Polynomials Prasolov

Theorem 1.1.1 (Rouché). Let f and g be polynomials, and γ a closed curve without self-intersections in the complex plane. If

$$|f(z) - g(z)| < |f(z)| + |g(z)|$$

for all $z \in \gamma$, then inside γ there is an equal number of roots of f and g (multiplicities counted).

Theorem 1.1.2. Let $f(z) = z^n + a_1 z^{n-1} + \cdots + a_n$, where $a_i \in \mathbb{C}$. Then, inside the circle $|z| = 1 + \max_i |a_i|$, there are exactly n roots of f (multiplicities counted).

Theorem 1.1.4 (Ostrovsky). Let $f(x) = x^n - b_1 x^{n-1} - \cdots - b_n$, where all the numbers b_i are non-negative and at least one of them is nonzero.
If the greatest common divisor of the indices of the positive coefficients b_i is equal to 1, then f has a unique positive root p and the absolute values of the other roots are $< p$.

Theorem 1.2.1 (Gauss-Lucas). The roots of P' belong to the convex hull of the roots of the polynomial P itself.

Theorem 1.2.2. Let $P(z) = (z - x_1) \cdot \cdots \cdot (z - x_n)$, where $x_{1,} < \cdots < x_n$.
If some root x_i is replaced $by\ x_i' \in (x_i, x_i + 1)$, then all the roots of P' increase their value.

Theorem 1.2.3 (van der Berg). Let the roots of a cubic polynomial P form the vertices of a triangle ABC in the complex plane. Then the roots of P' are at the focal points of the ellipse tangent to the sides of ΔABC at their midpoints.

Theorem 1.4.1 (Fourier-Budan). Let $N(x)$ be the number of sign changes in the sequence $f(x), f'(x), \ldots, f^{(n)}(x)$, where f is as polynomial of degree n.
Then the number of roots of f (multiplicities counted) between a and b, where $f(a) \neq (0)$, $f(b) \neq 0$ and $a < b$, does not exceed $N(a) - N(b)$. Moreover, the number of roots can differ from $N(a) - N(b)$ by an even number only.

Corollary 1. (The Descartes Rule) The number of positive roots of the polynomial $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$ does not exceed the number of sign changes in the sequence $a_0, a_1, \ldots, a_{n.}$

Corollary 2. (de Gua) If the polynomial lacks $2m$ consecutive terms (i.e., the coefficients of these terms vanish) then this polynomial has no less than $2m$ imaginary roots. If $2m + 1$ consecutive terms are missing, then if they are between terms of different signs, the polynomial has no less than $2m$ imaginary roots, whereas if the missing terms are between terms of the same sign the polynomial has no less than $2m + 2$ imaginary roots.

Theorem 1.4.3 (Sturm).

$$\begin{gathered} f = q_1 f_1 - f_2 \\ f_1 = q_2 f_2 - f_3 \\ \cdots\cdots\cdots\cdots\cdots \\ f_{n-2} = q_{n-1} f_{n-1} - f_{n,} \\ f_{n-1} = q_n f_{n.} \end{gathered}$$

The sequence $f, f_{1,\ldots,} f_{n-1}, f_n$ is called the *Sturm sequence* of the polynomial .
Let $w(x)$ be the number of sign changes in the sequence

$$f(x), f_1(x), \ldots, f_n(x).$$

The number of the roots of f (without taking multiplicities into account) confined between a and b, where $f(a) \neq 0, f(b) \neq 0$ and $a < b$, is equal to $w(a) - w(b)$.

1.2 Prove that the polynomial

$$a_0 + a_1x^{m_1} + a_2x^{m_2} + \cdots + a_nx^{m_n}$$

has at most n positive roots.

1.3 [Newton] Prove that if all the roots of the polynomial

$$P(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$$

with real coefficients are real and distinct, then

$$a_i^2 > \frac{n-i+1}{n-1} \cdot \frac{i+1}{i} a_{i-1}a_{i+1}$$

for $i = 1,2, \ldots, n-1$.

1.4 Prove that polynomial

$$a_0 + a_1x^{m_1} + a_2x^{m_2} + \cdots + a_nx^{m_n}$$

has no nonzero roots of multiplicity greater than $n-1$.

1.5 Find the number of real roots of the following polynomials:

a) $1 + x + \frac{x^2}{2} + \cdots + \frac{x^n}{n}$

b) $nx^n - x^{n-1} - \cdots - 1$.

