Teoria dos Números e a Lei de Reciprocidade Quadrática

Fernando Vieira Costa Júnior

Universidade Federal de Alagoas – *Campus* de Arapiraca
Matemática – Licenciatura

Outubro, 2014

Introdução

- Sobre o minicurso;
- Metodologia;
- Objetivo do Minicurso.

Sumário

Sumário

Divisibilidade

Definição 1.1.

Sejam $a \in \mathbb{Z}^*$ e $b \in \mathbb{Z}$. Diz-se que a *divide* b se existir $c \in \mathbb{Z}$ tal que $b = ac$. Neste caso, usaremos a notação $a|b$ para indicar que a divide b. Quando não existe $c \in \mathbb{Z}$ tal que $b = ac$, diz-se que a *não divide* b e escreve-se $a \nmid b$.

Observe que dizer a *divide* b é o mesmo que falar b *é divisível por* a ou b *é um múltiplo de* a.

Exemplo.

Notemos que $5|30$, $2|14$ e $3|18$, pois $30 = 5 \cdot 6$, $14 = 2 \cdot 7$ e $18 = 6 \cdot 3$, respectivamente. Temos ainda que $4 \nmid 10$, $3 \nmid 16$ e $10 \nmid 32$, pois não existem inteiros a, b, c tais que $10 = 4a$, $16 = 3b$ ou $32 = 10c$, respectivamente.

Divisibilidade

Teorema 1.1. (Principais propriedades)

Da definição, decorre que, para quaisquer $a, b, c, d \in \mathbb{Z}$:

1. $a|a$, $1|a$ e $a|0$;
2. se $a|b$ e $b|c$, então $a|c$;
3. se $a|b$ e $c|d$, então $ac|bd$;
4. se $ab|ac$ e $a \neq 0$, então $b|c$;
5. se $a|b$ e $b \neq 0$, então $|a| \leq |b|$;
6. $a|1 \Leftrightarrow a = \pm 1$;
7. $a|b$ e $b|a \Rightarrow |a| = |b|$;
8. se $c|a$ e $c|b$, então $c|(ma + nb)$, para quaisquer $m, n \in \mathbb{Z}$;
9. se $a|(b \pm c)$, então $a|b \Leftrightarrow a|c$.

Sumário

Algoritmo da Divisão

Teorema 1.2. (Algoritmo da Divisão – ADD)

Dados $a \in \mathbb{Z}$ e $b \in \mathbb{N}$, existem únicos $q, r \in \mathbb{Z}$ tais que

$$a = qb + r, \quad \text{com} \;\; 0 \leq r < b.$$

Corolário 1.1. (ADD, caso geral)

Dados $a, b \in \mathbb{Z}$ e $b \neq 0$, existem únicos $q, r \in \mathbb{Z}$ tais que

$$a = qb + r, \quad \text{com} \;\; 0 \leq r < |b|.$$

Algoritmo da Divisão

Exemplo.

Numa divisão por -6, os possíveis restos são os números pertencentes ao conjunto $X = \{r \in \mathbb{Z} : 0 \leq r < |-6|\}$, ou seja, ao conjunto $X = \{0, 1, 2, 3, 4, 5\}$.

Algoritmo da Divisão

Observações

Dizemos que um número inteiro é *par* quando é divisível por 2, ou seja, quando deixa 0 na divisão por 2. Dizemos que um número inteiro é *ímpar* se não é divisível por 2, ou seja, se deixa resto 1 na divisão por 2. Além disso, dizemos que dois números inteiros *a e b têm a mesma paridade* se são ambos pares ou ambos ímpares.

Não é difícil verificar que:

- a soma de um número ímpar com um número par é um número ímpar;
- a soma de dois números ímpares é um número par;
- a soma de dois números pares é um número par.

Sumário

Máximo Divisor Comum (MDC)

Definição 1.2. (Máximo Divisor Comum – MDC)

Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$. O *máximo divisor comum (MDC)* de a e b, denotado por $mdc(a, b)$, é um inteiro positivo d que satisfaz as condições:

1. $d|a$ e $d|b$;
2. se $\exists\ c \in \mathbb{Z}$ tal que $c|a$ e $c|b$, então $c|d$.

O item 1 nos diz que $mdc(a, b)$ é um divisor comum de a e b. Já o item 2 diz que d é o maior divisor comum de a e b.

Definição 1.3.

Quando $mdc(a, b) = 1$, diz-se que a *e* b *são relativamente primos* ou *primos entre si*.

Máximo Divisor Comum

Exemplo.

Como podemos verificar, $mdc(3,6) = 3$, $mdc(-5,-30) = 5$, $mdc(6,0) = 6$, $mdc(13,20) = 1$ e $mdc(4,-2) = 2$.

Máximo Divisor Comum (MDC)

Teorema 1.5.

Se $a|bc$ e $mdc(a,b) = 1$, então $a|c$.

Exemplo.

Como $4|24$, $24 = 3 \cdot 8$ e $mdc(4,3) = 1$, segue que $4|8$.

Sumário

Definição 1.6.

Um número $p \in \mathbb{Z}\backslash\{1, -1, 0\}$ diz-se *primo* se $a|p$ implicar $a = \pm 1$ ou $a = \pm p$. Um número $d \in \mathbb{Z}\backslash\{1, -1, 0\}$ diz-se *composto* quando não é primo.

Note que os números $-1, 0, 1$ não são primos e nem são compostos. Da definição, decorre que se d é um número composto, então existem inteiros r e s, com $1 < r \leq s < d$, tais que $d = rs$.

Como p é primo se, e somente se, $-p$ é primo, na maioria dos resultados que faremos, consideraremos $p > 1$. Além disso, definiremos agora os seguintes conjuntos, que serão utilizados no decorrer do livro para simplificar os enunciados:

$$\mathbb{P} = \{p \in \mathbb{N} : p \text{ é primo}\}, \quad \mathbb{P}^* = \{p \in \mathbb{N} : p \text{ é primo ímpar}\} \quad \text{e}$$
$$I_n = \{k \in \mathbb{N} : 1 \leq k \leq n\}.$$

Números Primos

Teorema 1.12.

Se $p|ab$ e p é primo, então $p|a$ ou $p|b$.

Teorema 1.13. (Fundamental da Aritmética – TFA)

Todo $a \in \mathbb{Z} \backslash \{-1, 0, 1\}$ pode ser escrito da forma

$$a = up_1 p_2 \cdots p_k, \quad \text{com} \quad p_1 \leq p_2 \leq \ldots \leq p_k,$$

onde $u = \pm 1$ e p_i é primo, para todo $i \in I_k$. Além disso, essa forma é única.

Corolário 1.6. (TFA, caso geral)

Todo $a \in \mathbb{Z} \backslash \{-1, 0, 1\}$ pode ser escrito de modo único na forma

$$a = up_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}, \quad \text{com} \quad p_1 < p_2 < \cdots < p_n,$$

onde $u = \pm 1$ e p_i é primo para todo $i \in I_n$.

Números Primos

Exemplo.

Decomponha os números 60, 124 e 500 como produtos de fatores primos.

Solução:

i) $60 = 6 \cdot 10 = 2 \cdot 3 \cdot 2 \cdot 5 = 2^2 \cdot 3 \cdot 5;$

ii) $124 = 2 \cdot 62 = 2 \cdot 2 \cdot 31 = 2^2 \cdot 31;$

iii) $500 = 5 \cdot 100 = 5 \cdot 4 \cdot 25 = 2^2 \cdot 5^3;$

iv) $666 = 2 \cdot 3 \cdot 111 = 2 \cdot 3 \cdot 3 \cdot 37 = 2 \cdot 3^2 \cdot 37.$

Sumário

Definição 2.1.

Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Dizemos que *a é congruente (ou côngruo) a b módulo n* e escrevemos

$$a \equiv b \ (mod \ n)$$

se, e somente se, n é um múltiplo de $a-b$, ou seja, se existe $k \in \mathbb{Z}$ tal que $a - b = kn$. Se, porém, n não é múltiplo de $a - b$, então dizemos que *a é incongruente a b módulo n*, e denotamos por

$$a \not\equiv b \ (mod \ n).$$

Congruências

Percebamos que, ao considerar $n \in \mathbb{N}$, dizer que $a \equiv b\ (mod\ n)$, para $a, b \in \mathbb{Z}$, equivale a dizer que $n|(a-b)$. Se $n = 1$, então a congruência $a \equiv b\ (mod\ 1)$ é trivialmente verdadeira, pois todo número inteiro é múltiplo de 1 (basta tomar $k = a - b$ na definição). Se $n = 0$, então a congruência $a \equiv b\ (mod\ 0)$ equivale à igualdade $a = b$, obviamente. Se, por acaso, $n < 0$, na congruência $a \equiv b\ (mod\ n)$, podemos avaliar o caso equivalente $a \equiv b\ (mod\ -n)$. Por definição, o caso $n \leq 0$ é desconsiderado. Além disso, não consideraremos também o caso em que $n = 1$ nos enunciados e demonstrações dos teoremas que se sucederão.

Congruências

Exemplo.

$12 \equiv 2 \ (mod\ 5)$, pois $12 - 2 = 10$ e $5|10$. Também é verdade que $13 \equiv -2 \ (mod\ 5)$, pois $5|[13 - (-2)]$. Porém, $42 \not\equiv 13 \ (mod\ 2)$, pois $42 - 13 = 29$ e $2 \nmid 29$, e, como $9 \nmid 11$ e $11 = 13 - 2$, $13 \not\equiv 2 \ (mod\ 9)$.

