilustrar o teorema nos seguintes exemplos:

(a) $p = 2$, assim $(p-1)! + 1 = 1! + 1 = 2 = 2.1$

(b) $p = 3$, assim $(p-1)! + 1 = 2! + 1 = 3 = 3 \cdot 1$

(c) $p = 5$, assim $(p-1)! + 1 = 4! + 1 = 25 = 5.5$ é múltiplo de 5

(d) $p = 7$, assim $(p-1)! + 1 = 6! + 1 = -721 = 7 \cdot 103$ é múltiplo de 7

John Wilson (1741–1793)

Para provar o resultado, primeiramente vamos provar os seguintes lemas.

Lemma 17.1

Seja p um primo. Para todo a em

$$C = \{1, 2, \ldots, p-1\}$$

existe unico inverso modular do a em C ou seja único $b \in C$, tal que

$$a \cdot b \equiv 1 (\mathrm{mod}\, p)$$

Prova

Como $\text{mdc}(a,p)=1$, logo a congruencias

$$a\cdot x\equiv 1 \pmod p$$

tem solução $t\in\mathbb{Z}$. Pelo Algoritmo da divição

$$t=q\cdot p+b,$$

com $0\leqslant b\leqslant p-1$, mas $b\neq 0$, pois caso contrario $at\equiv 0(\text{mod}\,p)$ assim $b\in C$ e $a\cdot b\equiv 1(\text{mod}\,p)$.

O lema antrerior pode ser ilustrado nos seguintes exemplos

Exemplo 17.4

Suponha $p=5$, assim $C=\{1,2,3,4\}$ e

$$\begin{aligned}1\cdot 1&\equiv 1\ (\text{mod}5),\\ 2\cdot 3&\equiv 1\ (\text{mod}5)\\ 3\cdot 2&\equiv 1\ (\text{mod}5),\\ 4\cdot 4&\equiv 1\ (\text{mod}5).\end{aligned}$$

Se $p=11$, assim

$$C=\{1,2,3,4,5,6,7,8,9,10\},$$

e

$$\begin{aligned}1\cdot 1&\equiv 1(\text{mod}11), & 2\cdot 6&\equiv 1(\text{mod}11),\\ 3\cdot 4&\equiv 1(\text{mod}11) & 8\cdot 7&\equiv 1(\text{mod}11),\\ 5\cdot 9&\equiv 1(\text{mod}11), & 10\cdot 10&\equiv 1(\text{mod}11)\end{aligned}$$

Observação 17.1

Em dois exemplos acima temos que $x=1,4$ são únicos tais que

$$x^2\equiv 1\ (\text{mod}5)$$

e $x=1,10$ são únicos tais que

$$x^2\equiv 1\ (\text{mod}11)$$

Lemma 17.2

Seja p um primo, e $x\in\{1,\ldots,p-1\}$. Assim:

$$x^2\equiv 1\ (\text{mod}11)$$

implique que $x=1$ ou $x=p-1$.

Prova

Se $x^2 \equiv 1 (\mathrm{mod}\, p)$ assim $p \mid x^2 - 1$ ou seja $p \mid (x-1)(x+1)$. Como p é um primo, assim $p \mid (x-1)$ e $p \mid (x+1)$. Como $1 \leqslant x \leqslant p-1$ assim temos que $x = 1$ ou $x = p-1$.

Agora estamos prontos para provar o Teorema de Wilson

Theorem 17.2: Wilson

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

$$(p-1)! \equiv -1 (\mathrm{mod}\, p).$$

Prova

Conforme Lemas 17.1 e 17.2 podemos agrupar os elementos

$$2, 3, \ldots, (p-3), (p-2)$$

em pares a, a' com $a \neq a'$ e

$$aa' \equiv 1 \pmod{p}$$

Consequentemente fazendo o produto de tais congruências temos:

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

Por outro lado

$$p - 1 \equiv -1 (\mathrm{mod}\, p)$$

Assim (fazendo o produto de 2 ultimas congruencias) temos que

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

Exemplo 17.5

Para ilustrar o argumento da prova, considere o caso $p = 11$, assim temos que

$$2 \cdot 6 \equiv 1 (\mathrm{mod}\, 11),$$
$$3 \cdot 4 \equiv 1 (\mathrm{mod}\, 11),$$
$$5 \cdot 9 \equiv 1 (\mathrm{mod}\, 11),$$
$$8 \cdot 7 \equiv 1 (\mathrm{mod}\, 11).$$