1.6 Let $0 = m_0 < m_1 < \cdots < m_n$ and $m_i \equiv i (mod\ 2)$. Prove that the polynomial

$$a_0 + a_1x^{m_1} + a_2x^{m_2} + \cdots + a_nx^{m_n}$$

has at most n real roots.

1.8 Let the numbers $a_1, \ldots, a_n$ be distinct and let the numbers $b_1, \ldots, b_n$ be positive. Prove that all the roots of the equation

$$\sum \frac{b_k}{x - a_k} = x - c,$$

where $c \in \mathbb{R}$, are real.

1.10 Find the number of roots of the polynomial $x^n + x^m - 1$ whose absolute values are less than 1.

Theorem 2.1.7. The polynomial $P(x) = x^4 + ax^2 + b^2$, where $a, b \in \mathbb{Z}$, is reducible over $\mathbb{F}_p$ for all primes p.

Theorem 2.2.1 (Dumas). Let $f = gh$, where f, g and h are polynomials with integer coefficients. Then the system of vector of the segments for f is the union of the systems of vectors of the segments for g and h(provided p is the same for all the polynomials).

Example 2.2.3 Let p be a prime, $(c, p) = 1$ and $(m, n) = 1$. Then the polynomial $x^n + cp^m$ is irreducible.

Example 2.2.4 Let p be a prime. If the polynomial $f(x) = x^n + px + bp^2$, where $(b, p) = 1$, has no integer roots, then this polynomial is irreducible.

Theorem 2.2.5 (Perron). Let $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ be a polynomial with integer coefficients such that $a_n \neq 0$.
a) If $|a_1| > 1 + |a_2| + \cdots + |a_n|$, then f is irreducible.
b) If $|a_1| \geq 1 + |a_2| + \cdots + |a_n|$ and $f(\pm 1) \neq 0$, then f is irreducible.

Theorem 2.2.6. Let $a_1 \geq a_2 \geq \cdots \geq a_n$ be positive integers and $n \geq 2$. Then the polynomial $p(x) = x^n - a_1x^{n-1} - a_2x^{n-2} - \cdots - a_n$ is irreducible over $\mathbb{Z}$.

Theorem 2.2.7. Let $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x \pm p$ be a polynomial with integers coefficients, where p is a prime.
a) If $p > 1 + |a_1| + \cdots + |a_{n-1}|$, then f is irreducible.
b) If $p \geq 1 + |a_1| + \cdots + |a_{n-1}|$ and among the roots of f there are no roots of unity, then f is irreducible.

Theorem 2.2.8 (Pólya). Let f be a polynomial of degree n with integer coefficients and define $m = \left[\frac{n+1}{2}\right]$. Suppose that, for n different integers $a_{1,\dots,}\ a_{n,}$ we have $|f(a_i)| < 2^{-m}m!$ and the numbers $a_{1,\dots,}\ a_n$ are not roots of f. Then f is irreducible.

2.1 Let $f \in \mathbb{Z}[x]$ be a polynomial with roots $\alpha_{1,\dots,}\ \alpha_n$ and let $M = \max|\alpha_i|$. Prove that, if $f(x_0)$ is a prime for an integer x_0 such that $|x_0| > M + 1$, then f is irreducible.

2.2 Let p be a prime, and a a positive integer not divisible by p. Prove that $x^p - x - a$ is irreducible.

2.6 Let $a_1, \dots, a_n$ be distinct integers.

a) Prove that the polynomial $(x - a_1)\,(x - a_2) \cdot \cdots \cdot (x - a_n) - 1$ is irreducible.

b) Prove that the polynomial $(x - a_1)\,(x - a_2) \cdot \cdots \cdot (x - a_n) + 1$ is irreducible except for the following cases:

$$(x-a)(x-a-2)+1 = (x-a-1)^2;$$
$$(x-a)(x-a-1)(x-a-2)(x-a-3)+1 = ((x-a-1)(x-a-2)-1)^2.$$

c) Prove that any polynomial $(x - a_1)^2\,(x - a_2)^2 \cdot \cdots \cdot (x - a_n)^2 + 1$ is irreducible.

