Elementos de Matemática Finita
Lema de Hensel

No que se segue $f(x)$ designa sempre um polinómio de coeficientes inteiros. Como se viu, o Teorema Chinês dos Restos reduz a resolução de uma equação

$$f(x) \equiv 0 \mod m$$

ao caso em que o módulo é a potência de um primo. A sequência de problemas que se segue aborda este problema.

1. O caso linear. Seja p primo e consideremos a equação linear

$$ax \equiv b \mod p^2.$$

Se a é primo com p a equação tem solução única, que pode ser descoberta aplicando o algoritmo de Euclides, como se viu.
Vamos ver como podemos resolver esta equação a partir da equação mais simples

$$ax \equiv b \mod p.$$

a) Seja x_0 a única solução desta última equação. Justificar que a solução da equação original é congruente módulo p^2 com $x_0 + py$ onde $0 \leq y < p$. Mostrar que, substituindo x por esta expressão na equação original, obtemos uma nova equaçãmódulo p na variável y.

b) Resolver por este método

$$91x \equiv 15 \mod 121.$$

c) Deduzir a generalização deste método para resolver uma equação

$$ax \equiv b \mod p^k,$$

e aplicá-lo no caso

$$47x \equiv 33 \mod 125.$$

2. Seja p primo. Suponhamos que a congruência

$$f(x) \equiv 0 \mod p^j$$

tem k soluções distintas $a_1, \cdots, a_k$.

a) Em que classes de congruência módulo p^{j+1} podem estar soluções de

$$f(x) \equiv 0 \mod p^{j+1}?$$

b) Fazendo apenas cálculos mod 3, determinar em que classes de congruência módulo 9 e módulo 27 respectivamente se poderão encontrar as soluções de

$$x^7 - 6x^5 + 2x^4 + 4x^2 + 1 \equiv 0 \mod 9$$

e

$$x^7 - 6x^5 + 2x^4 + 4x^2 + 1 \equiv 0 \mod 27.$$

3. Seja $f(x)$ um polinómio de grau n e coeficientes inteiros.
Deduzir a **Fórmula de Taylor** para polinómios:

$$f(a+x) = f(a) + f'(a)x + \frac{f^{(2)}(a)}{2}x^2 + \frac{f^{(3)}(a)}{3!}x^3 + \cdots + \frac{f^{(n)}(a)}{n!}x^n$$

onde $f^{(k)}$ designa a derivada de ordem k de f.
Sugestão: basta considerar o caso de um monómio (porquê?)

Nota: os coeficientes da representação de f na fórmula de Taylor continuam a ser inteiros.

4. Suponhamos que a é uma solução de

$$f(x) \equiv 0 \mod p^j$$

Diz-se que a é uma solução não singular daquela equação se $f'(a) \neq 0 \mod p$; caso contrário, diz-se uma solução singular.

a) Mostrar, usando a fórmula de Taylor, que $f(a+tp^j) \equiv f(a)+f'(a)tp^j \mod p^{j+1}$.

b) Mostrar que existe uma única solução (na variável t) módulo p de

$$f(a) + f'(a)tp^j \equiv 0 \mod p^{j+1}$$

c) Concluir que fica assim provado o
Lema de Hensel: Se $f(x)$ é um polinómio de coeficientes inteiros e a é uma solução não singular de

$$f(x) \equiv 0 \mod p^j$$

então, se z é a única solução de

$$xf'(a) \equiv 1 \mod p$$

$a - f(a)z$ é a única solução, congruente com a módulo p^j, da equação

$$f(x) \equiv 0 \mod p^{j+1}$$

5. Se f tem grau $n \geq p$, sabemos que existe um polinómio $r(x)$ de grau $< p$ (único módulo p) que tem as mesmas raízes que f módulo p.
Mostrar que mesmo que $f(a) \equiv r(a) \equiv 0 \mod p$ não é verdade em geral que se tenha

$$f'(a) \equiv r'(a) \mod p$$

Sugestão: considerar primeiro o exemplo $f(x) = x^7 + 3x^2 + 13$ e $p = 5$.
Nota: esta observação mostra que na aplicação do Lema de Hensel, embora possamos começar por substituir $f(x)$ por $r(x)$ para determinar as soluções de

$$f(x) \equiv 0 \mod p,$$

o caráter (singular ou não) dessas soluções e o valor da derivada tem que ser determinado usando o polinómio original.

