Aula 16. Teoremas de Fermat e Euler

16.1 Inverso modular (lembrete)

Lembrete.

a) Sejam a, n dois inteiros com $n > 0$. Um inteiro b chama-se inverso modular de a modulo n, se

$$a \cdot b \equiv 1 \pmod{n}.$$

b) Inverso modular de a modulo n existe se e somente se

$$\mathrm{mdc}(a, n) = 1.$$

c) O inverso modular pode ser encontrado através algoritmo de Euclides e desempenha um papel importante no Algoritmo de Gauss para resolver o sistema de cogerências através o Teorema chines de Resto.

Rierre de Fermat

Porem, em alguns casos é fácil encontrar o inverso modular via Teorema de Fermat e Teorema de Euler.

16.2 Teorema de Fermat

Theorem 16.1: Teorema de Fermat

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

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

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

Prova

Notamos que $p \nmid a$ implique que $\text{mdc}(a, p) = 1$. Agora considere o conjunto

$$X = \{a, 2a, 3a, \dots, (p-1)a\}.$$

Dados dois elementos diferentes em X, xa e ya com $x, y \in \{1, \dots, (p-1)\}$ e $x \neq y$, temos que se $xa \neq ya \pmod{p}$, fois se $xa \equiv ya \pmod{p}$, assim $x \equiv y \pmod{p}$ usando que $\text{mdc}(a, p) = 1$ é absurdo. Além disso nenhum elemento $xa \in X$ é congruente 0 modulo p, pois se $p \mid xa$ assim $p \mid x$ ou $p \mid a$ e ambas são impossíveis.
Assim os elementos do X sao congruentes aos elementos do conjunto $\{1, 2, \dots, p-1\}$, isto é

$$\begin{cases} a \equiv x_1 \pmod{p} \\ 2a \equiv x_2 \pmod{p} \\ \vdots \\ (p-1)a \equiv x_{p-1} \pmod{p}, \end{cases} \tag{16.1}$$

onde $x_1, \dots, x_{p-1}$ é uma permutação dos inteiros $1, 2, ...p-1$. Assim:

$$a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1)a \equiv x_1 \cdot x_2 \cdot x_3 \cdot \dots x_{p-1} \pmod{p},$$

ou seja

$$(p-1)!a^{p-1} \equiv (p-1)! (\text{mod}\, p).$$

Como $\text{mdc}((p-1)!, p) = 1$ assim oltimo igualdade implique que

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

Corolário 16.1

Sejam: p um primo e a um inteiro arbitrário, assim

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

Prova

Se $p \nmid a$, assim $a^p \equiv 1 (\text{mod}\, p)$ ou seja

$$a^p \equiv a (\text{mod}\, p).$$

Por outro lado, se $p \mid a$, assim $p \mid a$ e $p \mid a^p - a$, ou seja

$$a^p \equiv a (\text{mod}\, p).$$

Corolário 16.2

Se $p \nmid a$ assim a^{p-2} é inverso modular de a modulo p, pois

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

Exemplo 16.1

Sejam $a = 2$, $p = 3$, assim

$$a^{p-2} = 2^{3-2} = 2.$$

Ou seja 2 é inverso modular de 2 modulo 3. Na verdade

$$2 \cdot 2 = 4 \equiv 1 \pmod{3}.$$

Agora, se $a = 3$, $p = 5$, assim

$$a^{p-2} = 3^{5-2} = 3^3.$$

Portanto $3^3 = 27$ é inverso modular de 3 modulo 5. Na verdade

$$3 \cdot 3^1 = 81 \equiv 1 \pmod{5}.$$

Observem que podemos reduzir o $3^3 = 27$ modulo 5 recebendo 2 que também o inverso modular de 3

$$3 \cdot 2 = 6 \equiv 1 \pmod{5}.$$

Exemplo 16.2

Dados $a, b \in \mathbb{Z}$ e um primo p, mostre que

$$(a+b)^p \equiv a^p + b^p (\bmod p)$$

Temos que

$$a^p \equiv a(\bmod p)$$
$$b^p \equiv b(\bmod p)$$

Assim

$$a^p + b^p \equiv a + b(\bmod p)$$

Por outro lado

$$(a+b)^p = a + b(\bmod p).$$

Assim

$$a^P + b^p = (a+b)^p(\bmod p).$$

Exemplo 16.3

Mostre que $10 \mid a^5 - a$, para todo inteiro a.
Temos que $10 = 2.5$ e como $\text{mdc}(2,5) = 1$, assim basta ver que $2 \mid a^5 - a$ e $5 \mid a^5 - a$.
Pelo Corolário 1 (com $p = 5$)

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

assim $5 \mid a^5 - a$. Por outro lado

$$a^2 \equiv a(\text{mod} 2)$$

Multiplicando por a temos

$$a^3 \equiv a^2(\text{mod} 2).$$

Agora, multiplicando ultimas duas congruências, temos

$$a^5 \equiv a^3 \equiv a^2 \equiv a \pmod{2},$$

ou seja $2 \mid a^5 - a$.

