Resíduos Quadráticos e o Símbolo de Legendre

Nicholas Farrel

March 2021

1 Definições Básicas

Definição: Seja p um primo e $a \in \mathbb{Z}$. Se existe $x \in \mathbb{Z}$ tal que $x^2 \equiv a \pmod{p}$, dizemos que a é um *resíduo quadrático* módulo p. Caso contrário, a é um resíduo não quadrático módulo p.

Símbolo de Legendre: Seja p um primo e $a \in \mathbb{Z}$ definimos:

$$\left(\frac{a}{p}\right) = 1 \iff a \text{ é resíduo quadrático módulo p}$$
$$\left(\frac{a}{p}\right) = -1 \iff a \text{ é resíduo não quadrático módulo p}$$
$$\left(\frac{a}{p}\right) = 0 \iff a \text{ é múltiplo de p}$$

Lê-se: $\left(\frac{a}{p}\right)$ como "a legendre p"

2 Critério de Euler e Propriedades do Símbolo de Legendre

Critério de Euler: Seja p um primo ímpar e $a \in \mathbb{Z}$ tal que $mdc(a,p) = 1$, temos os seguintes resultados:

$$\left(\frac{a}{p}\right) = 1 \iff a^{\frac{p-1}{2}} \equiv 1 \pmod p \qquad \left(\frac{a}{p}\right) = -1 \iff a^{\frac{p-1}{2}} \equiv -1 \pmod p$$

Prova.(Ida Caso 1) Se a é resíduo quadrático módulo p $\Rightarrow \left(\frac{a}{p}\right) = 1 \Rightarrow \exists x \in \mathbb{Z}$ tal que $x^2 \equiv a \pmod p$ logo,
$mdc(p,x) = mdc(p,a) = 1 \Rightarrow a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \pmod p$ assim, pelo Pequeno Teorem de Fermat, temos que $x^{p-1} \equiv 1 \pmod p \Rightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod p$ como queríamos demonstrar.
(Volta Caso 1) Assuma que $a^{\frac{p-1}{2}} \equiv 1 \pmod p$. Seja g uma raiz primitiva módulo p, então, sabemos que

$$\{g^1, g^2, \ldots, g^{p-1}\} \equiv \{1, 2, \ldots, p-1\} \pmod p$$

Da suposição, $mdc(a,p) = 1 \Rightarrow$ a congruência de a está no segundo conjunto acima. Tome então $k \in \{1, 2, \ldots, p-1\}$ tal que $g^k \equiv a \pmod p$. Assim $(g^k)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod p \Rightarrow g^{\frac{k(p-1)}{2}} \equiv 1 \pmod p$ Daí, como $p-1$ é a ordem de g módulo p $\Rightarrow p-1/\frac{k}{2}(p-1) \Rightarrow \frac{k}{2} \in \mathbb{Z}_{>0} \Rightarrow k = 2k_0$, com k_0 pertencente aos inteiros positivos, logo, como $g^k \equiv a \pmod p \Rightarrow g^{2k_0} \equiv a \pmod p$, donde, por definição, a é resíduo quadrático no módulo $p \Rightarrow \left(\frac{a}{p}\right) = 1$
(Caso 2) Seja a primo com $p \Rightarrow mdc(a,p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod p$ pelo Pequeno teorema de Fermat, logo $p/a^{p-1} - 1$ e como p é impar, podemos fatorar a diferença de quadrados e obter $p/(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1$. Como p é impar e o mdc destes dois fatores é 2, p divide apenas um, logo $p/a^{\frac{p-1}{2}} + 1 \iff p \nmid a^{\frac{p-1}{2}} - 1 \iff a$ é resíduo não quadrático módulo p, de acordo com o (Caso 1) ■

Propriedades do Símbolo de Legendre: Seja p um primo ímpar e $a, b \in \mathbb{Z}$ tais que $mdc(a,p) = mdc(b,p) = 1$. Então são válidas as seguintes propriedades:

*P1)*Se $a \equiv b \pmod p$ então $\left(\dfrac{a}{p}\right) = \left(\dfrac{b}{p}\right)$

P2)$\left(\dfrac{a^2}{p}\right) = 1$

P3)$\left(\dfrac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$(Aplicação direta do Critério de Euler)

P4)$\left(\dfrac{ab}{p}\right) = \left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$(Também válido para p divisor de a, b ou ambos, esta prova fica para o leitor)

P5)$\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Prova. *P1, P2, P3* são bem diretas das definições e do teorema já visto, vamos então provar as propriedades 4 e 5.