Sumário

Proposição 2.1. (Relação de equivalência)

Sejam $a, b, c \in \mathbb{Z}$ e $n \in \mathbb{N}$. A congruência é uma relação reflexiva, simétrica e transitiva , isto é, as seguintes sentenças são verdadeiras:

1. $a \equiv a \ (mod\ n)$;
2. se $a \equiv b \ (mod\ n)$, então $b \equiv a \ (mod\ n)$;
3. se $a \equiv b \ (mod\ n)$ e $b \equiv c \ (mod\ n)$, então $a \equiv c \ (mod\ n)$.

Exemplo.

Como $8 \equiv -2 \ (mod\ 5)$ e $-2 \equiv 3 \ (mod\ 5)$, por transitividade, $8 \equiv 3 \ (mod\ 5)$.

Teorema 2.1. (Operações com $\equiv$)

Se $a, b, c, d \in \mathbb{Z}$ e $n \in \mathbb{N}$ são tais que $a \equiv b \ (mod\ n)$ e $c \equiv d \ (mod\ n)$, então

1. $a + c \equiv b + d \ (mod\ n)$, em particular, $a + k \equiv b + k \ (mod\ n)$;
2. $a - c \equiv b - d \ (mod\ n)$, em particular, $a - k \equiv b - k \ (mod\ n)$;
3. $ac \equiv bd \ (mod\ n)$, em particular, $ak \equiv bk \ (mod\ n)$.

Congruências Modulares

Exemplo.

Mostrar que $246^{2015} \equiv 1 \ (mod\ 7)$.

Solução: Note que $246 = 6 \cdot 41$. Como $6 \equiv -1 \ (mod\ 7)$, podemos elevar esta congruência a 2015, donde

$$6^{2015} \equiv (-1)^{2015} \equiv -1 \ (mod\ 7).$$

Analogamente, $41 \equiv -1 \ (mod\ 7)$. Então, elevando esta congruência a 2015, obtemos $41^{2015} \equiv (-1)^{2015} \equiv -1 \ (mod\ 7)$. Multiplicando as duas congruências obtidas membro a membro, ficamos com

$$6^{2015} \cdot 41^{2015} \equiv (-1) \cdot (-1) \ (mod\ 7).$$

Como $6^{2015} \cdot 41^{2015} = (6 \cdot 41)^{2015} = 246^{2015}$, segue que

$$246^{2015} \equiv 1 \ (mod\ 7).$$

Observação

Um cuidado deve ser tomado. Apesar da recíproca ser verdadeira pelo item 3 da proposição 2.1, a implicação

$$ac \equiv bc\ (mod\ n) \Rightarrow a \equiv b\ (mod\ n)$$

não é válida. Por exemplo, $6 \equiv 2\ (mod\ 4)$, isto é, $2 \cdot 3 \equiv 2 \cdot 1\ (mod\ 4)$, porém não é verdade que $3 \equiv 1\ (mod\ 4)$. Para tratar disto, temos a

Proposição 2.2. (Cancelamento do termo comum)

Se $a, b, c \in \mathbb{Z}$ e $n \in \mathbb{N}$ são tais que $ac \equiv bc \ (mod\ n)$, então $a \equiv b \ (mod\ \frac{n}{d})$, onde $d = mdc(c, n)$.

Exemplo.

Mostrar que, para $a, b, c \in \mathbb{Z}$ e $n \in \mathbb{N}$, se $ac \equiv bc \ (mod\ n)$ e se c e n são primos entre si, então

$$a \equiv b \ (mod\ n).$$

Solução: Como n e c são primos entre si, deve ser $mdc(c, n) = 1$ e o resultado é imediato.

Exemplo.

Todo inteiro é côngruo, módulo n, a seu resto na divisão por n.

Definição 2.2. (Resíduo)

Sejam $a \in \mathbb{Z}$ e $n \in \mathbb{N}$. Um inteiro b tal que $a \equiv b \ (mod\ n)$ é dito *resíduo de a módulo n*.

Definição 2.3. (Sistema Completo de Resíduos - SCR)

Dizemos que o conjunto $S = \{r_1, r_2, r_3, ..., r_n\}$ é um *Sistema Completo de Resíduos (SCR) módulo n* se são satisfeitas as condições:

1. $r_i \not\equiv r_j \ (mod\ n)$ sempre que $i \neq j, \quad i, j \in I_n$;
2. para todo inteiro a, existe $i \in I_n$ tal que $a \equiv r_i \ (mod\ n)$.

Exemplo.

Mostrar que o conjunto $S = \{0, 1, 2\}$ é um Sistema Completo de Restos módulo 3.

Solução: É claro que quaisquer dois elementos de S são incongruentes módulo 3. Devemos, portanto, mostrar que todo e qualquer número é congruente módulo 3 a um destes elementos. De fato, pelo Algoritmo da Divisão, segue-se que, para algum $k \in \mathbb{Z}$, n é de uma das seguintes formas:

i) $n = 3k$;

ii) $n = 3k + 1$;

iii) $n = 3k + 2$.

Em cada um dos casos, n será congruente a 0, 1 ou 2, respectivamente, como queríamos mostrar.

Lema 2.1. (SCR trivial)

Seja $n \in \mathbb{N}$. O conjunto $S = \{0, 1, 2, 3, ..., n-1\}$ é um Sistema Completo de Restos módulo n.

Sumário

Congruências Lineares

Definição 2.4. (Congruência Linear)

Sejam $a, b, x \in \mathbb{Z}$ e $n \in \mathbb{N}$. Chamamos de *congruência linear* toda congruência da forma

$$ax \equiv b \ (mod\ n).$$

O conjunto dos x para os quais esta congruência é verdadeira é chamado de *conjunto solução* da congruência linear.

Exemplo.

$6x \equiv 2 \ (mod\ 3)$ é um exemplo de congruência linear. O conjunto solução desta congruência é vazio, pois $mdc(6, 3) = 3$ e $3 \nmid 2$, isto é, $6x \equiv 2 \ (mod\ 3)$ não tem solução.

Exemplo.

A congruência linear $8x \equiv 4 \ (mod\ 6)$ tem solução, pois $mdc(8,6) = 2$ e $2|4$. Uma das soluções é 2, visto que $6|(8 \cdot 2 - 4)$. Além desta, 8, 14, -4, ou qualquer número da forma $2+6k,\ k \in \mathbb{Z}$ também é solução da congruência, pois

$$8 \cdot 2 \equiv 4 \ (mod\ 6) \tag{1}$$

e

$$8 \cdot 6k \equiv 0 \ (mod\ 6). \tag{2}$$

Somando (1) com (2), obtemos

$$8 \cdot 2 + 8 \cdot 6k \equiv 4 + 0 \ (mod\ 6),$$

ou seja,

Exemplo. (continuação)

$$8 \cdot (2 + 6k) \equiv 4 \ (mod\ 6).$$

Note, por fim, que 5 também é solução da congruência $8x \equiv 4 \ (mod\ 6)$, porém, 5 não é da forma $2 + 6k$, que só gera números pares. Portanto, o conjunto

$$S' = \{2 + 6k : k \in \mathbb{Z}\}$$

não contém todas as soluções desta congruência.

Definição 2.5. (Soluções distintas)

Duas soluções x_1 e x_2 da congruência linear

$$ax \equiv b \ (mod \ n)$$

são ditas *distintas módulo n* se

$$x_1 \not\equiv x_2 \ (mod \ n).$$

Congruências Lineares

Exemplo.

Assim, na congruência $8x \equiv 4 \ (mod\ 6)$, 2 e 5 são duas soluções incongruentes módulo 6, pois $2 \not\equiv 5 \ (mod\ 6)$, e, portanto, são soluções distintas módulo 6. Porém, as soluções do conjunto S' são todas congruentes módulo 6, pois $2 + 6k_1 \equiv 2 + 6k_2 \ (mod\ 6)$, $\forall\ k_1, k_2 \in \mathbb{Z}$.

Teorema 2.4. (Quantidade de soluções incongruentes)

Sejam $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$ e $d = mdc(a, n)$. Se $d|b$, então a congruência linear

$$ax \equiv b \ (mod\ n)$$

possui exatamente d soluções incongruentes módulo n.

Corolário 2.2. (Caso $d = 1$)

Se $mdc(a, n) = 1$, a congruência linear $ax \equiv b \ (mod\ n)$ tem uma única solução módulo n.

Congruências Lineares

Exemplo.

Resolver a congruência linear $12x \equiv 6 \ (mod \ 9)$ e encontrar soluções distintas módulo 9.

Solução: Como $mdc(12, 9) = 3$, a congruência tem exatamente 3 soluções distintas módulo 9. Uma destas soluções é $x_0 = 2$, pois $12 \cdot 2 - 6 = 18 = 2 \cdot 9$. Como

$$\frac{9}{mdc(12, 9)} = \frac{9}{3} = 3,$$

obtemos o conjunto de soluções

$$S = \{2 + 3k : k \in \mathbb{Z}\}.$$

Três soluções distintas módulo 9 são, por exemplo, 2, 5 e 8.

Exemplo.

Resolver a congruência linear $3x \equiv 15 \ (mod\ 2)$.