2.7 Prove that any polynomial with integer coefficients can be represented as the sum of two irreducible polynomials.

2.8 a) Let $f(x)$ be a polynomial with integer coefficients assuming the value $+1$ at more than three integer points. Prove that $f(n) \neq -1$ for any $n \in \mathbb{Z}$.
b) Let $a, b \in \mathbb{Z}$ and let the polynomial $ax^2 + bx + 1$ be irreducible. Let $n \geq 7$ and let $a_{1,\dots,}\ a_n$ be distinct integers; set $\varphi(x) = (x - a_1)(a - a_2) \cdot \dots \cdot (x - a_n)$. Prove that the polynomial $a(\varphi(x))^2$ $+b\varphi(x) + 1$ is irreducible.

2.10 Let $p > 3$ be a prime and let $n < 2p$. Prove that the polynomial $x^{2p} + px^n - 1$ is irreducible.

Theorem 3.2.1 Let p_k be a polynomial of degree k assuming integer values at $x = n, n+1, \dots, n+k$ for an integer n. Then

$$p_k(x) = c_0\binom{x}{k} + c_1\binom{x}{k-1} + c_2\binom{x}{k-2} + \cdots + c_k,$$

where $c_0, c_1, \dots, c_k$ are integers.

Theorem 3.2.2 Let $\mathcal{R}(x)$ be a rational function which takes integer values at all integer x. Then $\mathcal{R}(x)$ is an integer-valued polynomial.

Corollary. Let $f(x)$ and $g(x)$ by polynomials with integer coefficients and let $f(n)$ be divisible by $g(n)$ at all integer n . Then

$$f(x) = \left(\sum_{k=0}^{m} c_k \binom{x}{k}\right) g(x),$$

where $c_{0,\ldots}, c_m$ are integers.

3.3.1 Main properties of the cyclotomic polynomials

The polynomial

$$\Phi_\mathrm{n} = \prod (x - \varepsilon_k),$$

Where $\varepsilon_1, \ldots, \varepsilon_{\varphi(n)}$ are the primitive n-th roots of unity, is called the cyclotomic polynomial of degree n. For example,

$$\Phi_1(x) = x - 1, \qquad \Phi_2(x) = x + 1, \qquad \Phi_3(x) = x^2 + x + 1, \qquad \Phi_4(x) = x^2 + 1.$$

Theorem 3.3.1. Let $n > 1$ be odd. Then

$$\Phi_{2n}(x) = \Phi_n(-x).$$

3.3.2 The Mobius inversion formula

The relation

$$\prod_{d|n} \Phi_d(x) = x^n - 1$$

Enables us to express $\Phi_n(x)$ in terms of $x^d - 1$, where d runs over the set of divisors of n. To this end, we have a rather general construction based on the *Möbius function*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1; \\ (-1)^k & \text{if } n = p_1 \cdots p_k; \\ 0 & \text{if } n = p^2 m, \end{cases}$$

Where $p, p_1, \ldots, p_k$ are primes.

For cyclotomic polynomials, the Möbius inversion formula yields

$$\emptyset_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

Theorem 3.3.3. The coefficients of $\Phi_n(x)$ are integers.

Theorem 3.3.4. The polynomial Φ_n is irreducible over $\mathbb{Z}$.

Theorem 3.3.5. Let p be a prime. Then $\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) \text{ if } (\mathrm{n}, \mathrm{p}) = \mathrm{p}; \\ \dfrac{\Phi_n(x^p)}{\Phi_n(x)} \text{ if } (\mathrm{n}, \mathrm{p}) = 1. \end{cases}$

Theorem 3.3.7. Let $F_d(x)$ be the product of all irreducible monic polynomials of degree d over $\mathbb{F}_p$. Then

$$x^{p^n} - x = \prod_{d|n} F_d(x).$$

Lemma. a) Over an arbitrary field, the polynomial $x^n - 1$ divides $x^m - 1$ if and only if n divides m.
b) If $a \geq 2$ is a positive integer, then $a^n - 1$ divides $a^m - 1$ if and only if n divides m.