P4) Pelo Critério de Euler, temos que: $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p} \Rightarrow \left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p} \Rightarrow p/\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Porém, como $\left(\frac{x}{p}\right) = \pm 1$ é direto que $\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right) \in [-2, 2]$, como $p \neq 2$, o único múltiplo de p possível neste intervalo seria 0, o que nos dá: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, como queríamos demonstrar.

P5)Pelo Critério de Euler, temos que: $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p} \Rightarrow p/\left(\frac{-1}{p}\right) - (-1)^{\frac{p-1}{2}}$. Novamente, temos que $\left(\frac{-1}{p}\right) - (-1)^{\frac{p-1}{2}} \in [-2, 2]$ logo, o único múltiplo de p neste intervalo é o $0 \Rightarrow legendre{-}1p = (-1)^{\frac{p-1}{2}}$ ■

Corolário: Da Propriedade 5, temos então que:
-1 é resíduo quadrático módulo $p \iff p \equiv 1 \pmod{4}$
-1 é resíduo não quadrático módulo $p \iff p \equiv 3 \pmod{4}$

A partir dessas ideias inicias e propriedades, vamos derivar muitos teoremas relacionados a resíduos quadráticos, mas por enquanto,já podemos aplicar os conhecimentos aprendidos para resolver alguns problemas:

Exemplo 1. Mostre que existem infinitos primos da forma $4k + 1$.

Prova. Suponha que existam finitos primos da forma $4k + 1$: $\{p_1, p_2, \ldots, p_n\}$. Tome então o número $N = (p_1 p_2 \ldots p_n)^2 + 1$. Seja q um primo diferente de 2 que divide N, assim

$$(p_1 p_2 \ldots p_n)^2 \equiv -1 \pmod{q} \Rightarrow \left(\frac{-1}{q}\right) = 1 \Rightarrow (-1)^{\frac{p-1}{2}} = 1 \Rightarrow q \equiv 1 \pmod{4}$$

logo, $q = p_j$ para algum j $\Rightarrow q/(p_1 p_2 \ldots p_n)^2 \Rightarrow$ como $q/N \Rightarrow q/1$ o que é um absurdo. Logo, a afirmação inicial está incorreta, nos mostrando que existem infinitos primos da forma $4k+1$■

Exemplo 2. Seja p um primo ímpar, se n é o menor inteiro positivo que é resíduo não quadrático módulo p, prove que $n < \sqrt{p} + 1$.

Solução. Como nós só precisamos nos preocupar com as classes de resíduos módulo p, assuma que $1 \leq n \leq p - 1$ já que $mdc(n, p) = 1$. Seja então $an, a \in \mathbb{Z}_{>0}$ o menor múltiplo de n que é maior que $p \Rightarrow an - n < p < an \Rightarrow an = p + b$ com $0 < b < n$. Como $0 < b < n$, temos que , da propriedade de n ser o menor resíduo não quadrático, $\left(\frac{b}{p}\right) = 1 \Rightarrow$ como $b \equiv p + b \pmod{p} \Rightarrow$

$$\left(\frac{b+p}{p}\right) \equiv \left(\frac{b}{p}\right) \equiv 1 \pmod{p} (\text{P1}) \Rightarrow 1 \equiv \left(\frac{an}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{n}{p}\right) \equiv \left(\frac{a}{p}\right)(-1) \pmod{p} \Rightarrow \left(\frac{a}{p}\right) \equiv -1 \pmod{p}$$

logo, temos que $a \geq n \Rightarrow$

$n^2 \leq an = p+b < p+n \Rightarrow n(n-1) = n^2-n < p \Rightarrow (n-1)^2 < n(n-1) < p \Rightarrow n-1 < \sqrt{p} \Rightarrow n < \sqrt{p}-1$ ■

Exemplo 3. Prove que não existem a, b inteiros positivos tais que $4ab-a-b$ é um quadrado perfeito.