Solução: Primeiramente, note que resolver esta congruência é equivalente a resolver a congruência $3x \equiv 1 \ (mod\ 2)$, pois $15 \equiv 1 \ (mod\ 2)$. Como 3 e 2 são primos entre si, a congruência tem solução única módulo 2. Uma solução particular é $x_0 = 1$. Assim, o conjunto solução desta congruência é

$$S = \{1 + 2k : k \in \mathbb{Z}\}.$$

Lema 2.3.

Seja $r_i \in \mathbb{Z}$, para cada $i \in I_n$. Se $S = \{r_1, r_2, r_3, ..., r_n\}$ é um SCR módulo n, então $S_a = \{a \cdot r_1, a \cdot r_2, a \cdot r_3, ..., a \cdot r_n\}$ também é, desde que $mdc(a, n) = 1$.

Demonstração. Como S_a tem n elementos, precisamos apenas mostrar que estes são incongruentes dois a dois. Então, para cada $i, j \in I_n$, consideremos a congruência $ar_i \equiv ar_j \pmod{n}$. Como $mdc(a, n) = 1$, podemos cancelar o termo a e obter

$$r_i \equiv r_j \ (mod\ n).$$

Mas isso só acontece se $i = j$, pois $r_i, r_j \in S$, que é um SCR módulo n. Ou seja, os elementos de S_a são dois a dois incongruentes módulo n. Portanto, S_a é um SCR módulo n. ■

Teorema 2.4. (Pequeno Teorema de Fermat)

Se $p \in \mathbb{P}$, $a \in \mathbb{Z}$ e $p \nmid a$, então

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

Demonstração. Como $p \in \mathbb{P}$ e $p \nmid a$, segue-se que $mdc(a, p) = 1$. Se considerarmos o SCR módulo n trivial

$$S = \{0, 1, 2, 3, ..., p - 1\}$$

, o Lema 2.3 nos garante que $S_a = \{0, a, 2a, 3a, ..., (p - 1)a\}$ também é um SCR módulo n. Daí, cada elemento de S é congruente a um único elemento de S_a (estão numa correspondência biunívoca). É óbvio que $0 \equiv 0 \ (mod\ p)$. Portanto, ainda temos uma correspondência biunívoca do conjunto $S \backslash \{0\}$ com o conjunto $S_a \backslash \{0\}$.

Não sabemos quais são os pares de números congruentes gerados por esta correspondência, mas podemos multiplicar as congruências membro a membro. Fazendo isso, e reorganizando se necessário, obtemos

$$a \cdot 2a \cdot 3a \cdot ... \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) \ (mod\ p),$$

ou seja,

$$1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) \cdot a^{p-1} \equiv 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) \ (mod\ p).$$

Como p não divide nenhum número da lista $1, 2, 3, ..., p-1$, deve ser primo com todos eles. Cancelando estes termos, ficamos com

$$a^{p-1} \equiv 1 \ (mod\ p)$$

■

Exemplo.

Calcule o resto da divisão de $97^{88} + 89^{96}$ por 8633.
Solução: observe que $8633 = 97 \cdot 89$. Por Fermat,

$$89^{96} \equiv 1 \ (mod\ 97) \tag{3}$$

e

$$97^{88} \equiv 1 \ (mod\ 89). \tag{4}$$

Ora, $97 \equiv 0 \ (mod\ 97)$. Logo, $97^{88} \equiv 0 \ (mod\ 97)$. Somando isto a (3), obtemos

$$89^{96} + 97^{88} \equiv 1 + 0 \equiv 1 \ (mod\ 97).$$

Analogamente, $89^{96} \equiv 0 \ (mod\ 89)$. Somando a (4), obtemos

Exemplo. (continuação)

$$89^{96} + 97^{88} \equiv 1 + 0 \equiv 1 \ (mod\ 89).$$

Ou seja,

$$89|(89^{96} + 97^{88} - 1) \text{ e } 97|(89^{96} + 97^{88} - 1).$$

Como $mdc(89, 97) = 1$, pelo Teorema 1.6, segue-se que

$$89 \cdot 97|(89^{96} + 97^{88} - 1),$$

isto é,

$$97^{88} + 89^{96} \equiv 1 \ (mod\ 8633).$$

Portanto, $97^{88} + 89^{96}$ deixa resto 1 na divisão por 8633.

Sistema Reduzido de Resíduos

Definição 2.7. (SRR)

Dizemos que um conjunto $R = \{r_1, r_2, r_3, ..., r_k\}$, onde $r_i \in \mathbb{Z}$, $\forall\ i \in I_k$, é um *Sistema Reduzido de Resíduos (SRR) módulo* n se as seguintes condições são satisfeitas:

1. $mdc(r_i, n) = 1, \forall\ i \in I_k$;
2. $r_i \not\equiv r_j\ (mod\ n)$, se $i, j \in I_k$ e $i \neq j$; e
3. para cada $m \in \mathbb{N}$ com $mdc(m, n) = 1$, $\exists\ i \in I_k$ tal que $m \equiv r_i\ (mod\ n)$.

Sistema Reduzido de Resíduos

Exemplo.

Como bem sabemos, o conjunto $S = \{0, 1, 2, 3, 4, 5\}$ é um SCR módulo 6. Dentre os elementos de S, os únicos não primos com 6 são os números: 0, pois $mdc(0, 6) = 6$; 2, pois $mdc(2, 6) = 2$; 3, pois $mdc(3, 6) = 3$; e 4, pois $mdc(4, 6) = 2$. "Retirando" estes elementos de S, ficamos com o conjunto $R = \{1, 5\}$, que é um sistema reduzido de resíduos módulo 6 (verifique!).

Sistema Reduzido de Resíduos

Lema 2.4.

Se $R = \{r_1, r_2, r_3, ..., r_{\varphi(n)}\}$ é um SRR módulo n, então $R_a = \{a \cdot r_1, a \cdot r_2, a \cdot r_3, ..., a \cdot r_{\varphi(n)}\}$ também é um SRR módulo n, desde que se tenha $mdc(a, n) = 1$.

Sumário

Sumário

Definição 3.1. (Resíduo Quadrático)

Sejam $a, n \in \mathbb{Z}$ e primos entre si. Se $x^2 \equiv a \ (mod\ n)$ tiver solução, dizemos que a é um *resíduo quadrático módulo n*. Em caso contrário, isto é, $x^2 \not\equiv a \ (mod\ n)$ para todo inteiro x, dizemos que *a não é um resíduo quadrático módulo n*, ou ainda, a é um *resíduo não-quadrático*.

Exemplo.

Na congruência $x^2 \equiv 2 \ (mod\ 7)$, tem-se que 2 é resíduo quadrático módulo 7, pois $mdc(2, 7) = 1$ e $7|(3^2 - 2)$, isto é, $x = 3$ é solução da congruência.

Congruências Quadráticas

Teorema 3.1.

Se a congruência $x^2 \equiv a \ (mod\ p)$ tiver solução, ela tem exatamente duas soluções incongruentes módulo p, onde $p \in \mathbb{P}^*$, $mdc(p, a) = 1$ e $a \in \mathbb{Z}$.

Exemplo 3.3.

A congruência $3x^2 \equiv 12(mod\ 13)$ possui ou não solução?

Solução: Notemos que a congruência tem solução pois, para $x = 2$, tem-se que $3 \cdot 2^2 \equiv 12 \ (mod\ 13)$. Além disso, pelo Teorema 3.1, -2 também é solução.

Teorema 3.2. (Teorema de Lagrange)

Se $mdc(c_n, p) = 1$, com $p \in \mathbb{P}$, então a congruência

$$f(x) \equiv 0 \ (mod \ p)$$

tem, no máximo, n soluções incongruentes módulo p, onde

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + ... + c_2 x^2 + c_1 x + c_0 \text{ e } c_i \in \mathbb{Z}, \ i \in I_n.$$

Demonstração. Utilizemos o Princípio de Indução Finita sobre o grau do polinômio. Notemos que para $n = 1$ o resultado é válido, pois temos a congruência $c_1 x + c_0 \equiv 0 \ (mod \ p)$, ou ainda,

$$c_1 x \equiv -c_0 \ (mod \ p),$$

que possui uma única solução incongruente módulo p, pelo Corolário 2.2 do Teorema 2.4. Suponhamos válido para $n = k - 1$, isto é, se $g(x)$ é um polinômio de grau $k - 1$, então a congruência $g(x) \equiv 0 \ (mod \ p)$ tem, no máximo, $k - 1$ soluções incongruentes módulo p. Mostremos que o resultado é válido para $n = k$. Para tanto, suponhamos que não valha, isto é, que a congruência

$$c_k x^k + c_{k-1} x^{k-1} + ... + c_2 x^2 + c_1 x + c_0 \equiv 0 \ (mod \ p)$$

tenha (pelo menos) $k + 1$ soluções incongruentes módulo p. Digamos que estas soluções sejam: $x_0, x_1, x_2, ..., x_k$. Fixando x_0, temos que

$$f(x) - f(x_0) \equiv 0 \ (mod \ p)$$

tem $k + 1$ soluções distintas módulo p, pois $f(x_0) \equiv 0 \ (mod \ p)$.

