Polynomials

by: Adrian Tang

You will first warm-up by remembering how to factor certain common polynomials.

Exercise 1: Factor each of the following polynomials over $\mathbb{Z}$; $x^3 - y^3$, $x^4 + x^2 + 1$, $x^4 + 2x^3 + 3x^2 + 2x + 1$, $4x^3 + 6x^2 + 4x + 1$, $x^5 + x^4 + x^3 + x^2 + x + 1$.

We recall a very elementary, yet important fact about finding linear factors of polynomials.

Rational Roots Theorem: Let $f(x) \in \mathbb{Z}[x]$ and $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, with $a_n \geq 0$. If $f(r/s) = 0$ for $r, s \in \mathbb{Z}, gcd(r, s) = 1$. Then $(sx - r)$ is a factor of f. Furthermore, if $f(r/s) = 0$, then r divides a_0 and s divides a_n. If $f(r/s) \neq 0$ for all $r, s \in \mathbb{Z}$ such that $gcd(r, s) = 1$ and $r \mid a_0$ and $s \mid a_n$, then f has no linear factors. (Of course, f can still have non-linear factors, say, quadratic factors.)

Definition: We say that a polynomial $f(x) \in \mathbb{Z}[x]$ is *irreducible* over $\mathbb{Z}$ if $f(x) = g(x)h(x)$ implies at least one of g, h is a constant polynomial in $\mathbb{Z}[x]$. We define irreducibility over $\mathbb{R}[x]$ and $\mathbb{C}[x]$ similarly.

Fundamental Theorem of Algebra All polynomials $f(x) \in \mathbb{R}[x]$ factors completely and uniquely (up to order of factors) over $\mathbb{C}[x]$. For all $f(x) \in \mathbb{R}[x]$ with degree n, we have

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n).$$

for some $\alpha_1, \cdots, \alpha_n \in \mathbb{C}$. (The proof is omitted as it is difficult to prove.)

If $\alpha = a + bi$ with $b \neq 0$ is a root of f, then $\overline{\alpha} = a - bi$, the conjugate of α is also a root of f. i.e. a polynomial always has an even number of non-real roots, where the non-real roots come in pairs in the form of conjugates.

Irreducibility over $\mathbb{R}[x]$: All polynomials $f(x) \in \mathbb{R}[x]$ factors over $\mathbb{R}[x]$ into linear and quadratic polynomials, where the roots of each quadratic polynomial are non-real and are conjugates of each other. Recall $ax^2 + bx + c = 0, a \neq 0$ is irreducible over $\mathbb{R}[x]$ if $b^2 - 4ac < 0$.

Exercise 2: Let $f(x) \in \mathbb{R}[x]$ be a polynomial such that $f(x) \geq 0$ for all $x \in \mathbb{R}$. Prove that $f(x)$ can be written as the sum of two squares of real polynomials. i.e.

$$f(x) = g(x)^2 + h(x)^2$$

for some $a, b \in \mathbb{R}[x]$. (Hint: Recall Brahmagupta's identity, which is $(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$.)

Irreducibility over $\mathbb{Z}[x]$: It is in general difficult to determine whether a polynomial in $\mathbb{Z}[x]$ is irreducible over $\mathbb{Z}[x]$. Let $a, b, c, d \in \mathbb{Z}$.

• $ax^2 + bx + c, a \neq 0$ is irreducible over $\mathbb{Z}[x]$ if and only if $b^2 - 4ac$ is not a perfect square.

• $ax^3 + bx^2 + cx + d, a \neq 0$: If $f(m/n) \neq 0$ for all $m, n \in \mathbb{Z}, n \neq 0$ and $m|d$ and $n|a$, then $f(x)$ is irreducible over $\mathbb{Z}[x]$.

For higher degree polynomials, it is in general difficult to determine whether a polynomial with integer coefficients is irreducible over $\mathbb{Z}[x]$. We demonstrate a few irreducibility criterion in these notes. Keep in mind that these criterions only provide sufficient conditions for irreducibility, but not necessary conditions.

Eisenstein's Criterion: Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Suppose there is a prime number p such that $p \nmid a_n$, $p|a_i$ for all $i = 0, 1, 2, \cdots, n-1$ and p^2 does not divide a_0. Then $f(x)$ is irreducible.

