Resíduos quadráticos

Prof. Dr. Vinícius Wasques

Universidade Estadual Paulista "Júlio de Mesquita Filho" - Campus Rio Claro

20 de julho de 2020

Equação quadrática

Seja $p > 2$ um número primo e $a, b, c \in \mathbb{Z}$ com a não divisível por p.

Resolver a equação quadrática

$$ax^2 + bx + c \equiv 0 \ (mod \ p)$$

é equivalente a resolver

$$(2ax + b)^2 \equiv b^2 - 4ac \ (mod \ p)$$

(Verifique. Veja que 2 e a são invertíveis módulo p)

A equação anterior pode então ser escrita na seguinte forma:

$$X^2 \equiv d \ (mod \ p).$$

Estamos interessados em encontrar critérios de existência para esse tipo de equações.

Se a equação acima admite solução, (isto é, se $\overline{d}$ é um "quadrado perfeito" em $\mathbb{Z}_p$), então dizemos que d é um *resíduo* ou *resto quadrático* módulo p.

Há exatamente $\frac{p+1}{2}$ resíduos quadráticos módulo p:

$$0^2, 1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2 \ mod\ p$$

já que todo inteiro x é congruente a $\pm i\ mod\ p$ para algum i tal que $0 \leq i \leq \frac{p-1}{2}$, de modo que x^2 é congruente a um dos números listados acima.

Perceba estes números são todos distintos, módulo p. De fato,

$$
\begin{aligned}
i^2 \equiv j^2 \ (mod\ p) \quad &\Rightarrow \quad p|(i-j)(i+j) \\
&\Leftrightarrow \quad p|i-j \ \ ou \ \ p|i+j \\
&\Leftrightarrow \quad i \equiv \pm j \ (mod\ p)
\end{aligned}
$$

Como

$$0 \leq i, j \leq \frac{p-1}{2} \Rightarrow 0 < i + j \leq p - 1 \ \text{ ou } \ i = j = 0,$$

temos que a única possibilidade é $i \equiv j \ (mod\ p)$.

Embora saibamos a lista completa dos resíduos quadráticos, reconhecê-los se torna uma tarefa complicada.

Por exemplo, sabemos dizer se 2 é resíduo quadrático módulo 1019?

A seguir, veremos algumas ferramentas que permitem responder estas questões de maneira bastante eficiente.

Resíduos Quadráticos e Símbolo de Legendre

Seja $p > 2$ um número primo e a um inteiro qualquer. Para simplificar cálculos e notações definiremos o chamado *símbolo de Legendre*:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se p não divide a e a é um resíduo quadrático módulo p} \\ 0, & \text{se p divide a} \\ -1, & \text{caso contrário} \end{cases}$$

Critério de Euler

Seja $p > 2$ um primo e a um inteiro qualquer. Então

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

Demonstração

Para $a \equiv 0 \ (mod \ p)$ o resultado é claro, de modo que podemos supor $p \nmid a$.

Pelo teorema de Fermat temos que

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

assim,

$$\begin{aligned}(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \ (mod \ p) \quad &\Leftrightarrow \quad p | a^{\frac{p-1}{2}} - 1 \ \text{ ou } \ p | a^{\frac{p-1}{2}} + 1 \\ &\Leftrightarrow \quad a^{\frac{p-1}{2}} \equiv \pm 1 \ (mod \ p).\end{aligned}$$

Assim, devemos mostrar que $a^{\frac{p-1}{2}} \equiv 1 \ (mod \ p)$ se, e só se, a é um resíduo quadrático módulo p.

Se a é um resíduo quadrático, digamos $a \equiv i^2 \ (mod \ p)$, novamente pelo teorema de Fermat temos que

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

Assim, os resíduos quadráticos $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ módulo p são raízes do polinômio $f(x) = x^{\frac{p-1}{2}} - \bar{1}$ em $\mathbb{Z}_p[x]$.

Como $\mathbb{Z}_p$ é corpo, segue que $f(x)$ pode ter no máximo $deg\ f = \frac{p-1}{2}$ raízes em $\mathbb{Z}_p$.

Isto mostra que as raízes de $f(x)$ são exatamente os resíduos quadráticos não congruentes a zero módulo p e que, portanto,

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

se, e só se, a é um resíduo quadrático módulo p.

Propriedades do símbolo de Legendre

1. se $a \equiv b \ (mod \ p)$ então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;
2. se $p \nmid a$, então $\left(\frac{a^2}{p}\right) = 1$;
3. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, ou seja, -1 é resíduo quadrático módulo p se, e só se, $p \equiv 1 \ (mod \ 4)$;
4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Demonstração: Exercício.

Exemplo:

O polinômio $f(x) = x^4 - 10x^2 + 1$ é irredutível em $\mathbb{Z}[x]$, mas é redutível módulo p para todo primo p.

Note que $f(x)$ é irredutível em $\mathbb{Z}[x]$, uma vez que só admite raízes irracionais.

De fato, se $p, q \in \mathbb{Z}$ são tais que $mdc(p, q) = 1$ e $f(\frac{p}{q}) = 0 \Leftrightarrow p^4 - 10p^2q^2 + q^4 = 0$, temos da última igualdade que $q|p^4 \Rightarrow q = \pm 1$ e $p|q^4 \Rightarrow p = \pm 1$ já que p e q são primos entre si.