Congruências Quadráticas

Mas,

$$\begin{aligned} f(x) - f(x_0) &= c_k x^k + ... + c_1 x + c_0 - (c_k x_0^k + ... + c_1 x_0 + c_0) \\ &= c_k(x^k - x_0^k) + c_{k-1}(x^{k-1} - x_0^{k-1}) + ... + c_1(x - x_0). \end{aligned}$$

Percebamos que $(x - x_0)$ é um fator comum de cada parcela $c_i(x^i - x_0^i)$, com $i \in I_k$. Assim, para todo $i \in I_k$, tem-se

$$c_i(x^i - x_0^i) = (x - x_0) \cdot p_{i-1}(x),$$

onde $p_{i-1}(x)$ é um polinômio de grau $i - 1$. Seja

$$h(x) = \sum_{i=0}^{k-1} p_i(x).$$

Então $h(x)$ é um polinômio de grau $k-1$, com c_k sendo o coeficiente de x^{k-1}. Daí,

$$f(x) - f(x_0) = (x - x_0) \cdot h(x) \equiv 0 \ (mod \ p),$$

e isto significa que $p|(x - x_0) \cdot h(x)$. Como $p|(x - x_0) \Leftrightarrow x = x_0$, segue que $p|h(x)$ para todo $x_i, \quad i \in I_k$. Ou seja, a congruência

$$h(x) \equiv 0 \ (mod \ p)$$

possui k soluções incongruentes módulo p, contrariando a hipótese de indução. Logo, o resultado é válido para $n = k$ e, pelo PIF, vale para todo polinômio satisfazendo as condições do teorema.

■

Resíduos Quadráticos

Lema 3.1.

Seja $p \in \mathbb{P}^*$. Se $x, y \in \left\{1, 2, ..., \frac{p-1}{2}\right\}$, com $x \neq y$, então $x^2 \not\equiv y^2 \ (mod\ p)$.

Definição 3.2. (Função Maior Inteiro)

A função

$$\begin{array}{rccl} f: & \mathbb{R} & \longrightarrow & \mathbb{Z} \\ & x & \longmapsto & \lfloor x \rfloor \; = \text{máx}\{m \in \mathbb{Z} : m \leq x\} \end{array}$$

é denominada *função maior inteiro*.

Teorema 3.3.

Seja $p \in \mathbb{P}^*$. Dentre os números $1, 2, 3, ..., p-1$, temos exatamente $\lfloor \frac{p}{2} \rfloor$ resíduos quadráticos módulo p.

Exemplo.

Do Teorema 3.3 decorre que 6 é a quantidade de resíduos quadráticos que o primo ímpar 13 possui, assim como 15 é a quantidade de resíduos quadráticos módulo 31 e 18 é a quantidade de resíduos quadráticos módulo 37.

Sumário

Definição 3.3. (Símbolo de Legendre)

Sejam $a \in \mathbb{Z}$ e $p \in \mathbb{P}^*$. O *Símbolo de Legendre de a módulo p*, denotado por $(\frac{a}{p})$ (lê-se: a legendre p), é definido como:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{ se } p \nmid a \text{ e } a \text{ é resíduo quadrático módulo } p; \\ 0, \text{ se } p|a; \\ -1, \text{ se } p \nmid a \text{ e } a \text{ não é resíduo quadrático módulo } p. \end{cases}$$

Símbolo de Legendre, Critério de Euler e Lema de Gauss

Exemplo.

Determine:

1. $\left(\dfrac{1}{7}\right)$;
2. $\left(\dfrac{2}{3}\right)$;
3. $\left(\dfrac{110}{11}\right)$.

Solução: Note que resolver os problemas acima consiste em analisar se $p|a$ ou se $p \nmid a$ e, neste caso, se a congruência $x^2 \equiv a \ (mod\, p)$ tem solução. Deste modo,

1. $x^2 \equiv 1 \ (mod \ 7)$, $7 \nmid 1$ e $x = 1$ é solução, então $\left(\frac{1}{7}\right) = 1$;
2. $x^2 \equiv 2 \ (mod \ 3)$, $3 \nmid 2$, mas 2 não é resíduo quadrático módulo 3, uma vez que a congruência não tem solução, então $\left(\frac{2}{3}\right) = -1$;
3. $x^2 \equiv 110 \ (mod \ 11)$, então $\left(\frac{110}{11}\right) = 0$, pois $11|110$.

Teorema 3.4. (Critério de Euler)

Se $p \in \mathbb{P}^*$ e $mdc(p, a) = 1$, então

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (mod\ p).$$

Demonstração. Vamos considerar os casos em que a é ou não resíduo quadrático módulo p.
1º caso: a é resíduo quadrático módulo p. Então a congruência

$$a \equiv x^2 \ (mod\ p)$$

tem solução. Seja x_0 uma solução. Então $p \nmid x_0$, pois $p|(a - x_0^2)$ e, se $p|x_0$, teríamos $p|x_0^2$, o que implica que $p|a$, contrariando a hipótese.

Símbolo de Legendre, Critério de Euler e Lema de Gauss

Assim, por Fermat,

$$x_0^{p-1} \equiv 1 \ (mod \ p),$$

ou seja,

$$(x_0^2)^{\frac{p-1}{2}} \equiv 1 \ (mod \ p). \tag{5}$$

Por outro lado, como $a \equiv x_0^2 \ (mod \ p)$, segue que

$$a^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} \ (mod \ p). \tag{6}$$

Por transitividade em (6) e (5), temos que, se a é resíduo quadrático módulo p,

$$a^{\frac{p-1}{2}} \equiv 1 \equiv \left(\frac{a}{p}\right) \ (mod \ p).$$

2º caso: a não é resíduo quadrático módulo p.
Como $p \in \mathbb{P}^*$ e $mdc(p, a) = 1$, por Fermat, temos que

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

isto é,

$$p|[(a^{\frac{p-1}{2}})^2 - 1] = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1).$$

Como p é primo, segue que $p|(a^{\frac{p-1}{2}} - 1)$ ou $p|(a^{\frac{p-1}{2}} + 1)$, o que significa

$$a^{\frac{p-1}{2}} \equiv 1 \ (mod\ p) \quad \text{ou} \quad a^{\frac{p-1}{2}} \equiv -1 \ (mod\ p). \tag{7}$$

Símbolo de Legendre, Critério de Euler e Lema de Gauss

Seja

$$X = \left\{ i^2 : 1 \leq i \leq \frac{p-1}{2} \right\}.$$

Notemos que $a \notin X$, pois todo elemento de X é resíduo quadrático. Mostremos que todo elemento de X satisfaz $x^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$. Para isso, seja $k \in X$. Então $k = i^2$ para algum $i \in I_{\frac{p-1}{2}}$. Como $|i| \leq \frac{p-1}{2}$, tem-se $p \nmid i$, donde, por Fermat, $i^{p-1} \equiv 1 \ (mod\ p)$, o que equivale a $(i^2)^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$, ou seja, $k^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$, $\forall\ k \in X$.

Pelo Teorema de Lagrange, o polinômio

$$f(x) = x^{\frac{p-1}{2}} - 1 \equiv 0 \ (mod\ p)$$

tem, no máximo, $\frac{p-1}{2}$ raízes. Mas X tem $\frac{p-1}{2}$ elementos que satisfazem $f(x) \equiv 0 \ (mod\ p)$. Portanto, vale a implicação

$$k \text{ satisfaz } x^{\frac{p-1}{2}} \equiv 1 \ (mod\ p) \ \Rightarrow \ k \in X. \tag{8}$$

Como $a \notin X$, por (8), segue que a não satisfaz $x^{\frac{p-1}{2}}$. Assim, por (7), segue que, se a não é resíduo quadrático módulo p,

$$a^{\frac{p-1}{2}} \equiv -1 \equiv \left(\frac{a}{p}\right) \ (mod\ p).$$

■

Exemplo.

Como $2^4 \equiv -1 \ (mod\ 17)$, segue que $2^8 \equiv 1 \ (mod\ 17)$. Assim, pelo Critério de Euler, $\left(\frac{2}{17}\right) \equiv 2^{\frac{17-1}{2}} \equiv 2^8 \equiv 1 \ (mod\ 17)$. E isso só é verdadeiro se

$$\left(\frac{2}{17}\right) = 1.$$

Da definição do símbolo de Legendre também chegamos a esse resultado, pois 6 é solução da congruência $x^2 \equiv 2 \ (mod\ 17)$.

Teorema 3.5.

O Símbolo de Legendre é uma função completamente multiplicativa, isto é,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Exemplo.

Como o símbolo de Legendre é completamente multiplicativo, temos que

$$\left(\frac{8}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{4}{7}\right) = 1.$$

De fato, pois 3 é solução da congruência $x^2 \equiv 2 \ (mod\ 7)$ e 2 é solução da congruência $x^2 \equiv 4 \ (mod\ 7)$.

Teorema 3.6. (Lema de Gauss)

Sejam $a \in \mathbb{Z}$, $mdc(p, a) = 1$ e $p \in \mathbb{P}^*$. Consideremos os restos na divisão por p dos números

$$a, 2a, 3a, ..., \left(\frac{p-1}{2}\right) a.$$

Então,

$$\left(\frac{a}{p}\right) = (-1)^r,$$

onde r é o número dos restos que são maiores do que $\frac{p}{2}$.

Demonstração. Digamos que $a_1, a_2, ..., a_s$ sejam os restos menores que $\frac{p}{2}$ e $b_1, b_2, ..., b_r$ sejam os maiores que $\frac{p}{2}$.