Proof: Suppose $f(x) = g(x)h(x)$. Let

$$g(x) = \sum_{i=0}^{r} b_i x^i \text{ and } h(x) = \sum_{j=0}^{s} c_j x^j$$

where $b_r, c_s \neq 0$. Since p divides $b_0 c_0$ but p^2 does not, exactly one of b_0, c_0 is divisible by p. Without loss of generality, suppose b_0 is divisible by p. Let t be the smallest index such that $p \nmid b_t$. This must hold and $0 \leq t < r$ since $p \nmid a_n$ which implies $p \nmid b_r$. Since $p \nmid c_0$, we have that

$$p \nmid b_t c_0 + b_{t-1} c_1 + \cdots + b_0 c_t$$

since p divides all terms except $b_t c_0$. But this right-hand term is the coefficient of x^t in $f(x)$, which is divisible by p. This is a contradiction. Therefore, f is irreducible.

i.e. $f(x) = x^3 + 9x^2 - 6x + 3$ is irreducible over $\mathbb{Z}[x]$.

Exercise 3: Let p be a prime. Prove that $x^{p-1} + x^{p-2} + \cdots + 1$ is irreducible over $\mathbb{Z}[x]$. (Hint: Replace x with $x + 1$).

We say that $\alpha \in \mathbb{C}$ is algebraic if there exists a polynomial with integer coefficients such that $f(\alpha) = 0$. Otherwise, α is said to be transcendental. It is true (but difficult to prove) that e and π are transcendental. Another fact that is important but non-trivial to prove is that if α and β are algebraic, then $\alpha + \beta$ and $\alpha\beta$ are also algebraic.

Suppose $\alpha \in \mathbb{C}$ be an algebraic element and let $f(x)$ be the polynomial of minimum degree such that $f(\alpha) = 0$. Then $f(x)$ is unique. We call this polynomial the **minimal polynomial** over α.

Examples:
• If $\alpha = a/b \in \mathbb{Q}$, then $bx - a$ is the minimal polynomial of a/b

• If $\alpha = a + b\sqrt{D}$ where $a, b \in \mathbb{Q}$ and D is not a perfect square, then $x^2 - 2a + (a^2 - bD^2) = 0$ is the minimal polynomial of α.

• Let $\alpha = cis(2\pi/p)$, which is a root of $x^p - 1$. Then by Exercise 3, the minimal polynomial of α is $x^{p-1} + x^{p-2} + \cdots + x + 1$.

Exercise 4: Find the minimal polynomial for $\sqrt{2} + \sqrt{3}$.

Important Fact About Minimal Polynomials: Let $\alpha \in \mathbb{C}$ be an algebraic element with minimal polynomial $f(x) \in \mathbb{Z}[x]$. Then if $g \in \mathbb{Z}[x]$ with $g(\alpha) = 0$, then $f(x)$ divides $g(x)$. Note that this generalizes a part of the Rational Roots Theorem.

Lagrange Interpolation: Recall that $n + 1$ distinct pairs (a_i, b_i) (with a_i distinct) determine a unique polynomial $f \in \mathbb{R}[x]$ with $f(a_i) = b_i$. It is determined by the polynomial

$$f(x) = \sum_{i=1}^{n+1} \frac{\prod_{j \neq i} (x - a_j)}{\prod_{j \neq i} (a_j - a_i)} \cdot b_i.$$

It is easy to check that $f(a_i) = b_i$ in this equation. This is called Lagrange Interpolation.

Exercise 5: Let $f(x)$ be a polynomial with degree 2008 such that $f(n) = 2^n$ for $n = 0, 1, \cdots, 2008$. Find $f(2009)$.

Suppose $\alpha_1, \cdots, \alpha_n$ are the roots of a polynomial. (We are allowing repeated roots.) We can construct the polynomial of degree n that has $\alpha_1, \cdots, \alpha_n$ as roots. (This polynomial is of course unique up to a non-zero constant multiple.)

Exercise 6: Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ and $\alpha_1, \cdots, \alpha_n$ be the roots of this polynomial. Prove that

(a) $\alpha_1 + \alpha_2 + \cdots + \alpha_n = (-1) \cdot a_{n-1}$
(b) $\alpha_1\alpha_2 \cdots \alpha_n = (-1)^n a_0$.
(c) Let t be an integer such that $1 \leq t \leq n$. Prove that

$$\sum_{S \subseteq \{1, \cdots, n\}, |S| = t} \left(\prod_{i \in S} a_i \right) = (-1)^t \alpha_{n-t}.$$

Let $f_t(\alpha_1, \cdots, \alpha_n)$ be the expression on the left-hand side of c. This expression is called the degree

t elementary symmetric polynomials on n variables. For example, the degree 1, 2, 3 elementary symmetric functions on $\alpha_1, \alpha_2, \alpha_3$ are $\alpha_1 + \alpha_2 + \alpha_3, \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1, \alpha_1\alpha_2\alpha_3$, respectively.