3.2 For $r = 2, \ldots, n$, the elementary symmetric polynomials σ_i satisfy the inequality

$$\frac{\sigma_r(x+y)}{\sigma_{r-1}(x+y)} \geq \frac{\sigma_r(x)}{\sigma_{r-1}(x)} + \frac{\sigma_r(y)}{\sigma_{r-1}(y)}.$$

3.3 For $r = 1,2, \ldots, n$, we have

$$\sqrt[r]{\sigma_r(x+y)} \geq \sqrt[r]{\sigma_r(x)} + \sqrt[r]{\sigma_{r-1}(y)}.$$

3.5 If a polynomial $f(x)$ of degree n takes integer values at $x = 0,1,4,9 \ldots, n^2$, then it takes integer values at all $x = m^2$, where $m \in \mathbb{N}$.

3.6 Let m and n be positive integers. Prove that the following conditions are equivalent.
a) There exist integers $a_0, \ldots, a_n$ such that

$$\text{GDC}\left(a_0, \ldots, a_n, m\right) = 1$$

and the values of the polynomial $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ at all $x \in \mathbb{Z}$ are divisible by m.
b) $n!/m \in \mathbb{Z}$.

Example 2.1.6 Prove that for any positive integer n, the polynomial $1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!}$ is irreducible.

(**Extra!** The polynomial $1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!}$ has either no roots or one root according n is even or odd.)

Theorem 4.3.1 (Mason). Let $a(x), b(x)$ and $c(x)$ be pairwise relatively prime polynomials such that $a + b + c = 0$. Then the degree of each of these polynomials does not exceed $n_0(abc) - 1$, where $n_0(P)$ is the number of distinct roots of the polynomial P.

Theorem 4.3.2 (Davenport). Let f and g be relatively prime polynomials of nonzero degree. Then

$$deg\,(f^3 - g^2) \geq \frac{1}{2}\,deg\,f + 1$$

Theorem 4.3.3 Let f, g and h be relatively prime polynomials, at least one of them not being constant. Then the identity

$$f^n + g^n = h^n$$

cannot hold for $n \geq 3$.

Theorem 4.3.4 Let α, β, γ be positive integers and $2 \le \alpha \le \beta \le \gamma$. Then the equation

$$f^{\alpha} + g^{\beta} = h^{\gamma}$$

has relatively prime solutions only for the following collections (α, β, γ):

$$(2,2,\gamma), (2,3,3), (2,3,4), (2,3,5).$$

Theorem 4.3.5. Let $x(t)$ and $y(t)$ be rational functions; let $m \ge 2$ and $n \ge 2$. Then the equation

$$x^n - y^m = 1$$

has solutions only for $m = n = 2$.

Waring's problem for polynomials

The classical Waring's problem is as follows:

Given a positive integer n, find the minimal number $k = k(n)$ for which any positive integer m can be represented in the form $m = m_1^n + \cdots + m_k^n$, where $m_{1,} \ldots, m_k$ are non-negative integers.

Several generalizations of this problem for polynomials are known. Here by Waring's problem for polynomials we will mean the following problem:

Given a positive integer n, find the minimal number $k = k(n)$ for which any polynomial, $g \in \mathbb{C}[x]$ can be represented in the form $g = f_1^n + \cdots + f_k^n$, where $f_i \in \mathbb{C}[x]$.

Theorem 4.3.6. If $n \ge 3$, then
a) $k(n) \ge 3$;
b) $k(n) \le n < k^2(n) - k(n)$.

Homework:
Theorem 1.1.4 (Ostrovsky).; Theorem 1.2.2.; 1.10; Theorem 2.2.8 (Pólya).; 2.2; 2.6; 2.8; 2.10; Theorem 3.2.2; Theorem 3.3.3.; Theorem 3.3.4.; Theorem 3.3.5.; 3.6; Example 2.1.6; Theorem 4.3.5.

Preparação IMO 2012 – Polinômios – Ed

1) Encontre o menor inteiro n tal que um quadrado $n \times n$ pode ser particionado em quadrados 40×40 e 49×49 com os dois tipos presentes na partição.

2) Seja p um primo ímpar positivo e sejam m, n inteiros positivos divisíveis por p com n ímpar. Para cada m – upla $(c_1, \ldots, c_m)$, $c_i \in \{1, 2, \ldots, n\}$, tal que $p | \sum_{i=1}^{m} c_i$, considere o produto $c_1 \cdot \cdots \cdot c_m$. Prove que a soma de todos esses produtos é divisível por $\left(\frac{n}{p}\right)^m$.

3) Encontre todos os polinômios f com coeficientes reais satisfazendo, para qualquer número real x, a relação $f(x)f(2x^2) = f(2x^3 + x)$.

