

MATH 289, PROBLEM SET 9
DUE: 11/10/2004

HARM DERKSEN

Hand in solutions to 4 problems from the following list of problems: **Larson**, 4.2.7**, 4.2.8***, 4.2.9**, 4.2.10***, 4.2.11***, 4.2.12**, 4.2.13**, 4.2.14***, 4.2.15**, 4.2.16***, 4.2.17***, 4.2.18**, 4.2.19***, 4.2.20***, 4.2.21***, 4.3.11****, 4.3.12***, 4.3.17**, 4.3.20***, 4.3.21**. You may also choose problems from below.

In this problem set we will consider polynomials with coefficients in K , where K is the real numbers \mathbb{R} , the complex numbers \mathbb{C} , the rational numbers \mathbb{Q} or any other *field*. (A field is a number system satisfying certain axioms, but if you have not heard about this before, just think of the examples we just mentioned.) A polynomial in the variable x with coefficients in K is an expression

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

with $a_0, a_1, a_2, \dots, a_n \in K$. If $a_n \neq 0$ then f is said to have degree n . We may denote this by $\deg(f(x)) = n$. For convenience, we also define the degree of the zero polynomial 0 by $\deg(0) = -\infty$. The polynomial is called *monic* if $a_n = 1$. Now $K[x]$ denotes the set of all polynomials in the variable x with coefficients in K .

In many ways, polynomials behave similar to \mathbb{Z} (this is because $K[x]$ and \mathbb{Z} are both so-called *principal ideal domains*). As for the integers \mathbb{Z} , we can define gcd and lcm for polynomials. There also exists an Euclidean algorithm. To prove these results for polynomials, one could simply copy the proofs for the same results for the integers.

Suppose that $f(x), g(x) \in K[x]$. First, we say that a polynomial g divides a polynomial f if $f(x) = g(x)h(x)$ for some polynomial $h \in K[x]$. A monic polynomial f is called *irreducible* if it has exactly 2 monic divisors (namely 1 and itself).

For example, $x^2 + 1 \in \mathbb{R}[x]$ is irreducible. Indeed if $x^2 + 1$ is a product of two polynomials of degree 1, then $x^2 + 1 = (x + a)(x + b)$ and $-a \in \mathbb{R}$ would be a zero of $x^2 + 1$ which is impossible. Seen as a polynomial with complex coefficients $x^2 + 1 \in \mathbb{C}[x]$ is reducible, namely $x^2 + 1 = (x + i)(x - i)$. The polynomial $x^2 - 2 \in \mathbb{Q}[x]$ is irreducible by a similar reasoning because $\sqrt{2}$ is irrational.

These monic irreducible polynomials play the role of prime numbers. For example every monic polynomial is a unique product of monic irreducible polynomials (as we will see).

Sometimes we will also consider polynomials in several variables. For example $K[x, y]$ denotes the polynomials in x and y with coefficients in K . These can be seen as polynomials in y with coefficients in $K[x]$, or polynomials in x with coefficients in $K[y]$.

Problem 1. *** Find all polynomials (with real coefficients) $f(x)$ such that

$$f(x^2) = (f(x))^2.$$

Problem 2. ** If $f(x)$ is a polynomial, prove that we can write

$$f(x) - f(y) = a(x, y)(x - y)$$

where $a(x, y)$ is a polynomial in two variables. (*Hint: Reduce to the case $f(x) = x^n$.*)

1. DIVISION WITH REMAINDER

All polynomials considered have coefficients in K . We will develop a theory similar to the theory of integers.

Theorem 1. *If $f(x), g(x)$ are polynomials and $g(x) \neq 0$, then there are unique polynomials $q(x)$ and $r(x)$ such that*

$$f(x) = q(x)g(x) + r(x)$$

with $\deg(r(x)) < \deg(g(x))$.