(IMO Shortlist 1984 adaptada)

Solução. Assuma que existam tais inteiros $a, b \Rightarrow \exists x \in \mathbb{Z}_{>0}$ tal que $4ab - a - b = x^2 \Rightarrow 4ab - b = x^2 + a \Rightarrow b(4a-1) = x^2 + a \Rightarrow b = \frac{x^2+a}{4a-1}$ como $b \in \mathbb{Z} \Rightarrow 4a - 1/x^2 + a$. Como $4a - 1 \equiv -1 \pmod 4 \Rightarrow 4a - 1$ tem ao menos um primo congruente a -1 no módulo 4 (caso contrário,$4a - 1 \equiv 1 \Rightarrow -1 \equiv 1 \pmod 4$ o que gera absurdo), assim seja $p = 4k+3, k \in \mathbb{Z}_{>0}$ tal primo. Temos:

$$4a \equiv 1 \pmod p \Rightarrow 4a^2 \equiv a \pmod p \Rightarrow (2a)^2 \equiv a \ (\mathrm{mod}\ ) \Rightarrow \left(\frac{a}{p}\right) = 1 \tag{1}$$

$$p/4a - 1 \Rightarrow p/x^2 + a \Rightarrow -a \equiv x^2 \pmod p \Rightarrow \left(\frac{-a}{p}\right) = 1 \tag{2}$$

de (1) e (2), e das propriedades *P4, P5* temos que:

$$1 = \left(\frac{-a}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{-1}{p}\right) = (1)(-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1 \Rightarrow 1 = -1 \Rightarrow \textit{Absurdo!}$$

Logo, nossa afirmação inicial estava incorreta e não existem tais a, b inteiros positivos.■

3 Teoremas e a Lei da Reciprocidade Quadrática!

Teorema 1. Seja p um primo ímpar.Então:

$$\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)=0$$

Ou seja, dentro do conjunto $\{1,2,\ldots,p-1\}$, métade do números são resíduos quadráticos módulo p e a outra são de números resíduos não quadráticos módulo p. Outra maneira frequente de enunciar este teorema é a seguinte:

$\left(\dfrac{a}{p}\right)\equiv 1 \pmod p$ e $\left(\dfrac{a}{b}\right)\equiv -1 \pmod p$ possuem ambas $\dfrac{p-1}{2}$ soluções incongruentes no módulo p.

Solução. Seja g uma raiz primitiva de p. Sabemos que $\{g^1,g^2,\ldots,g^{p-1}\}\equiv\{1,2,\ldots,p-1\}\Rightarrow$ para cada $a\in\{1,2,\ldots,p-1\}$ existe $k\in\{1,2,\ldots,p-1\}$ único tal que $a\equiv g^k \pmod p$

$$\left(\frac{a}{p}\right)=\left(\frac{g^k}{p}\right)\equiv(g^k)^{\frac{p-1}{2}}=(g^{\frac{p-1}{2}})^k\equiv(-1)^k \pmod p\Rightarrow\left(\frac{a}{p}\right)\equiv(-1)^k\Rightarrow$$
$$\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\equiv\sum_{k=1}^{p-1}(-1)^k\equiv 0 \pmod p$$

esta ultima veio de que temos $\frac{p-1}{2}$ ímpares e $\frac{p-1}{2}$ pares de 1 a k, logo, cada -1 cancela com cada $+1$ e como $\left(\frac{a}{p}\right)=\pm1\Rightarrow\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\in[-(p-1),p-1]$ assim, como o único múltiplo de p nesse intervalo é 0, temos que:

$$\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)=0\blacksquare$$

Corolário: Da prova passada, podemos concluir que se $\left(\frac{a}{p}\right)=1\Rightarrow a\equiv g^j \pmod p$ para j par e se $\left(\frac{a}{p}\right)=-1\Rightarrow a\equiv g^i \pmod p$ para i ímpar, e para alguma raiz primitiva g de p.

