Introdução à Teoria dos Números

Ficha de preparação (semana de 20/10)

Resumo de resultados:

Símbolo de Legendre e Reciprocidade Quadrática

No caso de uma equação de grau 2, o critério de Euler, para um módulo primo ímpar p, pode enunciar-se do seguinte modo:

Proposição 0.1 *Se p é um primo ímpar e $a \in \mathbb{Z}$ é primo com p, então ou*

$$a^{\frac{p-1}{2}} \equiv 1 \mod p$$

e a equação $x^2 \equiv a \mod p$ tem duas soluções; ou

$$a^{\frac{p-1}{2}} \equiv -1 \mod p$$

e a equação $x^2 \equiv a \mod p$ não tem solução.

Definição 0.2 *Dado p primo ímpar e $a \in \mathbb{Z}$ primo com p, a diz-se um* ***resíduo quadrático*** $\mod p$ *se $a^{\frac{p-1}{2}} \equiv 1 \mod p$.*

Definição 0.3 (Símbolo de Legendre) *Dado p e $a \in \mathbb{Z}$, o símbolo $(a|p)$ define-se como*

$$(a|p) = \begin{cases} 0 & \text{se } p \mid a \\ 1 & \text{se } a^{\frac{p-1}{2}} \equiv 1 \mod p \\ -1 & \text{se } a^{\frac{p-1}{2}} \equiv -1 \mod p \end{cases}$$

Ou seja, $(a|p) \in \{-1, 0, 1\}$ e $(a|p) \equiv a^{\frac{p-1}{2}} \mod p$.

O símbolo de Legendre tem as seguintes propriedades, de verificação imediata a partir da definição:

1. $(1|p) = 1$ para todo o p;
2. $(-1|p) = 1$ se $p \equiv 1 \mod 4$, e $(-1|p) = -1$ se $p \equiv 3 \mod 4$;
3. $(a + kp|p) = (a|p)$;
4. $(ab|p) = (a|p)(b|p)$.

Deduz-se também

$$(2|p) = \begin{cases} 1 & \text{se } p \equiv \pm 1 \mod 8 \\ -1 & \text{se } p \equiv \pm 3 \mod 8 \end{cases}.$$

Teorema 0.4 (Lei da Reciprocidade Quadrática) *Dados primos ímpares p e q*

$$(p|q)(q|p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Por outras palavras, $(q|p) = (p|q)$ se pelo menos um dos dois primos é congruente com 1 módulo 4; se p e q são ambos congruentes com 3 módulo 4, então $(q|p) = -(p|q)$.

Resolução de equações módulo p^k.

Proposição 0.5 (Lema de Hensel) *Dado p primo, se x_1 é solução da equação*

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

e $f'(x_1) \neq 0 \mod p$, então, para cada $k > 0$, existe uma única solução x_{k+1} de

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

que satisfaz $x_k \equiv x_1$ módulo p.
Se $f(x_k) = p^k u$,

$$x_{k+1} \equiv x_k + p^k t \mod p^{k+1},$$

onde $0 \leq t < p$ é a solução de $u + f'(x_1)t \equiv 0 \mod p$

Problemas

Esta lista contém também problemas referentes aos tópicos já referidos na Ficha 5.

1. Usar o facto de que 2 é raiz primitiva módulo 13 para resolver a equação $4x^7 + 7x^4 \equiv 0 \mod 13$.

2. Determinar o número de soluções (distintas) de

$$(x^{30} - 1)(x^{45} - 1) \equiv 0 \mod 73.$$

3. Seja g uma raiz primitiva módulo p. Para quantos $0 < k < p$ é que a equação $x^k \equiv g \mod p$ tem

   a) exactamente uma solução?

   b) mais do que uma solução?

4. Dado p primo, mostrar que se $\mathrm{ord}_p(a)$ é ímpar, então a é resíduo quadrático módulo p.

5. Neste exercício demonstramos que se p é um primo ímpar e g é uma raiz primitiva módulo p, então ou g ou $g + p$ é uma raiz primitiva módulo p^2:

   i) Mostrar que $\mathrm{ord}_{p^2}(g) = p - 1$ ou $\mathrm{ord}_{p^2}(g) = p(p - 1)$, e que o mesmo se passa para $\mathrm{ord}_{p^2}(g + p)$;

   ii) suponhamos que $\mathrm{ord}_{p^2}(g) = p - 1$; aplicar a fórmula do binómio a $(g + p)^{p-1}$ e deduzir que $\mathrm{ord}_{p^2}(g + p) \neq p - 1$.

6. Calcular os símbolos de Legendre

$$(19|39), \qquad (-100|19).$$

7. Resolver as equações

   a) $3x^2 + 5x + 5 \equiv 0 \mod 13$;

   b) $7x^2 + 8x \equiv 5 \mod 17$;

c) $6x^{25} + x^5 + 5x \equiv 0 \mod 23$;

d) $2x^{17} + 5x + 1 \equiv 0 \mod 19$.

8. Para que primos p é que as seguintes equações têm soluções?

   a) $x^2 \equiv -2 \mod p$;

   b) $x^2 \equiv 3 \mod p$;

   c) $x^2 \equiv 5 \mod p$.

9. Justificar que se 1999 divide $a^2 + 2b^2$, então divide a e b.

10. Determinar o número de soluções das equações seguintes:

    a) $x^{80} + x^3 \equiv 8 \mod 3^{20}$;

    b) $x^{60} \equiv 1 \mod 73^{20}$;

11. Resolver a equação

$$x^6 + 4x \equiv a \mod 7^3$$

    para $a = 2$ e $a = 3$.