We will call $q(x)$ the *quotient* and $r(x)$ the *remainder*. Theorem 1 can be done explicitly using a long division just like you would do for integers. For example, let us divide $x^5 + 3x^3 + 2x - 1$ by $x^2 - x + 2$:

$$\begin{array}{r}
 x^2 - x + 2 \overline{) x^5 + 3x^3 + 2x - 1} \\
 \underline{x^5 - x^4 + 2x^3} \\
 x^4 + x^3 + 2x - 1 \\
 \underline{x^4 - x^3 + 2x^2} \\
 2x^3 - 2x^2 + 2x - 1 \\
 \underline{2x^3 - 2x^2 + 4x} \\
 -2x - 1
 \end{array}$$

Therefore the quotient is $x^3 + x^2 + 2x$ and the remainder is $-2x - 1$ (You may have learned the long division slightly different. For example, it is a cultural thing where you put the quotient. Also, the horizontal bars weren't meant to be quite this long but I didn't figure it out how to do this in \TeX properly.)

Theorem 2. *Suppose that $f(x), g(x)$ are nonzero polynomials, and let $h(x)$ be a nonzero monic polynomial of smallest degree such that both $f(x)$ and $g(x)$ divide $h(x)$. This polynomial $h(x)$ is unique and we call it $\text{lcm}(f(x), g(x))$. Moreover if $u(x)$ is any common multiple of $f(x)$ and $g(x)$ then $\text{lcm}(f(x), g(x))$ divides $u(x)$.*

Proof. If $u(x)$ is a common multiple of $f(x)$ and $g(x)$ then we can write $u(x) = q(x)h(x) + r(x)$ with $\deg(r(x)) < \deg(h(x))$ and $r(x)$ is a common multiple of $f(x)$ and $g(x)$. Now $r(x)$ cannot be nonzero by minimality of $\deg(h(x))$. Therefore $r(x) = 0$ and $h(x)$ divides $u(x)$. We now prove uniqueness of $h(x)$. If $v(x)$ were another nonzero monic polynomial with minimal degree such that $f(x)$ and $g(x)$ divide $v(x)$, then $h(x)$ must divide $v(x)$ and $v(x)$ must divide $h(x)$. Since both polynomials are monic, we get $h(x) = v(x)$. \square

Theorem 3. *If $f(x), g(x)$ are nonzero polynomials, then there is a nonzero monic polynomial $h(x)$ of largest degree such that $h(x)$ divides both $f(x)$ and $g(x)$. The polynomial $h(x)$ is unique and we call it $\text{gcd}(f(x), g(x))$. Moreover, if $u(x)$ is any polynomial dividing both $f(x)$ and $g(x)$ then $u(x)$ divides $\text{gcd}(f(x), g(x))$.*

Proof. Define $h(x)$ as a nonzero polynomial of smallest possible degree such that it is of the form

$$a(x)f(x) + b(x)g(x)$$

for some polynomials $a(x)$ and $b(x)$. We may assume that $h(x)$ is monic by multiplying with a constant. Using division with remainder, we find $q(x)$ and $r(x)$ such that

$$f(x) = q(x)h(x) + r(x)$$

with $\deg(r(x)) < \deg(h(x))$. Now

$$r(x) = f(x) - q(x)(a(x)f(x) + b(x)g(x)) = (1 - q(x)a(x))f(x) + (-q(x)b(x))g(x).$$

Because of the minimality of the degree of $h(x)$, we must have $r(x) = 0$. This shows that $h(x)$ divides $f(x)$. In a similar way one can prove that $h(x)$ divides $g(x)$. If $u(x)$ is any polynomial dividing both $f(x)$ and $g(x)$ then $u(x)$ also divides $h(x) = a(x)f(x) + b(x)g(x)$. This also shows immediately that $h(x)$ is a common divisor of $f(x)$ and $g(x)$ of largest possible degree. If $u(x)$ is another monic common divisor of $f(x)$ and $g(x)$ then $u(x)$ divides $h(x)$ and since both are monic of the same degree we get $u(x) = h(x)$. This shows the uniqueness. \square

The previous proof shows in particular that for nonzero polynomials $f(x)$ and $g(x)$, there always exists polynomials $a(x)$ and $b(x)$ such that

$$\text{gcd}(f(x), g(x)) = a(x)f(x) + b(x)g(x).$$

One could also define $\text{lcm}(f(x), 0) = \text{lcm}(0, f(x)) = 0$ and $\text{gcd}(f(x), 0) = \text{gcd}(0, f(x)) = f(x)$ for any polynomial $f(x)$.