Lema de Gauss. Sejam p um primo ímpar e a um inteiro não nulo tal que $mdc(a,p)=1$. Se n denota o número de inteiros do conjunto $S=\{a,2a,3a,\ldots,\frac{p-1}{2}a\}$ cujo resto na divisão por p excede $\frac{p}{2}$, então $\left(\frac{a}{p}\right)=(-1)^n$

Prova. Dentre os $\frac{p-1}{2}$ restos, assuma que m deles são menores que $\frac{p}{2}\Rightarrow m+n=\frac{p-1}{2}$ então tome $\{r_1,r_2,\ldots,r_m\}$ os restos menores que $\frac{p}{2}$, e $\{s_1,s_2,\ldots,s_n\}$ os restos maiores que $\frac{p}{2}$.
Se $ai\equiv aj \pmod p$, com $\frac{p-1}{2}\geq i>j\geq 1\Rightarrow p/a(i-j)\Rightarrow$ como $mdc(a,p)=1\Rightarrow p/i-j$ o que gera absurdo, já que $\frac{p-1}{2}>i-j\geq 1$. Logo, todos os elementos de S são incongruentes dois a dois $\Rightarrow$

$$\{a,2a,3a,\ldots,\frac{p-1}{2}a\}\equiv\{r_1,\ldots,r_m,s_1,\ldots,s_n\} \pmod p\Rightarrow r_1\ldots r_m s_1\ldots s_n\equiv(\frac{p-1}{2})!a^{\frac{p-1}{2}} \pmod p$$

Pelo Critério de Euler, sabemos que $a^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right) \pmod p\Rightarrow$

$$r_1\ldots r_m s_1\ldots s_n\equiv(\frac{p-1}{2})!\left(\frac{a}{p}\right) \pmod p \tag{1}$$

Agora, vamos tentar trabalhar com outros fatos relacionados aos r_i's e s_j's.Veja que, como $\frac{p}{2} < s_j < p \Rightarrow 0 < p - s_j < \frac{p}{2}$, considere então o conjunto $T = \{r_1, \ldots, r_m, p - s_1, \ldots, p - s_n\}$, ja vimos que os r_i's são incongruentes dois a dois, então são distintos 2 a 2. Também, s_j's sao incongruentes 2 a 2, então também são distintos dois a dois o que nos dá que os $(p - s_j)$'s também são distintos e incongruentes dois a dois.
Suponha agora que existem índices $i \in \{1, 2, \ldots, m\}$ e $j \in \{1, 2, \ldots, n\}$ tais que $r_i \equiv p - s_j \pmod p \Rightarrow$ como existem $u, v \in \{1, 2, \ldots, \frac{p-1}{2}\}$ tais que $r_i \equiv ua \pmod p$ e $s_j \equiv va \pmod p \Rightarrow$

$$ua \equiv p - va \equiv 0 - va \pmod p \Rightarrow ua + uv \equiv 0 \pmod p \Rightarrow p/a(u+v) \Rightarrow p/u+v$$
$$\textit{Absurdo, pois } 0 < u + v < p - 1$$