Símbolo de Legendre, Critério de Euler e Lema de Gauss

Pelo Exemplo 2.5, cada elemento da lista $1a, 2a, ..., \frac{p-1}{2}a$ é congruente a seu resto, isto é, a um a_i ou um b_j, com $i \in I_s$ e $j \in I_r$. Não sabemos quais são os pares de números congruentes gerados por esta correspondência, mas podemos multiplicar todas as congruências membro a membro, obtendo

$$1a \cdot 2a \cdot 3a \cdot ... \cdot \frac{p-1}{2}a \equiv a_1 a_2 \cdots a_s b_1 b_2 \cdots b_r \ (mod\ p).$$

Reescrevendo a congruência e multiplicando por $(-1)^r$, temos

$$(-1)^r \cdot a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^r a_1 a_2 \cdots a_s b_1 b_2 \cdots b_r \ (mod\ p). \quad (9)$$

Nossa demonstração consistirá agora em concluir que

$$a_1, a_2, ..., a_s, p - b_1, p - b_2, ..., p - b_r \tag{10}$$

são, a menos da ordem, os números $1, 2, ..., \frac{p-1}{2}$.

Uma vez que $\frac{p}{2} \leq b_j < p$, multiplicando por -1 e somando p a todos os membros da desigualdade, decorre que:

$$p - p < p - b_j < p - \frac{p}{2} = \frac{p}{2},$$

isto é, $1 \leq p - b_j \leq \frac{p-1}{2}$. Assim, basta mostrarmos que os números da lista (10) são todos incongruentes módulo p.

Para $i \in I_s$ e $j \in I_r$, suponhamos que $a_i \equiv b_j \ (mod \ p)$. Então $p|(a_i - b_j)$, o que é absurdo, pois $|a_i - b_j| \leq p$ e $a_i \neq b_j$. Logo, $a_i \not\equiv b_j \ (mod \ p)$. Além disso, $a_i \not\equiv p - b_j \ (mod \ p)$, qualquer que seja $i \in I_s$ e $j \in I_r$. A prova disso é que, se existissem $i \in I_s$ e $j \in I_r$ tais que $a_i \equiv p - b_j \ (mod \ p)$, então, como $p \equiv 0 \ (mod \ p)$, teríamos $a_i \equiv -b_j \ (mod \ p)$. Mas isto também é absurdo, pois a_i e b_j são côngruos a um dos elementos do conjunto $\{1a, 2a, ..., \frac{p-1}{2}a\}$ e $mdc(a, p) = 1$, o que nos fornece, após manipulações utilizando as propriedades de congruência, $k \equiv -t \ (mod \ p)$ com $k, t \in \{1, 2, ..., \frac{p-1}{2}\}$. Portanto, os números da lista (10) são os mesmos elementos da lista $1, 2, ..., \frac{p-1}{2}$.

Símbolo de Legendre, Critério de Euler e Lema de Gauss

Logo, por reflexividade,

$$a_1 a_2 \cdots a_s (p - b_1)(p - b_2) \cdots (p - b_r) \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot \left(\frac{p-1}{2}\right) \ (mod\, p),$$

o que, eliminando as parcelas côngruas a 0 após o desenvolvimento do produto do membro esquerdo, equivale a

$$(-1)^r a_1 a_2 \cdots a_s b_1 b_2 \cdots b_r \equiv \left(\frac{p-1}{2}\right)! \ (mod\ p).$$

Por transitividade com a congruência (9),

$$(-1)^r a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! \ (mod\ p).$$

Eliminando $(\frac{p-1}{2})!$ em ambos os membros (por que podemos fazer isso?), obtemos

$$(-1)^r a^{\frac{p-1}{2}} \equiv 1 \ (mod\ p).$$

Multiplicando ambos os membros por $(-1)^r$, teremos

$$a^{\frac{p-1}{2}} \equiv \ (-1)^r \ (mod\ p).$$

Mas, pelo Critério de Euler,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (mod\ p).$$

Assim,

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^r \ (mod\ p),$$

cuja validade implica

$$\left(\frac{a}{p}\right) = (-1)^r,$$

como queríamos demonstrar. $\blacksquare$

Exemplo.

Tomemos $a = 3$ e $p = 11$ no Lema de Gauss. Calculando os restos módulo 11 dos múltiplos de 3

$$1 \cdot 3,\ 2 \cdot 3,\ 3 \cdot 3,\ 4 \cdot 3 \text{ e } 5 \cdot 3,$$

temos:

$$\begin{array}{ll} 1 \cdot 3 \equiv 3\ (mod\ 11); & 4 \cdot 3 \equiv 1\ (mod\ 11); \\ 2 \cdot 3 \equiv 6\ (mod\ 11); & 5 \cdot 3 \equiv 4\ (mod\ 11). \\ 3 \cdot 3 \equiv 9\ (mod\ 11); & \end{array}$$

Dentre estes restos, apenas 6 e 9 são maiores do que $\frac{11}{2}$, ou seja, $r = 2$. Assim, pelo Lema de Gauss,

$$\left(\frac{3}{11}\right) = (-1)^2 = 1.$$

Sumário

Suplementos à Lei de Reciprocidade Quadrática

Teorema 3.7. (1º Teorema Suplementar)

Se $p \in \mathbb{P}^*$, então

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{se} \quad p \equiv 1 \ (mod\ 4); \\ -1, & \text{se} \quad p \equiv -1 \ (mod\ 4). \end{cases}$$

Demonstração. Pelo Algoritmo da Divisão, na divisão por 4, todos os inteiros são da forma $4k, 4k+1, 4k+2$ ou $4k+3$. Como p é ímpar, as possibilidades se reduzem a $4k+1$ ou $4k+3$. É fácil ver que $p = 4k+1$ equivale a $p \equiv 1 \ (mod\ 4)$ e que $p = 4k+3$ equivale a $p \equiv 3 \equiv -1 \ (mod\ 4)$. Vamos analisar o valor de $(-1)^{\frac{p-1}{2}}$ em cada um destes casos.

Suplementos à Lei de Reciprocidade Quadrática

1º caso: $p = 4k + 1$.

Então $p - 1 = 4k$, isto é, $\frac{p-1}{2} = 2k$ é par. Daí, $(-1)^{\frac{p-1}{2}} = 1$. Pelo Critério de Euler,

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv 1 \ (mod\ p),$$

ou seja,

$$\left(\frac{-1}{p}\right) = 1, \text{ se } p \equiv 1 \ (mod\ 4).$$

2º caso: $p = 4k + 3$.

Então $p - 1 = 4k + 2 = 2(2k + 1)$, isto é, $\frac{p-1}{2} = 2k + 1$ é ímpar. Daí, $(-1)^{\frac{p-1}{2}} = -1$. Pelo Critério de Euler,

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \equiv -1 \ (mod\ p),$$

ou seja,

$$\left(\frac{-1}{p}\right) = -1, \text{ se } p \equiv -1 \ (mod\ 4).$$

$\blacksquare$

Exemplo.

O Teorema 3.7 nos fornece $\left(\frac{-1}{13}\right) = 1$, pois $13 \equiv 1 \ (mod\ 4)$. De fato, -1 é um resíduo quadrático módulo 13, pois 5 é solução da congruência $x^2 \equiv -1 \ (mod\ 13)$. E, pelo mesmo teorema, $\left(\frac{-1}{7}\right) = -1$, já que $7 \equiv 3 \ (mod\ 4)$. Com efeito, a congruência $x^2 \equiv -1 \ (mod\ 7)$ não tem solução, pois, pelo Algoritmo da Divisão, x é da forma $7k, 7k+1, ..., 7k+5$ ou $7k+6$. Assim, x^2+1 é da forma

$$7r+1, 7r+2, 7r+3 \ \text{ ou } 7r+5,$$

e, em nenhum destes casos, $7|(x^2+1)$. Por isso, pela definição do símbolo de Legendre, $\left(\frac{-1}{7}\right) = -1$.

Suplementos à Lei de Reciprocidade Quadrática

Proposição 3.1

Seja n um natural ímpar maior do que 2. Então vale a igualdade

$$1 + 2 + 3 + ... + \frac{n-1}{2} = \frac{n^2-1}{8}.$$

Demonstração. Exercício.

Utilizaremos este resultado no próximo teorema.

Teorema 3.8. (2º Teorema Suplementar)

Se $p \in \mathbb{P}^*$, então

$$\left(\frac{2}{p}\right) = \begin{cases} \quad 1, & \text{se} \quad p \equiv \pm 1 \ (mod\ 8); \\ -1, & \text{se} \quad p \equiv \pm 3 \ (mod\ 8). \end{cases}$$

Demonstração. Pelo Critério de Euler, $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}}$. Mostraremos que a validade da congruência

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \ (mod\ p) \tag{11}$$

será suficiente para, por transitividade, concluirmos o teorema. Para isto, consideraremos todos os possíveis restos de p na divisão por 8.

Mas antes, vamos demonstrar que a congruência (11) é verdadeira.