Fundamental Theorem of Elementary Symmetric Polynomials: Every symmetric polynomial with n variables $\alpha_1, \cdots, \alpha_n$ can be written as a combination (via addition and multiplication) of the elementary symmetric polynomials on n variables.

For example, the symmetric polynomial $x^3 + y^3 + z^3$ and be written as $x^3 + y^3 + z^3 = (x + y + z)^3 - 3(x + y + z)(xy + yz + zx) + 3xyz$.

The point of this theorem is not to know the proof, but rather knowing that you can write any symmetric polynomials in terms of elementary symmetric polynomials. These elementary symmetric polynomials reveal the polynomial whose roots are the n variables. Try solving the following equations, particularly 7(b).

Exercise 7a: Solve the following system of equations: (Note that solutions are in $\mathbb{C}$)

$$\begin{array}{rcrcrcl} x & + & y & + & z & = & 6 \\ xy & + & yz & + & zx & = & 11 \\ & & & & xyz & = & 6 \end{array}.$$

Exercise 7b: Solve the following system of equations:

$$\begin{array}{rcrcrcl} x & + & y & + & z & = & 3 \\ x^2 & + & y^2 & + & z^2 & = & 3 \\ x^3 & + & y^3 & + & z^3 & = & 3 \end{array}.$$

We finish off this section by presenting three other irreducible criterion. We will prove one of them. We will simply state the remaining two since the proofs of these criterion are long.

Polynomials with Constant Terms Which Are Prime and Large Compared With Other Coefficients, are Irreducible. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients such that $|a_0|$ is prime and

$$|a_0| > |a_1| + |a_2| + \cdots + |a_n|.$$

Then f is irreducible.

Proof: We first prove that if $\alpha \in \mathbb{C}$ is a root of f, then $|\alpha| > 1$. Suppose $|\alpha| \leq 1$. Then $f(\alpha) = 0$ implies that $a_0 = -(a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha)$. Hence,

$$|a_0| = |a_n\alpha^n + \cdots + a_1\alpha| \leq |a_n\alpha^n| + \cdots + |a_1\alpha| < |\alpha_n| + \cdots + |\alpha_1|$$

which contradicts the statement in the problem. Therefore, $|\alpha| > 1$ for all roots α of f.

Finally, suppose $f = gh$ where g, h are non-constant polynomials. Since $|a_0|$ is prime, we have that one of the constant terms of g, h is equal to ± 1. Without loss of generality, suppose the constant term of g is ± 1. Let b be the leading coefficient of g. Let $\alpha_1, \cdots, \alpha_t$ be the roots of g. Since the constant term of g is 1 and the leading coefficient of g is b, we have that $|\alpha_1\alpha_2\cdots\alpha_t| = 1/|b| \leq 1$. This implies that $|\alpha_i| \leq 1$ for some i. But α_i is also a root of f and we proved that $|\alpha_i| > 1$. This is a contradiction. Therefore, f is irreducible. $\square$

Perron's Criterion - Second Coefficient is Large Compared of a Monic Polynomial with Other Coefficients Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients with $a_0 \neq 0$ and

$$|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_1| + |a_0|.$$

Then $f(x)$ is irreducible.

Cohn's Criterion - Prime Numbers in Base b Representation Form Irreducible Polynomials Let p be a prime number and $b \geq 2$ be an integer. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients where $p = a_n a_{n-1}\cdots a_0$, is the base-$b$ representation of p. i.e. $0 \leq a_i < p$ such that $p = \sum_{i=0}^{n} a_i p^i$. Then $f(x)$ is irreducible.

Finally, onto the problem set.

Warm-Up Problems

The following are a list of facts about polynomials that you need to know off the top off your head and how to prove them.

1. Suppose f, g are polynomials are agree on more than $\max\{\deg f, \deg g\} + 1$ number of points. Prove that $f \equiv g$. Conclude that if f, g agree on infinitely many points, then $f \equiv g$.

2. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ and $g(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$ be polynomials with integer coefficients with $a_n, a_0 \neq 0$. Prove that f is irreducible over $\mathbb{Z}[x]$ if and only if g is irreducible over $\mathbb{Z}[x]$.

3. Let $f(x) = x^3 - ax^2 + bx - c$ be a polynomial with three positive real roots. Prove that $a^2 \geq 3b$.

4. Let f be a polynomial with integer coefficients. Let a, b be distinct integers. Prove that $a - b$ divides $f(a) - f(b)$.

5. Let a, b be integers, n a positive integer and f a polynomial with integer coefficients. Prove that if $a \equiv b \bmod n$, then $f(a) \equiv f(b) \bmod n$.

6. Let f be a polynomial on m variables and n be a positive integer. Let $a_1, b_1, \cdots, a_m, b_m$ be integers such that $a_i \equiv b_i \bmod n$ for each i. Prove that $f(a_1, a_2, \cdots, a_m) \equiv f(b_1, b_2, \cdots, b_m) \bmod n$.

7. Find all polynomials f such that $f(x) = f(-x)$ for all $x \in \mathbb{R}$. Find all polynomials f such that $f(x) = -f(-x)$ for all $x \in \mathbb{R}$.

8. Prove that for any polynomial f, there exists a unique polynomial g such that $f(x) = g(x+1) - g(x)$ for all $x \in \mathbb{R}$.

9. (Calculus required:) Prove that every the roots of a polynomial f are pairwise distinct if and only if $gcd(f, f') = 1$ where f' is the standard derivative of f. Conclude that an irreducible polynomial cannot contain repeated roots.

10. The following examples draw parallels to the integers in the study of number theory. Let $f(x), g(x)$ be polynomials with integer coefficients.

    (a) Prove that there exists a unique pair of polynomials $q(x), r(x)$ with integer coefficients such that $f(x) = q(x)g(x) + r(x)$ where $\deg r < \deg g$.

    (b) Let $d(x) = gcd(f(x), g(x))$. Prove that there exist polynomials $a(x), b(x)$ with integer coefficients such that
    $$a(x)f(x) + b(x)g(x) = d(x).$$

(We note that the gcd of two polynomials is always monic.)

(c) Let $h(x)$ be a polynomial with integer coefficients. We say that $f(x) \equiv g(x) \mod h(x)$ if $h(x)$ divides $f(x) - g(x)$. Let $p_1(x), p_2(x), \cdots, p_n(x)$ be pairwise relatively prime polynomials with integer coefficients. Let $r_1(x), r_2(x), \cdots, r_n(x)$ be polynomials with integer coefficients. Prove that there exists a unique polynomial $u(x)$ such that $u(x) \equiv r_i(x) \mod p_i(x)^{e_i}$ for all $i \in \{1, 2, \cdots, n\}$, where $e_1, \cdots, e_i$ are positive integers and $\deg u < \sum_{i=1}^{n} e_i \deg p_i$.

Exercises:

1. Let f be a polynomial whose sum of the coefficients is 0. Prove that f is not irreducible.

2. Find all polynomials with integer coefficients such that $|f(n)|$ is prime for all $n \in \mathbb{Z}$.

3. Prove that there are infinitely many pairs of polynomials with integer coefficients $(f(x), g(x))$ with $gcd(f, g) = 1$ such that
$$\frac{f(x)^2}{g(x)^2} = \frac{f(x^2)}{g(x^2)} + 2.$$

4. (Sweden, unknown year) Find all polynomials P with real coefficients such that
$$1 + P(x) = \frac{1}{2}(P(x-1) + P(x+1))$$
for all real x.

5. (IMO 1993) For all positive integers n, $x^n + 5x^{n-1} + 3$ is irreducible over $\mathbb{Z}[x]$.

6. Find all polynomials f with real coefficients such that
   (a) $f(x^2) = f(x)^2$.
   (b) (New Zealand 2005) $f(x^2) = f(x)f(x+1)$

7. (APMO 2009 - Sane Version) Let a_1, a_2, a_3, a_4, a_5 be real numbers such that
$$\frac{a_1}{k^2+1} + \frac{a_2}{k^2+2} + \frac{a_3}{k^2+3} + \frac{a_4}{k^2+4} + \frac{a_5}{k^2+5} = \frac{1}{k^2}$$
for $k = 1, 2, 3, 4, 5$. Find $a_1 + a_2 + a_3 + a_4 + a_5$.