16.3 *Teorema de Euler*

Antes de formular o Teorema, precisamos definir a função de Euler.

Definição: Função de Euler

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

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

Leonhard Euler

$$
\begin{aligned}
\varphi(1) &= 1, && \text{pois } \text{mdc}(1,1) = 1 \\
\varphi(2) &= 1, && \{1, \cancel{2}\} \\
\varphi(3) &= 2, && \{1, 2, \cancel{3}\} \\
\varphi(4) &= 2, && \{1, \cancel{2}, 3, \cancel{4}\} \\
\varphi(5) &= 4, && \{1, 2, 3, 4, \cancel{5}\} \\
\varphi(6) &= 2, && \{1, \cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6}\} \\
\varphi(7) &= 6, && \{1, 2, 3, 4, 5, 6, \cancel{7}\}
\end{aligned}
$$

Observação 16.1

Notamos que se p um primo, assim

$$\varphi(p) = p - 1.$$

Theorem 16.2: Teorema de Euler

Sejam a, n dois inteiros, com $n \geq 1$ e $\mathrm{mdc}(a,n) = 1$, assim
$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Prova

Seja
$$S = \left\{ b_1, \ldots, b_t \middle| \begin{array}{c} 1 \leq b_i \leq n \\ \mathrm{mdc}\,(b_i, n) = 1 \end{array} \right\}.$$
Notamos que $t = \varphi(n)$. Agora considere
$$T = \{ab_1, ab_2, \ldots, ab_t\}\,.$$
Aplicando algoritmo da divição de ab_i por n temos que
$$ab_i = q_i \cdot n + r_i, \quad 0 \leq r_i < 0.$$
Portanto, temos que
$$\mathrm{mdc}\,(ab_i, n) = \mathrm{mdc}\,(n, r_i)\,.$$
Como $\mathrm{mdc}(a,n) = 1$ e $\mathrm{mdc}(b_i,n) = 1$ assim $\mathrm{mdc}(ab_i,n) = \mathrm{mdc}(n,r_i) = 1$. Por tanto os restos $r_1, r_2, \ldots, r_t$ é uma permutação dos $b_1, b_2, \ldots, b_t$. Temos ainda que $ab_i \equiv ab_j (\mathrm{mod}\, u)$ implique que $b_i = b_j$ pois $\mathrm{mdc}(a,n) = 1$. Assim temos
$$\begin{cases} ab_1 \equiv r_1 \pmod{n} \\ ab_2 \equiv r_2 \pmod{n} \\ \vdots \\ ab_t \equiv r_t \pmod{n}\,, \end{cases} \tag{16.2}$$
Multiplicando as congruencias, recebemos
$$a^t \cdot b_1 \cdot b_2 \cdots b_t \equiv b_1 \cdot \ldots b_t (\mathrm{mod}\, n).$$
Como $\mathrm{mdc}(b_i, n) = 1$ para todo i, assim $\mathrm{mdc}(b_1 \cdot b_2 \cdots b_t, n) = 1$ e podemos cancelar o termo $b_1 \cdot b_2 \cdots b_t$ da ultima congruência, recebendo
$$a^t = a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Observação 16.2

Notamos que o Teorema de Euler naturalmente generalize o Teorema de Fermat, pois se $n = p$ um primo, assim a condição $\mathrm{mdc}(a,n) = 1$ equivalente dizer que $p \nmid a$ e $\varphi(n) = \varphi(p) = p - 1$, assim a congruencia
$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$
escreva-se como
$$a^{p-1} \equiv 1 \pmod{p}.$$

Corolário 16.3

Se $\mathrm{mdc}(a, n) = 1$ assim $a^{\varphi(n)-1}$ é inverso modular de a modulo n, pois
$$a \cdot a^{\varphi(n)-1} = a^{\varphi(n)} \equiv 1 (\bmod p).$$

Exemplo 16.4

Suponha que $a = 25, n = 12$. Temos $\mathrm{mdc}(25, 12) = 1$, calculando $\varphi(12)$ temos
$$\{1, \cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}\}.$$
Portanto $\varphi(12) = 4$. Assim pelo Teorema de Euler $25^4 \equiv 1(\mathrm{mod} 12)$ ou seia 25^3 é inverso modular de 25.

Exercício 16.1: (Trabalho p/ casa)

Encontre
$$\varphi(21), \varphi(40), \varphi(55), \varphi(100).$$
Resposta:
$$12, 16, 40, 40.$$

Exercício 16.2: (Trabalho p/ casa)

Mostre que
$$15^{16} \equiv 1 \ (\mathrm{mod} 40).$$

Exercício 16.3: (Trabalho p/ casa)

Encontre inversos modulares de a modulo n
$$\begin{aligned} a &= 4, \quad n = 7 \\ a &= 10, \quad n = 13 \\ a &= 20, \quad n = 29 \\ a &= 5, \quad n = 6 \\ a &= 7, \quad n = 10 \end{aligned}$$