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.*

Dado um primo ímpar p fixo, o facto de a ser resíduo quadrático módulo p apenas depende, evidentemente, do resíduo de a módulo p. O que acontece se, ao invés, fixarmos um inteiro 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 $4a$. Por exemplo, 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 $a \in \mathbb{Z}$ com $a \perp p$. O facto de a ser resíduo quadrático módulo p apenas depende do resíduo de p módulo $4a$.*

Para mostrar este teorema vamos demonstrar a lei da reciprocidade quadrática de Gauss. Esta lei descreve de modo preciso a dependência mencionada no teorema acima. Fá-lo-emos na próxima secção. De seguida vamos introduzir alguma notação importante e demonstrar o chamado critério de Euler.

Seja dado p um primo ímpar e a um inteiro co-primo com p (i.e., p não divide a). 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:

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

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:*

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

Demonstração. Seja $r := \frac{p-1}{2}$. Comecemos por ver que os quadrados não nulos $\overline{a}$ de $\mathbb{Z}/p\mathbb{Z}$ são raízes do polinómio $X^r - \overline{1}$ de $\mathbb{Z}/p\mathbb{Z}[X]$. 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). Há, portanto, no máximo r quadrados não nulos em $\mathbb{Z}/p\mathbb{Z}$. Vamos ver que os quadrados (não nulos) $\overline{1}^2$, $\overline{2}^2$, $\ldots$, $\overline{r}^2$ de $\mathbb{Z}/p\mathbb{Z}$ são distintos dois a dois. Suponhamos que $\overline{n}^2 = \overline{m}^2$, onde $1 \leqslant n \leqslant m \leqslant r$. Então $n^2 - m^2 \equiv 0 \pmod{p}$. Logo, $(n+m)(n-m) \equiv 0 \pmod{p}$. Assim, ou $p \mid (n+m)$ ou $p \mid (n-m)$. O primeiro caso é impossível porque $n+m \leqslant 2r \leqslant p-1$. Conclui-se que $\overline{n} = \overline{m}$, como se queria. Logo, o polinómio $X^r - \overline{1}$ sobre o corpo $\mathbb{Z}/p\mathbb{Z}$ tem exatamente r raízes, nomeadamente os quadrados $\overline{1}^2$, $\overline{2}^2$, $\ldots$, $\overline{r}^2$. Acabámos de mostrar que as raízes do polinómio $X^r - \overline{1}$ são exatamente os quadrados não nulos módulo p.

Estamos agora em condições de demonstrar o critério. Suponhamos que $\left(\frac{a}{p}\right) = 1$. Por definição $\overline{a}$ é um quadrado (não nulo) de $\mathbb{Z}/p\mathbb{Z}$ e, como já vimos, $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Temos, pois (neste caso), a igualdade do critério. Suponhamos que $\left(\frac{a}{p}\right) = -1$. Por definição $\overline{a}$ não é um quadrado módulo p. Então, como vimos no parágrafo anterior, $a^r \not\equiv 1 \pmod{p}$. Mas $(a^r)^2 \equiv a^{p-1} \equiv 1 \pmod{p}$. Assim, $\overline{a}^r$ é raíz do polinómio $X^2 - \overline{1}$. Logo, $\overline{a}^r$ ou é $\overline{1}$ ou é $-\overline{1}$. Como não é $\overline{1}$, tem que ser $-\overline{1}$. Isto é o que queríamos obter. □

Uma aplicação deste critério justifica a propriedade (c) acima:

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

e o resultado sai. De facto, mostrámos que a aplicação de $(\mathbb{Z}/p\mathbb{Z})^*$ para $\{-1, 1\}$ dada por $\overline{a} \rightsquigarrow \left(\frac{a}{p}\right)$ é um epimorfismo de grupos cujo núcleo é constituído exatamente pelos quadrados de $(\mathbb{Z}/p\mathbb{Z})^*$.

Pelo critério de Euler:

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

Equivalentemente:

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