Aplicações de Corpos Finitos

Samuel Feitosa

1 Problemas

Exercício 1. (TST Polônia) Seja $p > 3$ um primo e $q = p^3$. A sequência (a_n) é definida por $a_n = a_{n-1} + a_{n-p}$, $n \geq p$ e $a_n = n$ para $0 \leq n \leq p-1$. Determine o resto de a_q por p

Exercício 2. (OBM 2017) Seja a um inteiro positivo e p um divisor primo de $a^3 - 3a + 1$, com $p \neq 3$. Prove que p é da forma $9k+1$ ou $9k-1$, onde k é um inteiro.

Exercício 3. (Romênia 2002) Sejam $P(x)$ e $Q(x)$ polinômios em $\mathbb{Z}[x]$ de graus p e q, respectivamente. Suponha que $P(x)$ divide $Q(x)$ em $\mathbb{Z}[x]$ e todos os coeficientes de ambos os polinômios são 1 ou 2002. Mostre que $p+1$ divide $q+1$.

Exercício 4. (IMO 1993) Para qualquer inteiro positivo $n > 1$, mostre que $x^n + 5x^{n-1} + 3$ é irredutível em $\mathbb{Z}[x]$

Exercício 5. (Generalização do problema anteiror) Se a, m, n são inteiros positivos e $p < a - 1$ é um primo, então $P(x) = x^m(x-a)^n + p$ é irredutível.

Exercício 6. (TST - Romênia) Mostre que para qualquer inteiro positivo n o polinômio $p(x) = (x^2+x)^{2^n} + 1$ é irredutível em $\mathbb{Z}[x]$.

Exercício 7. Prove que $x^5 + 5x^2 + 1$ é irredutível em $\mathbb{Q}[x]$.

Exercício 8. Mostre que se 5 é uma raiz primitiva para o primo p, então $p \mid F_{p+1}$, onde F_n denota o n-ésimo número de Fibonacci.

Exercício 9. Em qualquer corpo finito, todo elemento é soma de dois quadrados. Conclua que para todo primo p, dado m, sempre existem inteiros a e b tais que

$$m \equiv a^2 + b^2 \pmod{p}$$

Exercício 10. (São Petesburgo 2000) É possível selecionar 102 subconjuntos de 17 elementos de um conjunto de 102 elementos de modo que a interseção de quaisquer dois subconjuntos possui no máximo 3 elementos?

Exercício 11. (Irã 2006.) Seja A uma coleção de vetores de comprimento n com elementos em $\mathbb{Z}_3$ com a propriedade que para quaisquer dois vetores distintos $a, b \in A$ existe alguma coordenada i tal que $b_i = a_i + 1 \pmod 3$. Prove que $|A| \leq 2^n$.

Exercício 12. (Putnam 2000) Seja S_0 um conjunto finito de inteiros positivos. Definimos os conjuntos $S_1, S_2, \ldots$ de inteiros positivos como segue: o inteiro a está em S_{n+1} se, e somente se, exatamente um dentre $a-1$ ou a está em S_n. Mostre que existem infinitos inteiros N para os quais

$$S_N = S_0 \cup \{N + a : a \in S_0\}.$$

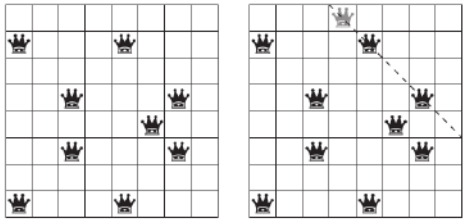
Exercício 13. (China TST) A sequência $\{x_n\}$ é definida por $x_1 = 2$, $x_2 = 12$ e $x_{n+2} = 6x_{n+1} - x_n$ para todos os inteiros positivos n. Seja p um número primo ímpar e seja q um divisor de x_p. Prove que se $q \neq 2, 3$, então $q \geq 2p - 1$.

Exercício 14. (Banco da IMO) A sequência $a_0, a_1, \ldots,$ é definida como segue: $a_0 = 2$, $a_{k+1} = 2a_k - 1$, para $k \geq 0$. Prove que se um primo ímpar divide a_n, então 2^{n+3} divide $p^2 - 1$.

Exercício 15. (IMO 1993) There are n lamps $L_0, L_1, \ldots, L_{n-1}$ in a circle ($n > 1$), where we denote $L_{n+k} = L_k$. (A lamp at all times is either on or off.) Perform steps $s_0, s_1, \ldots$ as follows: at step s_i, if L_{i-1} is lit, switch L_i from on to off or vice versa, otherwise do nothing. Initially all lamps are on. Show that:

1. There is a positive integer $M(n)$ such that after $M(n)$ steps all the lamps are on again;
2. If $n = 2k$, we can take $M(n) = n^2 - 1$;
3. If $n = 2k+1$, we can take $M(n) = n^2 - n + 1$.

Exercício 16. (Martin Gardner 1976/ Scientific American) Dizemos que uma distribuição de rainhas em um tabuleiro de xadrez é *boa* se não existem 3 delas em uma mesma linha, coluna ou diagonal (retas com inclinação ± 1). No desenho abaixo, temos uma distribuição *boa* em um tabuleiro 8×8. Seja $m_3(n)$ o maior número de rainhas que podem ser colocadas em um tabuleiro de xadrez $n \times n$ formando uma distribuição *boa*, mas com a propriedade de que qualquer acréscimo de uma rainha em uma casa vazia remove essa propriedade. Mostre que $m_3(n) \geq n$.