Problem 3. **

- (a) Prove Theorem 1 (for example by induction with respect to $\deg(f(x))$).

- (b) Suppose that $f(x)$ is a polynomial with coefficients in K and $f(a) = 0$ for some $a \in K$. Prove that you can write $f(x) = (x - a)q(x)$ for some polynomial $q(x) \in K[x]$.
- (c) Use this to show that a nonzero polynomial of degree n has at most n zeroes.

2. EUCLID'S ALGORITHM

We can also compute the greatest common divisor of two nonzero polynomials $f(x)$ and $g(x)$ using the Euclidean algorithm. Let us assume that $\deg(f(x)) \geq \deg(g(x))$. Put $r_0(x) = f(x)$ and $r_1(x) = g(x)$. If $r_i(x) \neq 0$ then we define $r_{i+1}(x)$ and $q_i(x)$ inductively by

$$r_{i-1}(x) = q_i(x)r_i(x) + r_{i+1}(x)$$

where $q_i(x), r_{i+1}(x) \in K[x]$ and $\deg(r_{i+1}(x)) < \deg(r_i(x))$. Since $\deg(r_0(x)) > \deg(r_1(x)) > \dots$ we must have $r_{k+1}(x) = 0$ for some k . So we have

$$\begin{aligned} r_0(x) &= q_1(x)r_1(x) + r_2(x) \\ r_1(x) &= q_2(x)r_2(x) + r_3(x) \\ &\vdots \\ r_{k-2}(x) &= q_{k-1}(x)r_{k-1}(x) + r_k(x) \\ r_{k-1}(x) &= q_k(x)r_k(x) \end{aligned}$$

Up to a constant $r_k(x)$ is equal to $\gcd(f(x), g(x))$. All proofs are similar to the GCD algorithm for integers.

Problem 4. * What are the quotient and the remainder of division of $x^7 + x^5 - x^4 + 2x^3 + 4x^2 - 1$ by $x^3 + x^2 - x + 1$?

3. CHINESE REMAINDER THEOREM

Definition 1. If $a(x), b(x), f(x) \in K[x]$ are polynomials then we write

$$a(x) \equiv b(x) \pmod{f(x)}$$

if $f(x)$ divides the $a(x) - b(x)$.

We now can formulate a Chinese Remainder Theorem for polynomials.

Theorem 4 (Chinese Remainder Theorem). *If $f(x)$ and $g(x)$ are polynomials with $\gcd(f(x), g(x)) = 1$ and $a(x), b(x) \in K[x]$ are polynomials, then there exists a polynomial $c(x) \in K[x]$ with $\deg(c(x)) < \deg(f(x)) + \deg(g(x))$ such that*

$$c(x) \equiv a(x) \pmod{f(x)}$$

and

$$c(x) \equiv b(x) \pmod{g(x)}$$

Problem 5. *** (Interpolation) Suppose that $a_1, a_2, \dots, a_n \in \mathbb{R}$ are distinct and that $b_1, b_2, \dots, b_n \in \mathbb{R}$. Prove that there exists a polynomial $f(x)$ with real coefficients such that $f(a_i) = b_i$ and f has degree at most $n - 1$. (*Hint: For $i = 1, 2, 3, \dots, n$ define a polynomial f_i such that $f_i(a_j) = 0$ for all $j \neq i$ and $f_i(a_i) = b_i$. Then define $f = \sum_i f_i$.)*)

4. UNIQUE FACTORIZATION

Just as for the unique factorization into prime numbers, every polynomial has a unique factorization into irreducible polynomials.