Logo $\frac{p}{q} = \pm 1$, nenhuma das quais é raiz de $f(x)$ (cujos zeros são $\pm\sqrt{2}$ e $\pm\sqrt{3}$).

Logo, se $f(x)$ for redutível ele é o produto de dois polinômios de grau 2, que podemos supor mônicos.

Como o produto dos coeficientes independentes destes dois fatores deve ser igual ao coeficiente independente de $f(x)$, que é 1, temos apenas duas possibilidades

$$f(x) = (x^2 + ax + 1)(x^2 + bx + 1) \quad \text{ou}$$

$$f(x) = (x^2 + ax - 1)(x^2 + bx - 1)$$

com $a, b \in \mathbb{Z}$.

Em ambos os casos, temos $a + b = 0$ (coeficiente de x^3). Logo, no primeiro caso, comparando o coeficiente de x^2 temos

$$ab + 2 = -10 \Leftrightarrow a^2 = 12,$$

o que é impossível.

O segundo caso é análogo.

Agora, para p = 2 e p = 3 temos (verifique)

$$f(x) \equiv (x+1)^4 \ (mod\ 2) \quad \text{e} \quad f(x) \equiv (x^2+1)^2 \ (mod\ 3)$$

Agora se $p > 3$ é um primo, temos que

$$\left(\frac{2}{p}\right) = 1 \quad \text{ou} \quad \left(\frac{3}{p}\right) = 1 \quad \text{ou} \quad \left(\frac{6}{p}\right) = 1$$

já que $\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{6}{p}\right)$.

No primeiro caso, se $a^2 \equiv 2 \ (mod \ p)$ temos

$$f(x) \equiv (x^2 + 2ax - 1)(x^2 - 2ax - 1) \ (mod \ p).$$

Já no segundo caso, se $b^2 \equiv 3 \ (mod \ p)$ temos

$$f(x) \equiv (x^2 + 2bx + 1)(x^2 - 2bx + 1) \ (mod \ p).$$

Finalmente, no último caso, se $c^2 \equiv 6 \ (mod \ p)$ temos

$$f(x) \equiv (x^2 + 2c - 5)(x^2 - 2c - 5) \ (mod \ p).$$

Isto mostra que $f(x)$ é redutível módulo p para todo p primo.

Reciprocidade Quadrática

1. Sejam p e q primos ímpares distintos. Então

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

2. Seja p um primo ímpar. Então

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

Dem: Consultar Martinez et al. ou Niven and Zuckerman.

Observação:

Para demonstrar a lei da reciprocidade quadrática, é necessário utilizar o seguinte lema de Gauss:

Lema. Sejam $p > 2$ um número primo e a um inteiro positivo primo entre si com p. Seja s o número de elementos do conjunto

$$\left\{a, 2a, \ldots, \frac{p-1}{2}a\right\}$$

tais que seu resto módulo p é maior do que $\frac{p-1}{2}$. Então

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

Exercício:

Se p é da forma $4n-1$ então $p | n^n + (-1)^{n+1} 2n$

Exercício:

Se p é da forma $4n-1$ então $p|n^n+(-1)^{n+1}2n$

Por hipótese temos que $4n \equiv 1 \ (mod \ p)$ e assim

$$(4n)^n = 2^{2n}n^n \equiv 1 \ (mod \ p) \tag{1}$$

Por outro lado, como $p = 4n-1$, então $p-1 = 4n-2$ e consequentemente $2n-1 = \frac{p-1}{2}$.
Além disso, elevando ao quadrado em ambos os lados da equação $p = 4n-1$, podemos obter $\frac{p^2-1}{8} = n(2n-1)$.

Logo, pelo critério de Euler e pela reciprocidade quadrática, temos:

$$2^{2n-1} = 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} = (-1)^{n(2n-1)} \ (mod \ p)$$

Exercício:

Assim, $2^{2n-1} \equiv (-1)^{n(2n-1)} \ (mod \ p)$ e portanto

$$2^{2n} \equiv 2(-1)^n \ (mod \ p). \tag{2}$$

De (1) e (2), concluímos que $2n^n \equiv (-1)^n \ (mod \ p)$.

Multiplicando por $2n$ e utilizando o fato de que $4n \equiv 1 \ (mod \ p)$ obtemos $n^n \equiv 2n(-1)^n \ (mod \ p)$, que é equivalente a dizer

$$p | n^n + (-1)^{n+1} 2n$$

Resíduos quadráticos podem ser utilizados em aplicações na área de criptografia, por exemplo:

Criptografia via método de Rabin: `https://repositorio.ufpb.br/jspui/bitstream/tede/7480/2/arquivototal.pdf`

Sugestão de material complementar sobre resíduos quadráticos:
`https://www.youtube.com/watch?v=iICMAjyCzjw`

Referências

MARTINEZ, F.E.B; MOREIRA, C.G.T; SALDANHA, N.,T.; TENGAN, E. Teoria dos Números. Um passeio com Primos e outros Números Familiares pelo Mundo Inteiro. IMPA, 2013.

GRAHAM, R. L., KNUTH, D. E., PATASHNIK, O Matemática Concreta. LTC, São Paulo, 1995

NIVEN, I. E.; ZUCKERMAN, N.S. An Introduction to the Theory of Numbers, NY, John Wiley & Sons, 1991.

Contato

Prof. Dr. Vinícius Wasques

email: viniciuswasques@gmail.com

Departamento de Matemática

site: `https://viniciuswasques.github.io/home/`