Logo $r_i \not\equiv p - s_j \forall i, j \Rightarrow$ Os elementos de T são dois a dois incongruentes módulo p, por sua vez, como são menores que $\frac{p}{2}$, são dois a dois distintos. Assim, T possui $\frac{p-1}{2}$ elementos inteiros positivos todos distintos e menores que $\frac{p}{2} \Rightarrow \{r_1, \ldots, r_m, p - s_1, \ldots, p - s_n\} = \{1, 2, \ldots, \frac{p-1}{2}\} \Rightarrow r_1 \ldots r_m(p - s_1) \ldots (p - s_n) = (\frac{p-1}{2})! \Rightarrow$

$$r_1 \ldots r_m(p - s_1) \ldots (p - s_n) \equiv (\frac{p-1}{2})! \pmod p \Rightarrow r_1 \ldots r_m(-s_1) \ldots (-s_n) \equiv (\frac{p-1}{2})! \pmod p$$
$$\Rightarrow r_1 \ldots r_m s_1 \ldots s_n (-1)^n \equiv (\frac{p-1}{2})! \pmod p \Rightarrow r_1 \ldots r_m s_1 \ldots s_n \equiv (-1)^n (\frac{p-1}{2})! \pmod p \tag{2}$$

Agora, substituindo *(1)* em *(2)*

$$(\frac{p-1}{2})! \left(\frac{a}{p}\right) \equiv (-1)^n (\frac{p-1}{2})! \Rightarrow \text{ como } p \nmid (\frac{p-1}{2})! \Rightarrow \left(\frac{a}{p}\right) \equiv (-1)^n \pmod p$$

Como $2 \geq \left(\frac{a}{p}\right) - (-1)^n \geq -2 \Rightarrow \left(\frac{a}{p}\right) = (-1)^n \blacksquare$

Teorema 2. Se p é um primo ímpar, então:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Prova. Pelo Lema de Gauss, $\left(\frac{2}{p}\right) = (-1)^n$, onde n é a quantidade de inteiros positivos do conjunto $S = \{2, 2 \cdot 2, 2 \cdot 3, \ldots, (\frac{p-1}{2}) \cdot 2\}$ cujo resto na divisão por p excede $\frac{p}{2}$
Observe que o maior elemento de S é $\frac{p-1}{2} \cdot 2 = p - 1 < p \Rightarrow$ todos os elementos de S já são restos por p, assim n é a quantidade de elementos de S que excedem $\frac{p}{2}$. Vamos dividir em casos relacionados à congruência de p no módulo 8 para descobrir se n é par ou ímpar.
(Caso 1: $p \equiv 1 \pmod 8$) Daí temos que $p = 8k+1$ para algum inteiro positivo $k \Rightarrow \frac{p}{2} = 4k + \frac{1}{2} \Rightarrow S = \{2, 4, \ldots, 4k, 4k+2, \ldots, 8k\} \Rightarrow |S| = 4k$ e $n = 2k \Rightarrow$ Pelo Lema de Gauss$\left(\frac{2}{p}\right) = (-1)^n = (-1)^{2k} = 1 \Rightarrow \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ já que $\frac{p^2-1}{2}$ é par.
(Caso 2: p equiv$3 \pmod 8$) Daí temos que $p = 8k + 3$ para algum inteiro positivo $k \Rightarrow \frac{p}{2} = 4k + 1 + \frac{1}{2} \Rightarrow S = \{2, 4, \ldots, 4k, 4k+2, \ldots, 8k+2\} \Rightarrow n = 2k + 1 \Rightarrow \left(\frac{2}{p}\right) = (-1)^n = (-1)^{2k+1} = -1 \Rightarrow \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

(Caso 3: $p \equiv 5 \pmod 8$) Daí temos que $p = 8k+5$ para algum inteiro positvo $k \Rightarrow \frac{p}{2} = 4k+2+\frac{1}{2} \Rightarrow S = \{2, 4, \dots, 4k+2, 4k+4, \dots, 8k+4\} \Rightarrow n = 2k+1 \Rightarrow \left(\frac{2}{p}\right) = (-1)^n = (-1)^{2k+1} = -1 \Rightarrow \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
De todo caso, o teorema está demonstrado ■

Teorema 3. Seja p um primo ímpar e a um inteiro ímpar tal que $mdc(a,p) = 1$. Se:

$$x = \left\lfloor \frac{a}{p} \right\rfloor + \left\lfloor \frac{2a}{p} \right\rfloor + \cdots + \left\lfloor \frac{\frac{p-1}{2}a}{p} \right\rfloor$$