Theorem 5. *Every monic polynomial in $K[x]$ can be uniquely (up to permutation) written as a product of monic irreducible polynomials.*

5. THE FUNDAMENTAL THEOREM OF ALGEBRA

Theorem 6 (Fundamental Theorem of Algebra). *If $P(z) = z^n + a_{n-1}z^{n-1} + \dots + a_1z + a_0$ is a polynomial with complex coefficients a_0, a_1, \dots, a_{n-1} , then*

$$P(z) = (z - x_1)(z - x_2) \cdots (z - x_n)$$

for some complex numbers x_1, x_2, \dots, x_n . Here x_1, x_2, \dots, x_n are exactly the zeroes of $P(z)$, (some zeroes may appear several times, we call them multiple zeroes).

The fundamental theorem of algebra implies that the only irreducible monic polynomials over the complex numbers are of the form $z - a$, with $a \in \mathbb{C}$.

Corollary 1. *If $P(z) = z^n + a_{n-1}z^{n-1} + \dots + a_1z + a_0$ is a polynomial with real coefficients a_0, a_1, \dots, a_{n-1} , then we can write*

$$P(z) = Q_1(z)Q_2(z) \cdots Q_r(z)$$

where $Q_i(z)$ is a monic polynomial of degree 1 or 2 for every i .

Proof. It suffices to show that irreducible polynomials over \mathbb{R} have degree 1 or 2. Suppose that $P(z)$ is an monic irreducible nonconstant polynomial. According to the previous theorem, there exists a complex root $a \in \mathbb{C}$. If a is real, then $P(z)$ is divisible by $z - a$ and we must have $P(z) = z - a$ because $P(z)$ is irreducible. If a is not real, then $P(\bar{a}) = 0$ as well, where \bar{a} is the complex conjugate of a . Let $Q(z) = (z - a)(z - \bar{a}) = z^2 - (a + \bar{a})z + a\bar{a}$. The polynomial $Q(z)$ divides $P(z)$ and $Q(z)$ has real coefficients. Because $P(z)$ is irreducible, we have that $P(z) = Q(z)$. \square

Suppose that $P(z)$ is a monic polynomial of degree n with zeroes x_1, x_2, \dots, x_n . Then we have

$$P(z) = (z - x_1)(z - x_2) \cdots (z - x_n).$$

If we multiply this out we get

$$P(z) = z^n - e_1z^{n-1} + e_2z^{n-2} - \cdots + (-1)^n e_n$$

where

$$e_k = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

are called the *elementary symmetric polynomials*. In particular we have

$$e_1 = x_1 + x_2 + \cdots + x_n$$

which is the sum of all zeroes,

$$e_2 = x_1 x_2 + x_1 x_3 + \cdots + x_1 x_n + x_2 x_3 + x_2 x_4 + \cdots + x_2 x_n + \cdots + x_{n-1} x_n.$$

which is the sum of all products of distinct variables, and

$$e_n = x_1 x_2 \cdots x_n$$

which is just the product of all variables. You probably know the case $n = 2$. In that case we get $P(z) = (z - x_1)(z - x_2) = z^2 - (x_1 + x_2)z + x_1 x_2$, so $s_1 = x_1 + x_2$ and $s_2 = x_1 x_2$.

A polynomial $Q(x_1, x_2, \dots, x_n)$ in the variables x_1, x_2, \dots, x_n is called *symmetric* if

$$Q(x_1, \dots, x_n) = Q(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

if $\sigma(1), \sigma(2), \dots, \sigma(n)$ is a permutation of $1, 2, \dots, n$. The *elementary symmetric polynomials* are of course symmetric. Other important symmetric polynomials are the power sums:

$$p_k = x_1^k + x_2^k + \cdots + x_n^k.$$

PROBLEMS

Problem 6. ** Show that

$$p_{n+k} - e_1 p_{n+k-1} + e_2 p_{n+k-2} - \cdots + (-1)^n e_n p_k = 0.$$

Problem 7. * Show that $e_2 = (p_1^2 - p_2)/2$, and $e_3 = (p_1^3 - 3p_1 p_2 + 2p_3)/6$.

