

O TEOREMA DA RECIPROCIDADE QUADRÁTICA

FERNANDO FERREIRA

Nas aulas anteriores estudámos equações lineares em módulo. As próximas aulas debruçam-se sobre equações quadráticas. Neste caso ainda é possível dar uma resposta completa e satisfatória sobre a existência (ou não) de soluções modulares, mas a teoria é muito mais subtil. Sejam $b, c \in \mathbb{Z}$ e p um número primo. Queremos estudar a equação quadrática

$$x^2 + bx + c = 0 \pmod{p}$$

Como sabemos, para p primo ímpar, o número de soluções desta equação depende do valor do discriminante da equação, ou seja, depende do valor de $\Delta = b^2 - 4c$. Se $\Delta = 0 \pmod{p}$, a equação tem exatamente uma solução. Se $\Delta \neq 0 \pmod{p}$ e Δ é um quadrado módulo p , a equação tem exatamente duas soluções. Se Δ não é um quadrado módulo p , então a quadrática não tem soluções.

O estudo da existência de raízes duma quadrática módulo um primo p ímpar resume-se, portanto, ao estudo de saber se um dado inteiro a , com $a \perp p$ é, ou não, um quadrado módulo p . É tradicional usar a seguinte linguagem:

Definição 1. *Seja p um primo ímpar e a um número inteiro tal que $a \perp p$. Diz-se que a é resíduo quadrático módulo p se a equação $x^2 \equiv a \pmod{p}$ tem solução. Caso contrário, diz-se que a é não resíduo quadrático módulo p .*

Seja dado p um primo ímpar e a um inteiro co-primo com p . O símbolo de Legendre define-se do seguinte modo:

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{se } a \text{ é resíduo quadrático módulo } p \\ -1 & \text{se } a \text{ é não resíduo quadrático módulo } p \end{cases}$$

Quando está definido, o símbolo de Legendre é 1 ou -1. Para p primo ímpar e $a, b \in \mathbb{Z}$ com $a \perp p$ e $b \perp p$, tem-se:

- (i) se $a \equiv b \pmod{p}$, então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
- (ii) $\left(\frac{a^2}{p}\right) = 1$.
- (iii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

As primeiras duas propriedades são imediatas. A terceira é consequência do seguinte resultado:

Crítério de Euler. *Seja p um primo ímpar e $a \in \mathbb{Z}$ tal que $a \perp p$. Então:*

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

Munidos deste critério, é fácil de argumentar (iii):

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

Para demonstrar o critério de Euler vamos necessitar do seguinte resultado.

Lema 1. *Seja p um primo ímpar. Um inteiro a , com $a \perp p$, é resíduo quadrático módulo p se, e somente se, $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$*

Demonstração. Seja $r := \frac{p-1}{2}$. Começemos por ver que os quadrados não nulos \bar{a} de $\mathbb{Z}/p\mathbb{Z}$ são raízes do polinómio $X^r - \bar{1}$ sobre o corpo $\mathbb{Z}/p\mathbb{Z}$. Com efeito, se $\bar{a} = \bar{b}^2$ então $a^r \equiv (b^2)^r \equiv b^{p-1} \equiv 1$, módulo p (pequeno teorema de Fermat). Provámos, pois, a implicação da esquerda para a direita.

De seguida, vamos ver que os quadrados (não nulos) $\bar{1}^2, \bar{2}^2, \dots, \bar{r}^2$ de $\mathbb{Z}/p\mathbb{Z}$ são distintos dois a dois. Suponhamos que $\bar{m}^2 = \bar{n}^2$, onde $1 \leq n \leq m \leq r$. Então $m^2 - n^2 \equiv 0 \pmod{p}$. Logo, $(m+n)(m-n) \equiv 0 \pmod{p}$. Assim, ou $p \mid (m+n)$ ou $p \mid (m-n)$. O primeiro caso é impossível porque $m+n \leq 2r \leq p-1$. Conclui-se que $\bar{m} = \bar{n}$, como se queria.

Dado que o polinómio $X^r - \bar{1}$ tem no máximo r raízes, conclui-se que essas raízes são exatamente os quadrados $\bar{1}^2, \bar{2}^2, \dots, \bar{r}^2$. Como se queria. \square

Estamos agora em condições de demonstrar o critério.

Demonstração do critério de Euler. Seja $r := \frac{p-1}{2}$. Suponhamos que $\left(\frac{a}{p}\right) = 1$. Por definição, \bar{a} é um quadrado (não nulo) de $\mathbb{Z}/p\mathbb{Z}$. Logo, pelo lema, $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Temos, pois (neste caso), a igualdade do critério. Suponhamos agora que $\left(\frac{a}{p}\right) = -1$. Por definição, \bar{a} não é um quadrado módulo p . Pelo lema acima, $a^r \not\equiv 1 \pmod{p}$. Mas $(a^r)^2 \equiv a^{p-1} \equiv 1 \pmod{p}$. Assim, \bar{a}^r é raiz do polinómio $X^2 - \bar{1}$. Como \bar{a}^r não é $\bar{1}$, conclui-se que \bar{a} tem que ser $-\bar{1}$. Isto é o que se queria obter. \square

Note-se que, pelo discutido, podemos concluir que a aplicação $\bar{a} \rightsquigarrow \left(\frac{a}{p}\right)$ do grupo finito $(\mathbb{Z}/p\mathbb{Z})^*$ para o grupo multiplicativo de dois elementos $(\{-1, 1\}, \cdot)$ é um epimorfismo de grupos cujo núcleo é constituído exatamente pelos quadrados de $(\mathbb{Z}/p\mathbb{Z})^*$.

Quando a é -1 , o critério de Euler dá-nos a seguinte igualdade importante:

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

Equivalentemente:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1 \pmod{4} \\ -1 & \text{se } p \equiv 3 \pmod{4} \end{cases}$$

Dado um primo ímpar p fixo, o facto de a ser resíduo quadrático módulo p apenas depende, evidentemente, do resíduo de a módulo p . Esta é a propriedade (i) acima. O que acontece se, ao invés, fixarmos um inteiro (não nulo) a e percorrermos os vários primos p (com $p \perp a$)? Um teorema profundo de Gauss diz-nos que o facto de a ser ou não resíduo quadrático módulo p apenas depende do resíduo de p módulo $4|a|$. Por exemplo, como se poderá ver mais tarde, 7 é um resíduo quadrático módulo um primo ímpar p diferente de 7 se, e somente se, p é congruente com 1, 3, 9, 19, 25 ou 27 módulo 28.

Teorema (Reciprocidade quadrática). *Seja p um número primo ímpar e a um inteiro (não nulo) com $a \perp p$. O facto de a ser resíduo quadrático módulo p apenas depende do resíduo de p módulo $4|a|$.*

Usando o símbolo de Legendre, podemos reformular o teorema acima da seguinte maneira: Seja a um inteiro (não nulo) e p e q são primos ímpares tais $p \perp a$ e $q \perp a$; então

$$p \equiv q \pmod{4|a|} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$$

Para mostrar este teorema vamos demonstrar a lei da reciprocidade quadrática de Gauss. Esta lei descreve de modo preciso a dependência mencionada acima. Fá-lo-emos na próxima secção.