Exercício 17. (Crux) Existem 2005 pessoas em um senado e cada um possui inimigos dentro do grupo. Prove que existe um subconjunto não vazio K de senadores tal que para cada senador no senado o seu número de inimigos em K é um número par.

Exercício 18. (Cauchy-Davenport) Se p é um número primo, A e B são suconjuntos não vazios de $\mathbb{Z}_p$, então

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

Exercício 19. (Putnam 1979) Seja F um corpo finito com um número ímpar de elementos m. Seja $p(x)$ um polinômio irredutível em $F[x]$ da forma

$$x^2 + bx + c$$

Para quantos valores de k o polinômio $p(x) + k$ é irredutível sobre F?

Exercício 20. Um retângulo pode ser coberto com quadrados se, e somente se, a razão entre seus lados é um número racional.

Exercício 21. (IMC 2010) Seja p um número primo. Dizemos que um inteiro positivo n é interessante se

$$x^n - 1 = (x^p - x + 1)f(x) + pg(x)$$

para polinômios f e g com coeficientes inteiros.

a) Prove que o número $p^p - 1$ é interessante.

b) Para quais p o número $p^p - 1$ é o menor número interessante?

Tecnologia

No que segue, F sempre denotará um corpo.

Teorema 1 (Algoritmo da divisão) Dados os polinômios $A(x)$, $B(x) \in F[x]$, com $B(x) \neq 0$, existem polinômios $Q(x)$, $R(x) \in F[x]$ tais que:

$$A(x) = B(x)Q(x) + R(x).$$

Corolário 1 Se $P(x) \in F[x]$ é não nulo, então $P(x)$ possui no máximo $\deg P$ raízes.

Lema 1 Se F é um corpo finito, existe um inteiro m, tal que $\sum_{i=0}^{m-1} 1_F = 0$. Além disso, o menor m com essa propriedade é um número primo, que será chamado de característica do corpo.

Teorema 2 O grupo multiplicativo dos elementos não nulos de um corpo finito F é cíclico, i.e., existe um elemento g tal que $ord(g) = \|F\| - 1$.

Corolário 2 Seja $a \in F^*$, então $x^n = a$ admite solução se e somente se $a^{(q-1)d} = 1$, onde $d = (n, q-1)$. Caso existam soluções, seu número é d.

Teorema 3 Se F é um corpo finito, então $\|F\| = p^n$ para algum primo p e algum inteiro positivo n. Além disso, para cada n e cada primo p existe um único corpo F, a menos de isomorfismos, que possui ordem p^n.

Teorema 4 O corpo F_{p^n} é o *corpo de decomposição* de qualquer polinômio irredutível $p(x)$ de grau n sobre F_p. (Isso significa que $p((x)$ se escreve como produto de fatores lineares sobre F_{p^n}, mas não sobre qualquer outro subcorpo de F_{p^n}.

Teorema 5 1) As raízes de qualquer polinômio irredutível sobre F_p são distintas.

2) Dois polinômios irredutíveis sobre F_q não podem ter uma raiz comum.

3) $F_{p^a} \subset F_{p^b}$ se, e somente se, a divide b.

Teorema 6 Sejam F um corpo e $p(x)$ um polinômio em $F[x]$. Se u é uma raiz de $p(x)$ em alguma extensão E de F, denotemos por $F(u)$ o subcorpo de E gerado por F e u. Então

$$F(u) = \{b_0 + b_1u + \ldots + b_mu^m \in E | b_0 + b_1x + \ldots + b_mx^m \in F[x]\}.$$

Definição 1 (Plano Projetivo) Dizemos que um conjunto S é um plano projetivo se existem subconjuntos $C_i \subset S$ que satisfazem as seguintes propriedades:

1. Se P e Q pertencem a S, um e somente um dos subconjuntos C_i contém P e Q.
2. A interseção de C_i e C_j consiste sempre de um único elemento, para todo $i \neq j$.
3. Existem pelo menos quatro elementos de S tais que, entre eles não haja três contidos em um dos conjuntos C_i.

Teorema 7 Sejam F um corpo arbitrário e $f = f(x_1, x_2, \ldots, x_n)$ seja um polinômio em $F[x_1, \ldots, x_n]$. Sejam $S_1, S_2 \ldots, S_n$ subconjuntos não vazios de F e defina $g(x_i) = \prod_{s \in S_i}(x_i - s)$. Se f se anula sobre todos os zeros comuns de $g_1, g_2, \ldots, g_n$, i.e., $f(s_1, s_2, \ldots, s_n) = 0$ para todo $s_i \in S_i$, então existem polinômios $h_1, h_2, \ldots, h_n$ em $F[x_1, x_2, \ldots, x_n]$, satisfazendo $\deg(h_i) \leq \deg(f) - \deg(g_i)$, de modo que

$$f = \sum_{i=1}^{n} h_i g_i.$$

Teorema 8 Sejam F um corpo arbitrário e $f = f(x_1, x_2, \ldots, x_n)$ seja um polinômio em $F[x_1, \ldots, x_n]$. Suponha que $\deg(f)$ é $\sum_{i=1}^{n} t_i$, onde cada t_i é um inteiro não negativo, e que o coeficiente de $\prod_{i=1}^{n} x_i^{t_i}$ em f é não-nulo. Então, se $S_1, S_2, \ldots, S_n$ são subconjuntos de F com $|S_i| > t_i$, existem $s_1 \in S_1, s_2 \in S_2, \ldots, s_n \in S_n$ tais que

$$f(s_1, s_2, \ldots, s_n) \neq 0.$$