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

Prova. Pelo algorítimo da divisão, tome:

$$\begin{aligned} &a = pq_1 + t_1 \\ &2a = pq_2 + t_2 \\ &\dots\dots \\ &\frac{p-1}{2} \cdot a = pq_{\frac{p-1}{2}} + t_{\frac{p-1}{2}} \end{aligned}$$

Assim, temos que:

$$ai = pq_i + t_i \Rightarrow \frac{ai}{p} = q_i + \frac{t_i}{p} \Rightarrow \lfloor \frac{ai}{p} \rfloor = q_i, \forall i = 1, 2, \dots \frac{p-1}{2} \Rightarrow x = \sum_{i=1}^{\frac{p-1}{2}} q_i \tag{1}$$

O conjunto $\{t_1, t_2, \dots, t_{\frac{p-1}{2}}\}$ é o conjunto dos restos de $\{a, 2a, \dots, \frac{p-1}{1}a\}$, então, se n desses restos são mairoes que $\frac{p}{2}$e $m = \frac{p-1}{2} - n$ são menores que $\frac{p}{2}$, pelo Lema de Gauss, $\left(\frac{a}{p}\right) = (-1)^n$ vamos então mostrar que n e x possuem a mesma paridade.
Sejam $\{r_1, r_2, \dots, r_n\}$ e $\{s_1, s_2, \dots, s_m\}$ os dois conjuntos de restos que definimos na prova do Lema de Gauss, então, também da mesma prova,

$$\{r_1, \dots, r_m, p - s_1, \dots, p - s_n\} = \{1, 2, 3, \dots, \frac{p-1}{2}\} \tag{2}$$

De *(1)* temos que

$$\begin{aligned} &a + 2a + \cdots + \frac{p-1}{2}a = p(q_1 + \cdots + q_2) + r_1 + \cdots + r_m + s_1 + \dots s_n \Rightarrow \\ &a \cdot \frac{\frac{p-1}{2} \cdot \frac{p+1}{2}}{2} = px + \sum_{i=1}^{m} + \sum_{j=1}^{n} \Rightarrow \sum_{i=1}^{m} r_i + \sum_{j=1}^{n} s_j = a \cdot (\frac{p^2-1}{8}) - px \end{aligned} \tag{3}$$

De *(2)*

$$\begin{aligned} &r_1 + \cdots + r_m + (p - s_1) + \cdots + (p - s_n) = 1 + 2 + \cdots + \frac{p-1}{2} \Rightarrow \\ &\sum_{i=1}^{m} r_i - \sum_{j=1}^{n} s_j = \frac{p^2-1}{8} - np \end{aligned} \tag{4}$$

Agora, somando *(3)*, *(4)*

$$2 \cdot \sum_{i=1}^{m} r_i = \frac{p^2-1}{8} \cdot (a+1) - px - np \Rightarrow \text{ como } a \text{ é ímpar, } (a+1) \text{ é par} \Rightarrow$$
$$0 \equiv 0 - p(x+n) \pmod 2 \Rightarrow p(x+n) \equiv 0 \pmod 2 \Rightarrow x+n \equiv 0 \pmod 2 \Rightarrow$$
$$x \equiv n \pmod 2 \Rightarrow (-1)^x = (-1)^n \Rightarrow \left(\frac{a}{p}\right) = (-1)^x \blacksquare$$

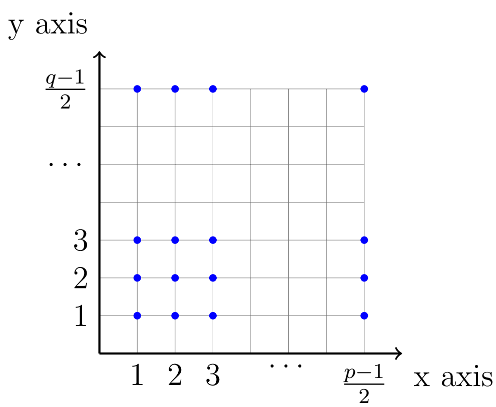
Lei da Reciprocidade Quadrática. Sejam p e q primos impares distintos. Então:

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

Prova. Defina:

$$X = \left\lfloor \frac{p}{q} \right\rfloor + \left\lfloor \frac{2p}{q} \right\rfloor + \cdots + \left\lfloor \frac{\frac{q-1}{2} \cdot p}{q} \right\rfloor \Rightarrow \left(\frac{p}{q}\right) = (-1)^X$$
$$Y = \left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{2q}{p} \right\rfloor + \cdots + \left\lfloor \frac{\frac{p-1}{2} \cdot q}{p} \right\rfloor \Rightarrow \left(\frac{q}{p}\right) = (-1)^Y$$

Vamos mostrar que $X + Y = \frac{p-1}{2} \cdot \frac{q-1}{2}$



Considere o retângulo mostrado na figura acima, cujos vértices possuem coordenadas $(1,1)$, $(1, \frac{q-1}{2})$,$(\frac{p-1}{2}, 1)$,$(\frac{p-1}{2}, \frac{q-1}{2})$. Marque todos os seus pontos, assim, marcamos um total de $\frac{p-1}{2} \cdot \frac{q-1}{2}$ pontos.Vamos então contar esta quandidade de pontos de outra maneira!
Considere a equação da reta l que passa pelos pontos $(0,0)$, $(\frac{p}{2}, \frac{q}{2}) \Rightarrow y = \frac{q}{p} \cdot x$. Se algum ponto de coordenadas inteiras (x_0, y_0) pertence a esta reta $\Rightarrow py_0 = qx_0 \Rightarrow p/x_0$ e q/y_0 o que gera absurdo, já que $1 \leq x_0 \leq \frac{p-1}{2}$ e $1 \leq y_0 \leq \frac{q-1}{2}$. Logo, tal reta não possui nenhum dos pontos marcados.Vamos contar a quandidade de pontos acima e abaixo desta reta.

*1º)*Considere agora a reta horizontal $y = k, 1 \leq k \leq \frac{q-1}{2}$. Etão, o número de pontos de coordenads inteiras na reta $y = k$ que estão acima de l é $\lfloor \frac{pk}{q} \rfloor$ de acordo com a equação da reta l. Logo, o total de pontos acima da reta l é:

$$\sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor = X$$

*2º)*Considere a reta vertical $x = k, 1 \leq k \leq \frac{p-1}{2}$.Então, o número de pontos de coordenadas inteiras na reta $x = k$ e estão abaixo de l é $\lfloor \frac{qk}{p} \rfloor$ de acordo com a equação da reta l. Logo, o total de pontos abaixo da reta l é:

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor = Y$$

Portanto, o total de pontos de coordenadas inteiras no retângulo é $X + Y = \frac{p-1}{2} \cdot \frac{q-1}{2} \Rightarrow \left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^X(-1)^Y = (-1)^{X+Y} \Rightarrow \left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$ ■

A partir de agora, temos o conteúdo necessário para resolver problemas (ou partes de problemas) que envolvam resíduos quadráticos. O exemplo a seguir utiliza todos os teoremas e conceitos vistos até agora:

Exemplo 4. Ache todos os primos p tais que $p! + p$ é um quadrado perfeito.

Solução: Inicialmente, vamos testar alguns casos iniciais:
Caso $p = 2$.Temos que $2 + 2! = 4$ que é quadrado perfeito.
Caso $p = 3$.Temos que $3 + 3! = 9$ que é quadrado perfeito.
Caso $p = 5$.Temos que $5 + 5! = 125$ que não é quadrado perfeito.
Caso $p = 7$.Temos que $7 + 7! = 5047$ que não é quadrado perfeito.
Agora, assuma que p é um primo maior que 7, também, assuma que $p + p! = a^2, a \in \mathbb{Z}_{>0}$, assim, temos que:
Como $p > 7 \Rightarrow 8/p! \Rightarrow a^2 = p + p! \equiv p + 0 \equiv p \pmod 8 \Rightarrow p \equiv a^2 \pmod 8 \Rightarrow$ como quadrados são congruentes a 0, 1, ou 4 no módulo 8, e p é ímpar, temos que $p \equiv 1 \pmod 8 \Rightarrow \frac{p^2-1}{8}$ é par $\Rightarrow$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1 \tag{1}$$