Problem 8. ** Suppose that $P(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_0$ is a polynomial with n distinct real zeroes, x_1, x_2, \dots, x_n . Express

$$\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n}$$

in terms of a_0, a_1, \dots, a_{n-1} .

Problem 9. *** Suppose that x_1, x_2, x_3 are complex numbers with

$$x_1 + x_2 + x_3 = x_1^2 + x_2^2 + x_3^2 = x_1^3 + x_2^3 + x_3^3 = 10.$$

What is $x_1^4 + x_2^4 + x_3^4$? (*Hint:* Use problem 6 and problem 7.)

Problem 10. **** Show that we have equality of *formal* power series

$$\sum_{k=1}^{\infty} \frac{(e_1 z - e_2 z^2 + e_3 z^3 - \cdots + (-1)^{n-1} e_n z^n)^k}{k} = p_1 z + \frac{p_2}{2} z^2 + \frac{p_3}{3} z^3 + \cdots.$$

Problem 11. *** Suppose that $|z| < 1$. Show that

$$\prod_{n=1}^{\infty} \frac{1}{(1 - z^{2^{n-1}})} = \prod_{n=1}^{\infty} (1 + z^n).$$

Problem 12. (Polya's Theorem)**** If $P(z) = z^n + a_{n-1}z^{n-1} + \dots + a_0$ is a polynomial with real coefficients, such that $P(z) > 0$ for $z > 0$. Prove that $(1 + z)^n P(z)$ has nonnegative coefficients. (For example, $1 - 3z + 3z^2 > 0$ for all $z > 0$, and

$$(1 + z)^{13}(1 - 3z + 3z^2) = 1 + 10z + 42z^2 + 91z^3 + 91z^4 + 1287z^8 + 429z^7 + 2002z^9 + 2002z^{10} + 1365z^{11} + 637z^{12} + 196z^{13} + 36z^{14} + 3z^{15}$$

has nonnegative coefficients. By the way, 13 was the smallest power with this property here. *Hint:* Use the fundamental theorem of algebra for polynomials with real coefficients.)

Problem 13. *** A polynomial $P(z)$ with real coefficients of degree n starts with

$$az^n + bz^{n-1} + cz^{n-2} + \dots$$

Show that if $P(z)$ cannot have n real zeroes if $b^2 - 2ac < 0$. Also show that there exists a polynomial $P(z)$ with n real zeroes for which $b^2 - 4ac < 0$.

Problem 14. * A polynomial $P(z) = a_n z^n + a_{n-1} z^{n-1} + \dots + a_1 z + a_0$ is called symmetric if $a_i = a_{n-i}$ for all i . (Assume that $a_n \neq 0$.) Prove that for a symmetric polynomial $P(z)$ we have that x is a zero of $P(z)$ if and only if $1/x$ is a zero of $P(z)$.

Problem 15. ** Find all zeroes of the (symmetric) polynomial

$$P(z) = z^4 + 10z^3 + 23z^2 + 10z + 1.$$

(*Hint:* first prove that there exists a factorization $P(z) = (z^2 + az + 1)(z^2 + bz + 1)$ using the previous problem.)

6. EXTRA PROBLEMS

Problem 16. * Suppose that $f(x)$ is a polynomial with integer coefficients, and that a, b are integers. Show that $f(a) - f(b)$ is divisible by $a - b$. In particular, if $a \equiv b \pmod{n}$ for some integer n , then $f(a) \equiv f(b) \pmod{n}$.

Problem 17. *** Let $P(x)$ be a polynomial with integer coefficients. Prove: There do not exist three distinct integers a, b, c such that $P(a) = b$, $P(b) = c$ and $P(c) = a$.

Problem 18. *** Find a polynomial $P(x, y, z, t)$ (with real coefficients) such that $P(2, 0, 0, 1) = 2001$, but $P(a, b, c, d) = 0$ for all other quadruples of integers with $0 \leq a, b, c, d \leq 9$.

Problem 19. ***

(a) Prove the identity

$$\cos(nx) = 2 \cos(x) \cos((n-1)x) - \cos((n-2)x)$$

for natural numbers n and $x \in \mathbb{R}$.