Seja $i \in \{1, 2, 3, ..., \frac{p-1}{2}\}$. Então, se i é par, segue que

$$i \equiv 2k \equiv 2k \cdot (-1)^{2k} \equiv i \cdot (-1)^{i} \ (mod\ p).$$

Se, porém, i é ímpar, segue que

$$p-i \equiv p-(2k+1) \equiv -(2k+1) \equiv (-1)^{2k+1} \cdot (2k+1) \equiv (-1)^{i} \cdot i \ (mod\ p).$$

Ou seja, para números pares, podemos afirmar congruências do tipo

$$i \equiv i \cdot (-1)^{i} \ (mod\ p), \tag{12}$$

e, para números ímpares, podemos formar congruências do tipo

$$p - i \equiv (-1)^{i} \cdot i \ (mod\ p). \tag{13}$$

Percebamos que, em ambos os tipos, (12) ou (13), os números dos membros esquerdos das congruências são sempre números pares. Mais ainda, estes números são $2, 4, 6, ..., p-1$. Assim, multiplicando todas essas $\frac{p-1}{2}$ congruências membro a membro, obtemos

$$2\cdot 4\cdot 6\cdot ...\cdot (p-1) \equiv 1\cdot 2\cdot ...\cdot \frac{p-1}{2}\cdot (-1)^1\cdot (-1)^2\cdot ...\cdot (-1)^{\frac{p-1}{2}} \ (mod\, p),$$

ou seja,

$$2\cdot 4\cdot 6\cdot ...\cdot (p-1) \equiv \left(\frac{p-1}{2}\right)!(-1)^{(1+2+...+\frac{p-1}{2})} \ (mod\ p).$$

Mas

$$2 \cdot 4 \cdot 6 \cdot ... \cdot (p-1) = 2^{\frac{p-1}{2}} (\frac{p-1}{2})!$$

e, pela Proposição 3.1,

$$1 + 2 + ... + \frac{p-1}{2} = \frac{p^2-1}{8}.$$

Assim,

$$2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{p^2-1}{8}} \left(\frac{p-1}{2}\right)! \ (mod\ p).$$

Cancelando o fator $(\frac{p-1}{2})!$ em ambos os membros, obtemos o resultado.

Agora, precisamos mostrar que

$$(-1)^{\frac{p^2-1}{8}} = 1, \text{ se } p \equiv \pm 1 \ (mod\ 8)$$

e

$$(-1)^{\frac{p^2-1}{8}} = -1, \text{ se } p \equiv \pm 3 \ (mod\ 8).$$

Como p é ímpar, pelo Algoritmo da Divisão, p é de uma das seguintes formas: $8k+1, 8k+3, 8k+5$ ou $8k+7$. Vamos analisar cada um destes quatro casos e, em cada um deles, utilizaremos a igualdade

$$\frac{p^2-1}{8} = \frac{(p-1)(p+1)}{8}. \tag{14}$$

1º caso: $p = 8k + 1$.

Então $p - 1 = 8k + 1 - 1 = 8k$ e $p + 1 = 8k + 1 + 1 = 8k + 2$. Substituindo em (14), obtemos

$$\frac{8k(8k+2)}{8} = \frac{8 \cdot 2k(4k+1)}{8} = 2(4k^2 + k).$$

Assim, se $p = 8k + 1$, então $\frac{p^2-1}{8}$ é par. Portanto,

$$(-1)^{\frac{p^2-1}{8}} = 1, \text{ se } p \equiv 1 \ (mod\ 8).$$

2º caso: $p = 8k + 3$.

Então $p - 1 = 8k + 3 - 1 = 8k + 2$ e $p + 1 = 8k + 3 + 1 = 8k + 4$. Substituindo em (14), temos

$$\frac{(8k+2)(8k+4)}{8} = \frac{8 \cdot (4k+1)(2k+1)}{8} = (4k+1)(2k+1).$$

Assim, se $p = 8k + 3$, então $\frac{p^2-1}{8}$ é ímpar. Portanto,

$$(-1)^{\frac{p^2-1}{8}} = -1, \text{ se } p \equiv 3 \ (mod\ 8).$$

3º caso: $p = 8k + 5$.

Então $p-1 = 8k+5-1 = 8k+4$ e $p+1 = 8k+5+1 = 8k+6$. Substituindo em (14), segue que

$$\frac{(8k+4)(8k+6)}{8} = \frac{8 \cdot (2k+1)(4k+3)}{8} = (2k+1)(4k+3).$$

Assim, se $p = 8k+5$, então $\frac{p^2-1}{8}$ é ímpar. Daí,

$$(-1)^{\frac{p^2-1}{8}} = -1, \text{ se } p \equiv 5 \equiv -3 \ (mod\ 8).$$

4º caso: $p = 8k + 7$.

Então $p - 1 = 8k + 7 - 1 = 8k + 6$ e $p + 1 = 8k + 7 + 1 = 8k + 8$. Substituindo em (14), obtemos

$$\frac{(8k+6)(8k+8)}{8} = \frac{8 \cdot 2(4k+3)(k+1)}{8} = 2(4k+3)(k+1).$$

Assim, se $p = 8k + 7$, então $\frac{p^2-1}{8}$ é par. Portanto,

$$(-1)^{\frac{p^2-1}{8}} = 1, \text{ se } p \equiv 7 \equiv -1 \ (mod\ 8),$$

o que conclui o teorema. ∎

Exemplo.

Do Teorema 3.8, segue que $\left(\frac{2}{5}\right) = -1$ e $\left(\frac{2}{7}\right) = 1$, pois $5 \equiv -3 \ (mod\ 8)$ e $7 \equiv -1 \ (mod\ 8)$. Esse é o mesmo resultado obtido através da definição do símbolo. Com efeito, a congruência $x^2 \equiv 2 \ (mod\ 5)$ não tem solução, pois o Algoritmo da Divisão garante que x é da forma

$$5t, 5t+1, 5t+2, 5t+3 \text{ ou } 5t+4.$$

Daí, $x^2 - 2$ é da forma

$$5m+2, 5m+3 \text{ ou } 5m+4,$$

e nenhum destes números é múltiplo de 5, donde $\left(\frac{2}{5}\right) = -1$. Por outro lado, 3 é solução da $x^2 \equiv 2 \ (mod\ 7)$ e, por isso, $\left(\frac{2}{7}\right) = 1$.

Sumário

Nesta seção apresentaremos um importante teorema que nos ajudará a determinar a solução para o símbolo de Legendre. Conhecendo o valor para $\left(\frac{p}{q}\right)$, será que temos condições de determinarmos $\left(\frac{q}{p}\right)$? A Lei mostrará em qual caso isso é possível.

O próximo resultado é fundamental para a demonstração da Lei. Para demonstrá-lo, utilizaremos alguns resultados, tais como o Algoritmo da Divisão e o Lema de Gauss. Pedimos aos espectadores, caso não recordem, que revejam estes teoremas.

Teorema 3.9.

Sendo $M = \left\lfloor \frac{a}{p} \right\rfloor + \left\lfloor \frac{2a}{p} \right\rfloor + \left\lfloor \frac{3a}{p} \right\rfloor + ... + \left\lfloor \frac{p-1}{2} \cdot \frac{a}{p} \right\rfloor$, a um inteiro ímpar e $p \in \mathbb{P}^*$, tal que $mdc(p, a) = 1$, temos

$$\left(\frac{a}{p}\right) = (-1)^M.$$

Demonstração. Nossa demonstração consiste, inicialmente, em determinar os restos módulo p de $Y_a = \{a, 2a, ..., \frac{p-1}{2}a\}$.

Lei de Reciprocidade Quadrática

Para isso, apliquemos o Algoritmo da Divisão para cada elemento do conjunto Y_a:

$$\begin{aligned} a &= p\left\lfloor \frac{a}{p} \right\rfloor + r_1 \\ 2a &= p\left\lfloor \frac{2a}{p} \right\rfloor + r_2 \\ 3a &= p\left\lfloor \frac{3a}{p} \right\rfloor + r_3 \\ &\vdots \\ \frac{p-1}{2}a &= p\left\lfloor \frac{p-1}{2} \cdot \frac{a}{p} \right\rfloor + r_{\frac{p-1}{2}} \end{aligned}$$

Perceba que cada $r_1, r_2, ..., r_{\frac{p-1}{2}}$ são os a_i e b_j definidos na demonstração do Lema de Gauss (com a característica de serem menores do que $\frac{p}{2}$ e maiores do que $\frac{p}{2}$, respectivamente). Agora, somando membro a membro cada uma das igualdades acima, obtemos

$$a\left(1+...+\frac{p-1}{2}\right)=p\left(\left\lfloor\frac{a}{p}\right\rfloor+...+\left\lfloor\frac{p-1}{2}\cdot\frac{a}{p}\right\rfloor\right)+r_1+...+r_{\frac{p-1}{2}},$$

o que, pela proposição 3.1, equivale a

$$\frac{p^2-1}{8}\cdot a=p\left(\left\lfloor\frac{a}{p}\right\rfloor+...+\left\lfloor\frac{p-1}{2}\cdot\frac{a}{p}\right\rfloor\right)+r_1+...+r_{\frac{p-1}{2}}.$$

Agora, seja $I = a_1 + a_2 + ... + a_s$ e $S = b_1 + b_2 + ... + b_r$, então

$$\frac{p^2-1}{8} \cdot a = pM + I + S. \qquad (3.3.11)$$

Mas, como verificamos na demonstração do Lema de Gauss, os números $a_1, a_2, ..., a_s, p-b_1, p-b_2, p-b_3, ..., p-b_r$ são, a menos da ordem, os números $1, 2, 3, ..., \frac{p-1}{2}$. Portanto,

$$1 + 2 + ... + \frac{p-1}{2} = a_1 + a_2 + ... + a_s + rp - (b_1 + b_2 + ... + b_r).$$