4) Uma função $f: R^2 \to R$ é chamada *olímpica* se possui a seguinte propriedade : dados $n \ge 3$ pontos distintos $A_1, A_2, \ldots, A_n \in R^2$, se $f(A_1) = f(A_2) = \cdots = f(A_n)$ então os pontos $A_1, A_2, \ldots, A_n$ são os vértices de um polígono convexo. Seja $P \in C[x]$ um polinômio não constante. Prove que a função $f: R^2 \to R$, definida por $f(x, y) = |P(x + iy)|$, é olímpica se, e somente se, todas as raízes de P são iguais.

5) Sejam $P(z)$ e $Q(z)$ polinômios não constantes com coeficientes complexos tais que $P(z) = 0 \Leftrightarrow Q(z) = 0$ e $P(z) = 1 \Leftrightarrow Q(z) = 1$. Prove que os polinômios são iguais.

6) Seja p um número primo positivo. Prove que o polinômio

$$P(x) = x^{p-1} + 2x^{p-2} + 3x^{p-3} + \cdots + (p-1)x + p$$

é irredutível em $Z[x]$.

7) Um semigrupo S *concorda com* um par ordenado (i, j) de inteiros positivos se $ab = b^j a^i$ para quaisquer elementos distintos a e b de S. Encontre todos os pares ordenados (i, j) de inteiros positivos tais que se S concorda com (i, j), então S tem um elemento idempotente.

8) Prove que todo polinômio mônico de grau n com coeficientes reais é a média aritmética de dois polinômios mônicos de grau n com n raízes reais.

9) Para m inteiro, seja $p(m)$ o maior fator primo de m. Por convenção, $p(\pm 1) = 1$ e $p(0) = +\infty$. Encontre todos os polinômios $f(x)$ com coeficientes inteiros tais que a sequência $\{p(f(n^2)) - 2n\}_{n\geq 0}$ é limitada superiormente.

10) Prove que, para todo natural n, o número $7^{7^n} + 1$ tem pelo menos $2n + 3$ fatores primos (não necessariamente distintos).

11) Dadas duas sequências (possivelmente idênticas) $\{b_n\}$ e $\{c_n\}$ podemos formar as sequências $\{b_n + c_n\}$, $\{b_n - c_n\}$, $\{b_n c_n\}$ e $\{b_n / c_n\}$ (se todos os termos de c_n são diferentes de zero). Podemos também, dada uma sequência, formar uma nova sequência apagando uma quantidade finita de seus termos iniciais.

a) A partir da sequência $\{n^2\}$ podemos obter a sequência $\{n\}$?
b) E a sequência $\{n + \sqrt{2}\}$?
c) E a sequência $\left\{\frac{n^{2000}+1}{n}\right\}$?

12) Seja $P(x)$ um polinômio mônico e sejam $a_1, a_2, a_3, \ldots$ inteiros distintos satisfazendo as equações $P(a_1) = 0$, $P(a_2) = a_1$, $P(a_3) = a_2$, ... Quais são os possíveis valores do grau de $P(x)$?

13) Suponha que $q_0, q_1, q_2, \ldots$ é uma sequência de inteiros satisfazendo as seguintes condições:
(i) $m - n$ divide $q_m - q_n$ para $m > n \geq 0$;
(ii) existe um polinômio P tal que $|q_n| < P(n)$ para todo n natural.
Prove que existe um polinômio Q tal que $q_n = Q(n)$ para todo n natural.

14) Prove que, para todo n inteiro positivo, existe um racional a_n tal que o polinômio $x^2 + (1/2)x + 1$ divide $x^{2n} + a_n x + 1$.

15) a) Encontre um par de inteiros (a, b) de modo que $x^{13} - 233x - 144$ e $x^{15} + ax + b$ não sejam primos entre si.
b) A solução encontrada é única?

Sugestões para alguns problemas

1) Sendo $\zeta = e^{i\frac{\pi}{20}}$ e $\xi = e^{i\frac{2\pi}{49}}$ atribua ao quadrado unitário (j, k) o complexo $\zeta^j \xi^k$. Considerando a partição possível, ao somarmos quadrado por quadrado, teremos que a soma total é zero. Logo n é múltiplo de 40 ou de 49. Então obtemos que $n = 2000$.