Considere agora q um primo menor que $p \Rightarrow q/p! \Rightarrow a^2 = p + p! \equiv p + 0 \equiv p \pmod q \Rightarrow p \equiv a^2 \pmod q$ logo, p é resíduo quadrático módulo $q \Rightarrow \left(\frac{p}{q}\right) = 1$ assim, pela Lei da Reciprocidade Quadrática e como $\frac{p-1}{2}$ é par:

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

Agora, se n é um número menor que p de fatoração em primos $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ sabemos que $p_i < p$ para todo i, assim, como de *(1)*, *(2)* todos os primos menores que p são resíduos quadráticos módulo p, temos da propriedade 4:

$$\left(\frac{n}{p}\right) = \left(\frac{p_1}{p}\right)^{\alpha_1} \cdots \left(\frac{p_k}{p}\right)^{\alpha_k} = 1 \cdots 1 = 1$$

assim, todos os inteiros menores que p são resíduos quadráticos módulo p, o que gera absurdo, pelo Teorema1. Logo, não existe primo maior que 7 tal que $p+p!$ é quadrado perfeito, então, os primos válidos são $p = 1, 2$■

4 Problemas

Problema 1. Prove que todo fator primo do número $(2^{2^n}+1)$, $n > 1$, é da forma $(2^{n+2}k+1)$ como $k \in \mathbb{Z}_{>0}$

Problema 2. Prove que se p é um primo da forma $4k+3$, então $2p+1$ também é primo $\iff 2p+1/2^p-1$

Problema 3. Se a é um inteiro positivo, defina $x_1 = a, x_{n+1} = 2x_n+1$. Ache o maior inteiro positvio k para o qual existe um inteiro positivo a tal que os números $\{2^{x_1}, 2^{x_2}, \cdots, 2^{x_k}\}$ são todos primos.

(Romanian Masters of Mathematics 2013)

Problema 4. Seja $k = 2^{2^n}+1$ para algum inteiro positivo n. Mostre que k é primo se e somente se k é fator de $3^{\frac{k-1}{2}}+1$

(Taiwanese Mathematical Olympiad 1997)

Problema 5. Sejam m, n inteiros positivos tsis que

$$A = \frac{(m+3)^n+1}{3m}$$

é um inteiro. Prove que A é ímpar.

(Bulgarin Mathematical Olympiad 1998)

Problema 6. Encontre todos os inteiros positivos n tais que $2^n-1/3^n-1$

(American Mathematical Monthly)

Problema 7. As sequências (a_n) e (b_n) são definidas como a seguir: $a_0 = 1, b_0 = 4$ e para $n \geq 0$:

$$a_{n+1} = a_n^{2001} + b_n$$
$$b_{n+1} = b_n^{2001} + a_n$$

Prove que 2003 não divide nenhum dos termos da sequência.

(Iberoamericana 2003)

Problema 8. Encontre todos os inteiros positivos n para os quais existe um inteiro m tal que m^2+9 é múltiplo de 2^n-1

(IMO Shortlist 1998)

Problema 9. Os inteiros positivos a e b são tais que os números $15a+16\text{b}$ e $16a-15b$ são ambos quadrados perfeitos. Qual é o menor valor possível que pode ter o menor destes dois números?

(IMO 1996)

Probleama 10. Encontre um número n entre 100 e 1997 tal que $n/2^n+2$

(APMO 1997)

5 Bibliografia

Number Theory - Structures, Examples, and Problems
://www.obm.org.br/content/uploads/2017/02/Matheus-Secco-Residuos$_{Q}uadraticos_{N}3.pdf$