Daí,

$$\frac{p^2-1}{8} = I + rp - S. \qquad (3.3.12)$$

Logo, subtraindo 3.3.12 de 3.3.11, temos que

$$\frac{p^2-1}{8}(a-1) = p(M-r) + 2S.$$

Como a é ímpar por hipótese, segue que $\frac{(p^2-1)}{8} \cdot (a-1)$ é par, ou seja, $p(M-r)+2S$ é par. Como $2S$ é par, segue que $M-r$ também é par. Portanto M e r possuem a mesma paridade (são ambos pares ou ambos ímpares) e, pelo Lema de Gauss, sabemos que $\left(\frac{a}{p}\right) = (-1)^r$. Logo,

$$\left(\frac{a}{p}\right) = (-1)^M.$$

■

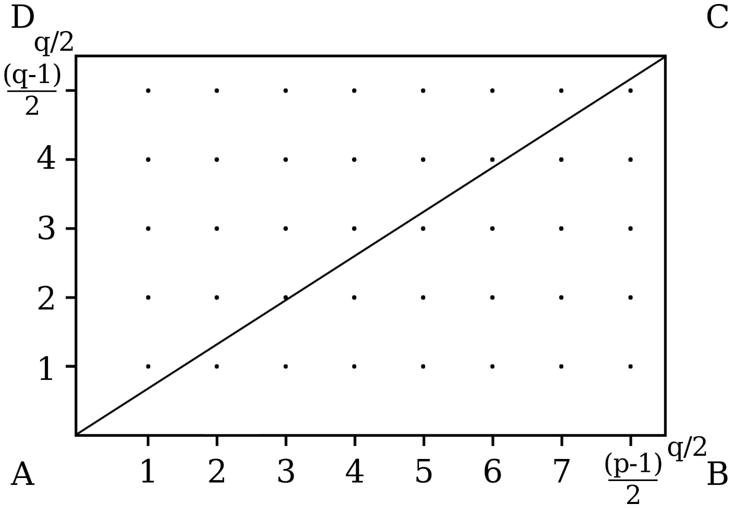
Lei de Reciprocidade Quadrática (LRQ)

Teorema 3.10 (LRQ)

Sejam $p, q \in \mathbb{P}^*$ distintos, então

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

DEMONSTRAÇÃO DA LEI



Observação

Como vimos na demonstração do Teorema 3.7, $\frac{p-1}{2}$ é par se, e somente se, $p \equiv 1 \ (mod \ 4)$. Desta forma, $\frac{p-1}{2} \cdot \frac{q-1}{2}$ é ímpar se, e só se, $p \equiv q \equiv 3 \ (mod \ 4)$. Assim, a depender do resto de p e q na divisão por 4, $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = 1$ ou -1. Ou seja, se pelo menos um, entre p e q, tiver resto 1 na divisão po 4, a Lei nos diz que

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right).$$

Lei de Reciprocidade Quadrática (LRQ)

Observação (continuação)

Se, porém, ambos p e q deixam resto 3 na divisão por 4, a Lei nos diz que

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right).$$

Portanto, podemos optar por calcular o mais simples entre os dois símbolos e, dessa forma, julgar se, no primeiro caso, ambos são ou não resíduos quadráticos e, no segundo caso, se um deles é e outro não.

Lei de Reciprocidade Quadrática (LRQ)

Exemplo.

Verifique se 6481 é resíduo quadrático módulo 6661, onde $6481, 6661 \in \mathbb{P}^*$.

Solução: Notemos que isto equivale a calcular $(\frac{6481}{6661})$. Como tanto 6481 quanto 6661 são primos ímpares, pela Lei de Reciprocidade Quadrática,

$$\left(\frac{6481}{6661}\right)\left(\frac{6661}{6481}\right) = (-1)^{\frac{6661-1}{2}\cdot\frac{6481-1}{2}} = 1,$$

ou seja, ou 6661 e 6481 são resíduos quadráticos ou ambos não são. Dessa forma, precisamos verificar apenas um deles.

Lei de Reciprocidade Quadrática (LRQ)

Exemplo. (continuação)

Primeiramente, note que

$$6661 \equiv 180 \ (mod\ 6481),$$

ou seja,

$$\left(\frac{6661}{6481}\right) = \left(\frac{180}{6481}\right).$$

Mas $180 = 2^2 \cdot 3^2 \cdot 5$, isto é,

$$\left(\frac{180}{6481}\right) = \left(\frac{2^2 \cdot 3^2 \cdot 5}{6481}\right) = \left(\frac{2^2}{6481}\right)\left(\frac{3^2}{6481}\right)\left(\frac{5}{6481}\right).$$

Lei de Reciprocidade Quadrática (LRQ)

Exemplo. (continuação)

Deste modo,

$$\left(\frac{180}{6481}\right) = \left(\frac{2^2}{6481}\right)\left(\frac{3^2}{6481}\right)\left(\frac{5}{6481}\right) = 1 \cdot 1 \cdot \left(\frac{5}{6481}\right) = \left(\frac{5}{6481}\right).$$

Como $5 \equiv 1 \ (mod\ 4)$, aplicando a Lei novamente, temos que

$$\left(\frac{5}{6481}\right) = \left(\frac{6481}{5}\right).$$

Lei de Reciprocidade Quadrática (LRQ)

Exemplo. (continuação)

Finalmente, pelo fato de $6481 \equiv 1 \ (mod\ 5)$, segue que

$$\left(\frac{6481}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Portanto, 6481 é resíduo quadrático módulo 6661.

Sumário

Símbolo de Jacobi

Como vimos, o Símbolo de Legendre de a módulo n está definido quando n é, necessariamente, um número primo ímpar. Podemos generalizar definindo o Símbolo de Jacobi que exige, tão somente, que n seja ímpar e $mdc(a, n) = 1$ para estar bem definido.

Definição 3.4. (Símbolo de Jaconi)

Sejam $a \in \mathbb{Z}$ e $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ a decomposição em fatores primos de um inteiro positivo e ímpar n, com $mdc(a, n) = 1$. *O símbolo de Jacobi*, denotado por $\left[\frac{a}{n}\right]$ (lê-se: a jacobi n), é definido por

$$\left[\frac{a}{n}\right] = \left[\frac{a}{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}}\right] = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_t}\right)^{\alpha_t}.$$

Símbolo de Jacobi

Observação

É importante ressaltar que, embora o símbolo de Jacobi seja uma extensão do símbolo de Legendre, ao contrário deste, pode ocorrer que a não seja resíduo quadrático módulo n mesmo que $\left[\frac{a}{n}\right] = 1$. Convidamos o leitor a exemplificar esta afirmação.

Teorema 3.12. (LRQ versão Jacobi)

Se $n, m \in \mathbb{Z}_+$, ímpares, são tais que $mdc(m,n) = 1$, então

$$\left[\frac{n}{m}\right]\left[\frac{m}{n}\right] = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

Demonstração. Sejam $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ e $q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$ as decomposições em fatores primos de n e m, respectivamente. Da definição do símbolo de Jacobi e pelo teorema 3.5, temos:

$$\left[\frac{n}{m}\right] = \prod_{j=1}^{s} \left(\frac{n}{q_j}\right)^{\beta_j} = \prod_{i=1}^{t} \prod_{j=1}^{s} \left(\frac{p_i}{q_j}\right)^{\beta_j \alpha_i},$$

e, analogamente,

Símbolo de Jacobi

$$\left[\frac{m}{n}\right] = \prod_{i=1}^{t} \left(\frac{m}{p_i}\right)^{\alpha_i} = \prod_{j=1}^{s} \prod_{i=1}^{t} \left(\frac{q_j}{p_i}\right)^{\alpha_i \beta_j}.$$

Multiplicando estas igualdades e agrupando os produtórios, obtemos

$$\left[\frac{n}{m}\right]\left[\frac{m}{n}\right] = \prod_{i=1}^{t} \prod_{j=1}^{s} \left\{ \left(\frac{p_i}{q_j}\right) \left(\frac{q_j}{p_i}\right) \right\}^{\alpha_i \beta_j}.$$

Pela Lei de Reciprocidade Quadrática, tem-se

$$\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = (-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}}. \tag{15}$$

Assim,

Símbolo de Jacobi

$$
\begin{aligned}
\left[\frac{n}{m}\right]\left[\frac{m}{n}\right] &= \prod_{i=1}^{t}\prod_{j=1}^{s}\left\{\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)\right\}^{\alpha_i\beta_j} \\
&= \prod_{i=1}^{t}\prod_{j=1}^{s}(-1)^{\alpha_i(\frac{p_i-1}{2})\beta_j(\frac{q_j-1}{2})} \\
&= \prod_{i=1}^{t}[(-1)^{\alpha_i(\frac{p_i-1}{2})\beta_1(\frac{q_1-1}{2})}\cdot\ldots\cdot(-1)^{\alpha_i(\frac{p_i-1}{2})\beta_s(\frac{q_s-1}{2})}] \\
&= \prod_{i=1}^{t}[(-1)^{\sum_{j=1}^{s}\alpha_i(\frac{p_i-1}{2})\beta_j(\frac{q_j-1}{2})}] \\
&= [(-1)^{\sum\alpha_1(\frac{p_1-1}{2})\beta_j(\frac{q_j-1}{2})}]\cdot\ldots\cdot[(-1)^{\sum\alpha_t(\frac{p_t-1}{2})\beta_j(\frac{q_j-1}{2})}] \\
&= (-1)^{\sum_{i=1}^{t}\sum_{j=1}^{s}\alpha_i(\frac{p_i-1}{2})\beta_j(\frac{q_j-1}{2})}.
\end{aligned}
$$

AFIRMAÇÃO:

$$\sum_{i=1}^{t}\sum_{J=1}^{s}\alpha_i(\frac{p_i-1}{2})\beta_J(\frac{q_j-1}{2}) \quad \text{e} \quad \frac{n-1}{2}\cdot\frac{m-1}{2}$$

têm a mesma paridade. Perceba que essa afirmação conclui a demonstração.

