O TEOREMA DA RECIPROCIDADE QUADRÁTICA

FERNANDO FERREIRA

Nas aulas anteriores estudámos equações lineares em módulo. As próximas aulas debruçam-se sobre equações quadráticas. Não é difícil de dar uma resposta completa e satisfatória sobre a existência (ou não) de soluções modulares de quadráticas. Porém, em torno desta questão, podem ser estabelecidos factos inesperados e profundos, como é o caso da lei da reciprocidade quadrática.

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 raizes duma quadrática módulo um primo p ímpar resume-se, portanto, ao estudo de saber se um dado inteiro a, coprimo com p é, ou não, um quadrado módulo p. É costume usar a seguinte terminologia:

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 coprimo 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:

Critério 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 mostrar o seguinte resultado.

Lema 1. *Seja p um primo ímpar e $r = \frac{p-1}{2}$. As raízes do polinómio $X^r - \overline{1}$ sobre o corpo $\mathbb{Z}/p\mathbb{Z}$ são exatamente os quadrados $\overline{1}^2$, $\overline{2}^2$, ..., $\overline{r}^2$.*

Demonstração. Comecemos por ver que os quadrados não nulos $\overline{a}$ de $\mathbb{Z}/p\mathbb{Z}$ são raizes do polinómio $X^r - \overline{1}$. Com efeito, se $\overline{a} = \overline{b}^2$ então $a^r \equiv (b^2)^r \equiv b^{p-1} \equiv 1$, módulo p (pequeno teorema de Fermat). Provámos, pois, que $\overline{1}^2$, $\overline{2}^2$, ..., $\overline{r}^2$ são raízes do polinómio $X^r - \overline{1}$.

De seguida, vamos ver que os quadrados (não nulos) $\overline{1}^2$, $\overline{2}^2$, ..., $\overline{r}^2$ de $\mathbb{Z}/p\mathbb{Z}$ são distintos dois a dois. Suponhamos que $\overline{m}^2 = \overline{n}^2$, onde $1 \leqslant n \leqslant m \leqslant r$. 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 $2 \leqslant m + n \leqslant 2r \leqslant p - 1$. Conclui-se, pois, que $m = n$.

Dado que o polinómio $X^r - \overline{1}$ tem no máximo r raizes, conclui-se que as suas raizes são exatamente $\overline{1}^2$, $\overline{2}^2$, ..., $\overline{r}^2$. Como se queria. □

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, $\overline{a}$ é um quadrado (não nulo) de $\mathbb{Z}/p\mathbb{Z}$. Pelo pequeno teorema de Fermat, vem $a^r \equiv 1 \pmod{p}$. Suponhamos agora que $\left(\frac{a}{p}\right) = -1$. Por definição, $\overline{a}$ não é um quadrado módulo p. Logo não está na lista $\overline{1}^2$, $\overline{2}^2$, ..., $\overline{r}^2$. Pelo lema acima não se tem $a^r \equiv 1 \pmod{p}$. Ora, dado que $a^{2r} \equiv 1 \pmod{p}$ (pequeno teorema de Fermat), tem-se necessariamente $a^r \equiv -1 \pmod{p}$, pois o polinómio $X^2 - \overline{1}$ sobre o corpo $\mathbb{Z}/p\mathbb{Z}$ tem apenas as soluções $\overline{1}$ e $-\overline{1}$. □

Note-se que, pelo discutido, podemos concluir que a aplicação $\overline{a} \rightsquigarrow \left(\frac{a}{p}\right)$ 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 verá mais tarde num exercício, 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.