3) Se z é uma raiz complexa do polinômio, então $2z^3 + z$ também é uma raiz. Logo se f não é o polinômio nulo, todas as suas raízes têm módulo menor ou igual a 1.

Fazendo $x = 0$ e mostrando que 0 não pode ser raiz de f, temos que o seu termo independente é 1. Considerando a identidade polinomial obtida a partir da equação funcional, concluímos que f é um polinômio mônico e, portanto, todas as suas raízes têm módulo 1.
Novamente considerando uma raiz z de f, $1 = |2z^3 + z| = |2z^2 + 1| \geq 2|z|^2 - 1 = 1$, ou seja, $z = \pm i$. Assim, as demais soluções são $f(x) = (x^2 + 1)^n$ com n natural.

4) Supondo que as raízes não são todas iguais, existem z_1 e z_2 distintos e um polinômio $Q(z)$ tais que $P(z) = (z - z_1)(z - z_2)Q(z)$ e que $|z_1 - z_2|$ é mínimo. Seja, então, z_3 o ponto médio de $z_1 z_2$. Temos que $f(z_3) > 0$ e podemos obter $z_4 \in \overrightarrow{z_3 z_1}$, $z_5 \in \overrightarrow{z_3 z_2}$ que satisfazem $f(z_3) = f(z_4) = f(z_5)$, uma contradição. Assim, provamos a ida. A volta é simples.

5) A dificuldade do problema reside nas raízes múltiplas (caso contrário, apenas a primeira condição já "quase" seria suficiente). Considerando $A(z) = \big(P(z) - Q(z)\big)P'(z)$ e as raízes de $P(z) = 0$ e $P(z) = 1$ resolvemos o problema.

6) A partir de $(x - 1)P(x) = x^p + x^{p-1} + x^{p-2} + \cdots + x - p$ podemos concluir que todas as raízes de P têm módulo maior do que 1. E a demonstração torna-se simples.

7) Supondo que S não tenha a propriedade para o par (i, j), então, para $k \geq 0$ e $x \in S$, $xx^2x^k = (x^2)^j x^i x^k$, ou seja, $x^{3+k} = x^{2j+i+k}$. Assim, $2j + i + k \neq 6 + 2k$, para todo $k \geq 0$. Logo $3 \leq 2j + i \leq 5$. Os casos $2i + i = 4$ e $2i + i = 5$ são tratados facilmente. Para o único caso restante, $2i + i = 3 \Leftrightarrow (i, j) = (1,1)$ há um contra – exemplo.

8) Sejam $p(x)$ o polinômio dado e $g(x) = (x - 2)(x - 4)\cdots(x - 2(n - 1))$. Para k suficientemente grande, os polinômios $a(x) = x^n - kg(x)$ e $b(x) = 2p(x) - x^n + kg(x)$ satisfazem as condições do problema.

9) O polinômio f que possui a propriedade se, e somente se, $f(x) = c(4x - {a_1}^2)(4x - {a_2}^2)\cdots(4x - {a_k}^2)$, em que $a_1, a_2, \ldots, a_k$ são ímpares positivos e c é um inteiro não nulo. A verificação de que tais polinômios têm a propriedade é simples. Vamos detalhar um pouco a ida.
Considere um polinômio f não nulo com a propriedade. Como f é um polinômio, existe uma sequência infinita de primos $\{p_j\}$ e uma sequência correspondente infinita de inteiros $\{r_j\}$ tais que $p_j | f({r_j}^2)$, com $0 \leq r_j \leq \frac{p_j - 1}{2}$. Daí, utilizando a propriedade, segue a existência de um a_1 satisfazendo $a_1 = p_j - 2r_j$para infinitos j. Sendo m o grau de f, $p_j | 4^m f\left(\left((p_j - a_1)/2\right)^2\right)$ e $4^m f(((x - a_1)/2)^2) \in \mathbb{Z}[x]$. Consequentemente, $(a_1/2)^2$ é uma raiz de f.
Indutivamente chegamos ao resultado.

10) A partir de
$$\frac{x^7 + 1}{x + 1} = \frac{(x + 1)^7 - \big((x + 1)^7 - (x^7 + 1)\big)}{x + 1} = (x + 1)^6 - 7x(x^4 + 2x^3 + 3x^2 + 2x + 1)$$
Obtemos uma fatoração que leva a uma demonstração por indução.

15) b) É.