Dividiremos a demonstração da afirmação em duas partes. Mostraremos primeiramente que

$$\sum_{i=1}^{t}\alpha_i(\frac{p_i-1}{2}) \equiv \frac{n-1}{2} \ (mod\ 2).$$

Demonstração da AFIRMAÇÃO:

Notemos que

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t} =$$
$$= (1 + (p_1 - 1))^{\alpha_1} (1 + (p_2 - 1))^{\alpha_2} \cdots (1 + (p_t - 1))^{\alpha_t}$$

e, claro, que $p_i - 1$ é par, ou seja, $p_i - 1 = 2k$.
Dois fatos serão necessários à conclusão de nossa demonstração.
O primeiro é que $[1 + (p_i - 1)]^{\alpha_i} \equiv 1 + \alpha_i(p_i - 1) \ (mod\ 4)$. Para este, temos dois casos a considerar.

Símbolo de Jacobi

1º caso: α_i é par, i.e., $\alpha_i = 2v$.

Então $[1 + (p_i - 1)]^{\alpha_i} = (1 + 2k)^{2v}$ é da forma $1 + 4g$, e $1 + \alpha_i(p_i - 1) = 1 + 2v \cdot 2k$ é da forma $1 + 4h$, donde

$$[1 + (p_i - 1)]^{\alpha_i} \equiv 1 + \alpha_i(p_i - 1) \ (mod\ 4).$$

2º caso: α_i é ímpar, i.e., $\alpha_i = 2v + 1$.

Então $[1 + (p_i - 1)]^{\alpha_i} = (1 + 2k)^{2v+1} = (1 + 2k)^{2v} \cdot (1 + 2k)$ é da forma $1 + 4g + 2k$, e $1 + \alpha_i(p_i - 1) = 1 + (2v + 1) \cdot 2k$ é da forma $1 + 2k + 4h$, donde

$$[1 + (p_i - 1)]^{\alpha_i} \equiv 1 + \alpha_i(p_i - 1) \ (mod\ 4).$$

Símbolo de Jacobi

O segundo fato é que

$$(1+\alpha_i(p_i-1))(1+\alpha_j(p_j-1)) \equiv 1+\alpha_i(p_i-1)+\alpha_j(p_j-1)\ (mod\, 4).$$

Este fato é de verificação imediata, pois basta notar que, sendo (p_i-1) e (p_j-1) pares, $(p_i-1)(p_j-1)$ é da forma $4h$. Em geral, vale que

$$(1+\alpha_1(p_1-1))\cdots(1+\alpha_t(p_t-1)) \equiv 1+\alpha_1(p_1-1)+...+\alpha_t(p_t-1)\ (mod\, 4).$$

Símbolo de Jacobi

Ou seja,

$$n \equiv 1 + \alpha_1(p_1 - 1) + ... + \alpha_t(p_t - 1) \ (mod\ 4).$$

Daí,

$$\frac{n-1}{2} \equiv \frac{\alpha_1(p_1 - 1)}{2} + \frac{\alpha_2(p_2 - 1)}{2} + ... + \frac{\alpha_t(p_t - 1)}{2} \ (mod\ 2),$$

isto é,

$$\sum_{i=1}^{t} \alpha_i(\frac{p_i - 1}{2}) \equiv \frac{n-1}{2} \ (mod\ 2).$$

Analogamente mostra-se que

$$\sum_{j=1}^{s} \beta_j (\frac{q_j - 1}{2}) \equiv \frac{m-1}{2} \ (mod\ 2).$$

Portanto,

$$\sum_{i=1}^{t} \sum_{J=1}^{s} \alpha_i (\frac{p_i - 1}{2}) \beta_J (\frac{q_j - 1}{2}) \equiv \frac{n-1}{2} \cdot \frac{m-1}{2} \ (mod\ 2),$$

ou melhor,

$$\sum_{i=1}^{t} \sum_{J=1}^{s} \alpha_i (\frac{p_i - 1}{2}) \beta_J (\frac{q_j - 1}{2}) \quad \text{e} \quad \frac{n-1}{2} \cdot \frac{m-1}{2}$$

têm a mesma paridade, como queríamos demonstrar. ■

Símbolo de Jacobi

Exemplo.

Quanto vale $\left[\frac{25725}{17303}\right]$? E $\left[\frac{17303}{25725}\right]$?
Solução: Pelo Teorema 3.12,

$$\left[\frac{25725}{17303}\right]\left[\frac{17303}{25725}\right] = (-1)^{\frac{25725-1}{2}\frac{17303-1}{2}} = 1.$$

Símbolo de Jacobi

Exemplo. (continuação)

Como $25725 = 7^2 \cdot 7 \cdot 5^2 \cdot 3$ e $17303 = 11^2 \cdot 11 \cdot 13$, segue que

$$\left[\frac{17303}{25725}\right] = \left(\frac{17303}{7}\right)^2 \left(\frac{17303}{7}\right) \left(\frac{17303}{5}\right)^2 \left(\frac{17303}{3}\right) =$$

$$= \left(\frac{11^2}{7}\right) \left(\frac{11}{7}\right) \left(\frac{13}{7}\right) \left(\frac{11^2}{3}\right) \left(\frac{11}{3}\right) \left(\frac{13}{3}\right) =$$

$$= \left(\frac{11}{7}\right) \left(\frac{13}{7}\right) \left(\frac{11}{3}\right) \left(\frac{13}{3}\right).$$

Símbolo de Jacobi

Exemplo. (continuação)

Como $11 \equiv -3 \ (mod\ 7)$, $13 \equiv -1 \ (mod\ 7)$, $11 \equiv -1 \ (mod\ 3)$ e, ainda, $13 \equiv 1 \ (mod\ 3)$, tem-se

$$\left[\frac{17303}{25725}\right] = \left(\frac{11}{7}\right)\left(\frac{13}{7}\right)\left(\frac{11}{3}\right)\left(\frac{13}{3}\right) =$$

$$= \left(\frac{-3}{7}\right)\left(\frac{-1}{7}\right)\left(\frac{-1}{3}\right)\left(\frac{1}{3}\right) = \left(\frac{-1}{7}\right)^2\left(\frac{3}{7}\right)\left(\frac{-1}{3}\right) =$$

$$= \left(\frac{3}{7}\right)\left(\frac{-1}{3}\right).$$

Símbolo de Jacobi

Exemplo. (continuação)

Do fato de $3 \equiv -1 \ (mod\ 4)$, segue que $\left(\frac{-1}{3}\right) = -1$. Além disso, pelo Critério de Euler,

$$\left(\frac{3}{7}\right) \equiv 3^{\frac{7-1}{2}} \equiv 3^3 \equiv 27 \equiv -1 \ (mod\ 7),$$

isto é, $\left(\frac{3}{7}\right) = -1$. Portanto,

$$\left[\frac{25725}{17303}\right] = \left[\frac{17303}{25725}\right] = \left(\frac{3}{7}\right)\left(\frac{-1}{3}\right) = (-1) \cdot (-1) = 1.$$

Sumário

Referências

[da Rocha] da Rocha, L. V. A Lei de Reciprocidade Quadrática. Seminário Matemático (Disciplina de Licenciatura Matemática), Universidade de Coimbra, Departamento de Matemática: Faculdade de de Ciências e Tecnologia.

[1] Freire, B. T. V. (2009). Notas de aula - Teoria dos Números.

[2] Halmos, P. R. (2001). *Teoria Ingênua dos Conjuntos*. Ed. Ciência Moderna, Rio de Janeiro.

[3] Hefez, A. (2006). *Elementos de Aritmética*. Ed. SBM, Rio de Janeiro.

[4] Landau, E. (2002). *Teoria Elementar dos Números*. Ed. Ciência Moderna, Rio de Janeiro.

[5] Maier, R. R. (2005). Teoria dos Números - Texo de aula. Universidade de Brasília (Departamento de Matemática - IE).

Referências

[6] Martinez, F. B., Moreira, C. G., Saldanha, N., e Tengan, E. (2013). *Teoria dos Números - Um passeio com primos e outros números familiares pelo mundo inteiro*. IMPA, Rio de Janeiro.

[7] Milies, F. C. P. e Coelho, S. P. (2006). *Números: Uma introdução à matemática*. EDUSP, S.Paulo.

[8] Pickover, C. A. (2009). *The Math Book: From Pythagoras to the 57th Dimension, 250 Milestones in the History of Mathematics*. Sterling, New York.

[9] Santos, J. P. (2012). *Introdução à Teoria dos Números*. IMPA, Rio de Janeiro.

[Silva] Silva, A. A. Números, Relações e Criptografia. Universidade Federal da Paraíba, Centro de Ciências Exatas e da Natureza, Departamento de Matemática.

OBRIGADO!