6. Usar o Lema de Hensel para determinar as soluções de

a) $x^7 - 6x^5 + 2x^4 + 4x^2 + 1 \equiv 0 \mod 27$;

b) $x^3 + x + 57 \equiv 0 \mod 5^3$;

c) $x^7 + 3x^2 + 13 \equiv 0 \mod 25$

7. Mostrar que se p é um primo ímpar, $a \neq 0 \mod p$ e $x^2 \equiv a \mod p$ tem solução, então

$$x^2 \equiv a \mod p^j$$

também tem solução, para todo o natural j.

8. É possível "acelerar" a obtenção de soluções: nas mesmas condições do Lema de Hensel, se b satisfaz a congruência $bf'(a) \equiv 1 \mod p^j$ e $c = a - f(a)b$ então $f(c) \equiv 0 \mod p^{2j}$.

9. Suponhamos agora que a é uma solução singular de

$$f(x) \equiv 0 \mod p^j$$

ou seja que $f'(a) \equiv 0 \mod p$.

a) Mostrar, por uma aplicação semelhante da fórmula de Taylor, que

$$f(x) \equiv 0 \mod p^{j+1}$$

ou não tem soluções congruentes com a módulo p^j, ou tem p soluções nessas condições (e distintas módulo p^{j+1}).

b) No caso de existirem p soluções para

$$f(x) \equiv 0 \mod p^{j+1}$$

congruentes com a módulo p^j, não há à partida garantias de que alguma delas seja também solução de

$$f(x) \equiv 0 \mod p^{j+2}$$

Mostrar que

$$f(a + p^j t) \equiv p^{j+1}(q + rt + st^2) \mod p^{j+2}$$

onde q, r, s são inteiros dependentes dos valores de $f^{(k)}(a)$, e que portanto a resolução desse problema passa apenas pela determinação das raízes módulo p de um polinómio de grau ≤ 2.

10. Usar os resultados provados até aqui para mostrar que a equação

$$x^3 + 2x^2 + 34 \equiv 0 \mod 5^k$$

tem 2 soluções para $k = 1$, 6 soluções para $k = 2$ e apenas 1 para $k \geq 3$.

11. Neste exercício continuamos a supor que a é uma solução singular de $f(x) \equiv 0 \mod p^j$.

    a) Seja i a maior potência de p que divide $f'(a)$. Usa-se a notação $p^i \parallel f'(a)$. Supondo que $j \geq 2i + 1$, mostrar, usando de novo a fórmula de Taylor, que se $b = a + tp^{j-i}$ com t inteiro, então $f(b) \equiv 0 \mod p^j$.

    b) Deduzir que, nessas condições, se tem a seguinte congruência:

$$\frac{f(a + tp^{j-i})}{p^j} \equiv \frac{f(a)}{p^j} + t\frac{f'(a)}{p^i} \mod p$$

    e que em consequência existe uma única solução (na variável t) de

$$f(a + tp^{j-i}) \equiv 0 \mod p^{j+1}$$

    c) Sempre nas condições da alínea a), justificar as congruências

$$f'(a + tp^{j-i}) \equiv f'(a) \mod p^{i+1}$$

$$p^i \parallel f'(a + tp^{j-i})$$

12. Aplicar os resultados anteriores para descrever o melhor possível as soluções de

    a) $4x^3 + x^2 + 2x + 5 \equiv 0 \mod 3^k$;

    b) $2x^3 + x^2 + 2x + 1 \equiv 0 \mod 5^k$.