Ou seja agrupamos elementos $2, 3, \ldots, 9$ em pares $(2,6), (3,4), (5,9), (7,8)$. Fazendo o produto das congruências temos

$$2 \cdot 3 \cdot \ldots \cdot 9 \equiv 1 (\mathrm{mod}\, 11)$$

por outro lado

$$10 \equiv -1 (\mathrm{mod}\, 11)$$

assim recebemos

$$10! \equiv -1 (\mathrm{mod}\, 11).$$

Exemplo 17.6

Observando que 2017 é primo vamos mostrar que mostre que

$$2015^{2016} + 2016!$$

é um múltiplo de 2017. Pelo Teorema de Fermat temos

$$2015^{2016} \equiv 1 \pmod{2017}$$

Pelo Teorema de Wilson temos

$$(2016)! \equiv -1 \ (mod 2017)$$

Assim, somando as congruências, temos que

$$2015^{2016} + 2016! \equiv 0 (\mathrm{mod}\, 2017).$$

Exemplo 17.7

Vamos encontrar o resto da divisão de 10! por 13. Pelo Teorema de Wilson, temos que

$$12! \equiv -1 \pmod{13}$$

Observem que

$$11 \equiv -2 (\mathrm{mod}\, 13), \qquad 12 \equiv -1 (\mathrm{mod}\, 13)$$

assim

$$10! \cdot 11 \cdot 12 = 10!(-2) \cdot (-1) \equiv (-1) (\mathrm{mod}\, 13).$$

Portanto

$$2 \cdot 10! \equiv -1 \pmod{13}.$$

o inverso modular de 2 modulo 13 e 7, pois $2 \cdot 7 \equiv 1 (\mathrm{mod}\, 13)$, assim

$$2 \cdot 7 \cdot 10! \equiv 10! \equiv -7 \equiv 6 \pmod{13}.$$

Assim resto é 6.

17.3 *Como calcular $\varphi(n)$*

Como a gente viu, calcular os valores da função $\varphi(n)$ "manualmente" pode ser bem complicado se n é grande. Na aula que vem vamos mostrar as seguinte regras

Regra 1:

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

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

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

Ou seja

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

Exemplo 17.8

Suponha que $n = 100$. Assim $100 = 2^2 \cdot 5^2$. Temos

$$\varphi(100) = \varphi(2^2 \cdot 5^2) \overset{Regra2}{=} \varphi(2^2) \cdot \varphi(5^2) \overset{Regra1}{=} (2^2 - 2^1) \cdot (5^2 - 5^1) = 2 \cdot 20 = 40.$$

Exemplo 17.9

Suponha que $n = 760$. Assim $760 = 2^3 \cdot 5 \cdot 19$. Temos

$$\varphi(760) = \varphi(2^3 \cdot 5 \cdot 19) \overset{Regra2}{=} \varphi(2^3) \cdot \varphi(5) \cdot \varphi(19) \overset{Regra1}{=} (2^3 - 2^2) \cdot 4 \cdot 18 = 144.$$

Exemplo 17.10

Vamos encontrar 3 ultimos digitos de 2017^{2001}. Para fazer isso, observem que 3 últimos dígitos de qualquer inteiro é o resto da divisão dele por 1000. Agora

$$\varphi(1000) = \varphi(2^3 \cdot 5^3) \overset{Regra2}{=} \varphi(2^3) \cdot \varphi(5^3) \overset{Regra1}{=} (2^3 - 2^2) \cdot (5^3 - 5^2) = 400.$$

Assim, pelo Teorema de Euler

$$2017^{400} \equiv 1 (\text{mod} 1000).$$

Portanto $2017^{2000} = 1 (\text{mod} 1000)$, ou seja

$$2017^{2001} \equiv 2017 (\text{mod} 1000)$$

Assim 3 ultinos digitos sao 017.

Exercício 17.1: (Trabalho p/ casa)

Encontre o resto da divisão de 67! por 71.
Reposta: 35.

Exercício 17.2: (Trabalho p/ casa)

Encontre o resto da divisão de 53! por 61.
Reposta: 53.

Exercício 17.3: (Trabalho p/ casa)

Calcule $\varphi(n)$ para $n = 90, 300, 2310$
Reposta: $24, 80, 480$.

Exercício 17.4: (Trabalho p/ casa)

Encontre 2 últimos dígitos de 3^{399} e 5^{2011}.