O LEMA DE HENSEL

FERNANDO FERREIRA

O seguinte resultado esclarece uma questão posta na última secção:

Proposição 1. *Seja n um número natural ímpar diferente de 1 e a um inteiro com $a \perp n$. Então, a é um quadrado módulo n se, e somente se, $\left(\frac{a}{p}\right) = 1$ para todo o primo p que divide n.*

Suponhamos que a é um quadrado módulo n. Então existe $b \in \mathbb{Z}$ tal que $b^2 \equiv a \,(\mathrm{mod}\ n)$. Logo, para todo p primo tal que $p \mid n$, tem-se $b^2 \equiv a \,(\mathrm{mod}\ p)$ e, portanto, $\left(\frac{a}{p}\right) = 1$. Foi fácil argumentar esta direção. Como consequência tem-se, obviamente, que neste caso o símbolo de Jacobi $\left(\frac{a}{n}\right)$ é 1. Dito de outro modo, $\left(\frac{a}{n}\right) = 1$ é condição necessária para que a seja um quadrado módulo n. Não é em geral condição suficiente, como foi observado na secção anterior.

Para argumentar a implicação contrária da proposição acima falta-nos um ingrediente:

Lema 1. *Seja p um primo ímpar e a um inteiro tal que $a \perp p$. Se $\left(\frac{a}{p}\right) = 1$, então para todo o natural r, a é um quadrado módulo p^r.*

Com a ajuda deste lema podemos concluir a demonstração da proposição. Suponhamos, por hipótese, que $\left(\frac{a}{p}\right) = 1$ para todo o primo p tal que $p \mid n$. Seja $n = p_1^{r_1} \cdots p_k^{r_k}$ a fatorização de n como produtos de primos distintos $p_1, \ldots, p_k$. Dado $1 \leqslant i \leqslant k$, pelo lema acima existe $b_i \in \mathbb{Z}$ tal que $b_i^2 \equiv a \,(\mathrm{mod}\ p_i^{r_i})$. Considere-se agora o seguinte sistema de equações:

$$\begin{aligned} x &\equiv b_1 \,(\mathrm{mod}\ p_1^{r_1}) \\ x &\equiv b_2 \,(\mathrm{mod}\ p_2^{r_2}) \\ \cdots &\quad \cdots \quad \cdots \\ x &\equiv b_k \,(\mathrm{mod}\ p_1^{r_k}) \end{aligned}$$

Pelo teorema chinês dos restos, este sistema tem solução. Seja $b \in \mathbb{Z}$ uma tal solução. É claro que, para todo $1 \leqslant i \leqslant k$, $b^2 \equiv b_i^2 \,(\mathrm{mod}\ p_i^{r_i})$ e, portanto, $b^2 \equiv a \,(\mathrm{mod}\ p_i^{r_i})$. Sai claramente que $b^2 \equiv a \,(\mathrm{mod}\ n)$, como se queria.

O lema acima é consequência do seguinte resultado importante:

Lema de Hensel. *Seja $P(X) \in \mathbb{Z}[X]$, p um número primo e $k \in \mathbb{N}$. Suponhamos que existe $b \in \mathbb{Z}$ tal que*

$$P(b) \equiv 0 \,(\mathrm{mod}\ p^k) \quad e \quad P'(b) \not\equiv 0 \,(\mathrm{mod}\ p)$$

Então existe $c \in \mathbb{Z}$ tal que $P(c) \equiv 0 \,(\mathrm{mod}\ p^{k+1})$ e, além disso, $c \equiv b \,(\mathrm{mod}\ p^k)$.

Demonstração. Vamos ver que podemos tomar c da forma $b + tp^k$ para certo inteiro t a determinar. Pelo teorema de Taylor aplicado à função polinomial $x \rightsquigarrow P(x)$ de $\mathbb{R}$ para $\mathbb{R}$, temos

$$P(b + x) = P(b) + \frac{P'(b)}{1!}x + \frac{P''(b)}{2!}x^2 + \frac{P'''(b)}{3!}x^3 + \cdots$$

para todo o $x \in \mathbb{R}$ (note-se que os coeficientes da série de Taylor são todos zero a partir de certa ordem). Daqui conclui-se que os coeficientes $\frac{P''(b)}{2!}$, $\frac{P''(b)}{3!}$, etc. do polinómio do lado direito são

inteiros pois são iguais aos (correspondentes) coeficientes do polinómio do lado esquerdo, que são inteiros. Assim, temos (e faz sentido escrever):

$$P(b+tp^k) = P(b) + \frac{P'(b)}{1!}tp^k + \frac{P''(b)}{2!}(tp^k)^2 + \frac{P'''(b)}{3!}(tp^k)^3 + \cdots \equiv P(b) + tp^k P'(b) \pmod{p^{k+1}}$$

Por hipótese, $P(b) = p^k q$, para certo inteiro q. Vem:

$$P(b+tp^k) \equiv p^k q + tp^k P'(b) \equiv p^k(q + tP'(b)) \pmod{p^{k+1}}$$

Dado que $P'(b) \not\equiv 0 \pmod{p}$, existe $t_0 \in \mathbb{Z}$ com $q + t_0 P'(b) \equiv 0 \pmod{p}$. Isto é, $p \mid (q + t_0 P'(b))$. Logo, $P(b + t_0 p^k) \equiv 0 \pmod{p^{k+1}}$. Como se queria demonstrar. □

O seguinte corolário do lema de Hensel é importante e desempenha um papel importante na chamada teoria dos números p-ádicos:

Corolário 1 (Levantamento de Hensel)**.** *Seja $P(X) \in \mathbb{Z}[X]$ e p um número primo. Suponhamos que existe $b \in \mathbb{Z}$ tal que $P(b) \equiv 0 \pmod{p}$ e $P'(b) \not\equiv 0 \pmod{p}$. Então, para todo o natural r, existe $c \in \mathbb{Z}$ tal que $c \equiv b \pmod{p}$ e $P(c) \equiv 0 \pmod{p^r}$.*

Demonstração. Aplicando uma vez o lema de Hensel (com $k = 1$), existe um inteiro c_1 tal que $P(c_1) \equiv 0 \pmod{p^2}$ e $c_1 \equiv b \pmod{p}$. Note-se que se infere $P'(c_1) \not\equiv 0 \pmod{p}$. Aplicando outra vez o lema de Hensel (com $k = 2$), existe um inteiro c_2 tal que $P(c_2) \equiv 0 \pmod{p^3}$ e $c_2 \equiv c_1 \pmod{p^2}$. Note-se que sai $c_2 \equiv b \pmod{p}$ e, portanto, $P'(c_2) \not\equiv 0 \pmod{p}$. Ao fim de $r-1$ aplicações de lema de Hensel obtemos a conclusão desejada. □

Podemos agora demonstrar o Lema 1. Considere-se o polinómio $P(X) := X^2 - a$. Por hipótese, existe $b \in \mathbb{Z}$ tal que $P(b) \equiv 0 \pmod{p}$. Note-se que $P'(b) \equiv 2b$ e que $2b \not\equiv 0 \pmod{p}$ (pois p é ímpar e, como $p \nmid a$, tem-se $p \nmid b$). Por levantamento (o corolário acima), então para todo a número natural r, a é um quadrado módulo p^r.