(b) Prove that for every natural number n there exists a polynomial $T_n(x)$ of degree n such that $T_n(\cos(x)) = \cos(nx)$. (These polynomials $T_n(x)$ are called *Chebyshev Polynomials*).

(c) Prove that $|T_n(x)| \leq 1$ for $|x| \leq 1$ and that the leading coefficient of $T_n(x)$ is 2^{n-1} (i.e., $T_n(x) = 2^{n-1}x^n + \dots$).

Problem 20. ***** Suppose that $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ is a polynomial of degree n and $|P(x)| \leq 1$ for $|x| \leq 1$. Prove that $|a_n| \leq 2^{n-1}$. (*Hint: You may use the results of the previous problem. If $|a_n| > 2^{n-1}$, then show that $T_n(x) - \frac{2^{n-1}}{a_n} P(x)$ is a polynomial of degree $n-1$ with at least n zeroes.*)

Problem 21. ***** Suppose

$$f(x) - f(y) = a(x, y)(g(x) - g(y))$$

for some polynomials $f(x)$ and $g(x)$ and a polynomial $a(x, y)$ in two variables. Prove that there exists a polynomial h such that $f(x) = h(g(x))$.

Problem 22 (Putnam 1986, A6). ***** Let a_1, a_2, \dots, a_n be real numbers, and let b_1, b_2, \dots, b_n be distinct positive integers. Suppose that there is a polynomial $f(x)$ satisfying the identity

$$(1-x)^n f(x) = 1 + \sum_{i=1}^n a_i x^{b_i}.$$

Find a simple expression (not involving any sums) for $f(1)$ in terms of b_1, b_2, \dots, b_n and n (but independent of a_1, a_2, \dots, a_n).

Problem 23 (Putnam). ***** Let $f(x)$ be a polynomial with integer coefficients. Define a sequence a_0, a_1, \dots of integers such that $a_0 = 0$ and $a_{n+1} = f(a_n)$ for all $n \geq 0$. Prove that if there exists a positive integer m for which $a_m = 0$, then either $a_1 = 0$ or $a_2 = 0$.

Problem 24. ***** (Gauss' Lemma)

- (a) If $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ is a polynomial with integer coefficients, then the *content* $c(f(x))$ of $f(x)$ is defined as $\gcd(a_n, a_{n-1}, \dots, a_0)$. Prove that $c(f(x)g(x)) = c(f(x))c(g(x))$ if $f(x)$ and $g(x)$ are polynomials with integer coefficients. (*Hint: Reduce to the case that $c(f(x)) = c(g(x)) = 1$. Then reduce the polynomials modulo some prime numbers and see what happens.*)
- (b) If $f(x)$ is a polynomial with integer coefficients and $f(x) = a(x)b(x)$ with $a(x)$ and $b(x)$ nonconstant polynomials with rational coefficients, then one can find polynomials $\tilde{a}(x)$ and $\tilde{b}(x)$ with *integer* coefficients such that

$f(x) = \tilde{a}(x)\tilde{b}(x)$. (In other words, $f(x)$ is reducible over \mathbb{Q} if and only if $f(x)$ is reducible over \mathbb{Z} .)

Problem 25. ***** Prove the Eisenstein criterion. If $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ is a polynomial with integer coefficients, and p is a prime number such that p divides a_1, a_2, \dots, a_{n-1} , p does not divide a_n and p^2 does not divide a_0 . Then $f(x)$ is irreducible over \mathbb{Q} (it suffices to show, using the previous problem, that it is impossible to write $f(x)$ as a product of two nonconstant polynomials with integer coefficients).

Problem 26 (Putnam 1985, B2). *** Let k be the smallest positive integer for which there exist distinct integers m_1, m_2, m_3, m_4, m_5 such that the polynomial

$$p(x) = (x - m_1)(x - m_2)(x - m_3)(x - m_4)(x - m_5)$$

has exactly k nonzero coefficients. Find, with proof, a set of integers m_1, m_2, m_3, m_4, m_5 for which this minimum k is achieved.