8. a.) Let $f(x) \in \mathbb{Z}$ and $k \geq 3$ be an odd positive integer. Suppose $a_1, a_2, \cdots, a_k$ be integers such that $a_{i+1} = P(a_i)$ for $i = 1, 2, \cdots, k-1$ and $a_1 = P(a_k)$. Prove that $a_1 = a_2 = \cdots = a_k$.

   b.) (IMO 2006) Let $P(x)$ be a polynomial of degree $n > 1$ with integer coefficients and $k \in \mathbb{N}$. Consider the polynomial
   $$Q(x) = P(P(\cdots(P(x)\cdots))).$$
   (where P appears k times). Prove that there are at most n integers t such that $Q(t) = t$.

   c.) (Japan 2005) Let $P(x, y), Q(x, y)$ be two-variable polynomials with integer coefficients. Let $\{a_n\}_{n\in\mathbb{N}}, \{b_n\}_{n\in\mathbb{N}}$ be sequences such that
   $$a_{n+1} = P(a_n, b_n), b_{n+1} = Q(a_n, b_n).$$
   Suppose $(a_2, b_2) \neq (a_1, b_1)$ and $(a_k, b_k) = (a_1, b_1)$ for some $k > 2$. Prove that the number of internal lattices points on the segment with endpoints (a_n, b_n) and (a_{n+1}, b_{n+1}) is constant for all $n \in \mathbb{N}$.

9. (Romania TST 2005) Let $p \geq 5$ be a prime number and n be a positive integer. Find the number of polynomials of the form
   $$x^n + px^k + px^l + 1$$
   where $1 \leq l < k < n$, that are irreducible. Express your answer in terms of n.

10. (Iran 2005) Let $p(x) \in \mathbb{Q}[x]$ be an irreducible polynomial such that $\deg p$ is odd. Let $q(x), r(x) \in \mathbb{Q}[x]$ such that
    $$p(x) \mid q(x)^2 + q(x)r(x) + r(x)^2.$$
    Prove that
    $$p(x)^2 \mid q(x)^2 + q(x)r(x) + r(x)^2.$$

11. (Iran 2007) Find all polynomials f with integer coefficients such that $a + b + c$ divides $f(a) + f(b) + f(c)$ for all positive integers a, b, c.

12. (Iran 2004) Find all polynomials f with integer coefficients such that $gcd(a, b) = 1$ implies $gcd(f(a), f(b)) = 1$ for all positive integers a, b.

13. (Iran 2003) Let $f_1, f_2, \cdots, f_n$ be polynomials with integer coefficients. Prove that that there exists a reducible polynomial g such that $f_1 + g, f_2 + g, \cdots, f_n + g$ are irreducible polynomials over $\mathbb{Z}[x]$.

14. Let $f(x)$ be a polynomial with integer coefficients. Prove that there exists a positive integer k such that $f(x) - k$ is irreducible over $\mathbb{Z}[x]$.

15. Let f be an integer with positive integer coefficients. Alice and Bob play the following game. Bob knows f but Alice does not. Alice gives Bob a positive integer a of her choice. Bob then tells Alice $f(a)$. Alice then gives Bob a positive integer b of her choice and Bob then tells Alice $f(b)$. Prove that Alice can choose a, b such that Alice can figure out what f is.

16. Does there exist a sequence of pairwise relatively prime integers $a_0, a_1, a_2, \cdots$ such that for each $n \geq 1$, the polynomial
$$a_0 + a_1 x + \cdots + a_n x^n$$
is irreducible?

17. (IMO 2002) Find all pairs of positive integers (m, n) with $m, n \geq 3$ such that there exist infinitely many positive integers a such that
$$\frac{a^m + a - 1}{a^n + a^2 - 1}$$
is an integer.

18. (IMO 2005 Shortlist) Let a, b, c, d, e and f be positive integers. Suppose that the sum $S = a + b + c + d + e + f$ divides both $abc + def$ and $ab + bc + ca - de - ef - fd$. Prove that S is composite.

19. Let $f(x)$ be a monic polynomial with integer coefficients such that all its zeros lie on the unit circle. Show that all the zeros of $f(x)$ are roots of unit, i.e. $f(x) \mid (x^n - 1)^k$ for some positive integers n, k.

20. Find all positive integers k for which the following statement is true: if $P(x)$ is a polynomial with integer coefficients satisfying the condition $0 \leq P(c) \leq k$ for $c = 0, 1, \cdots, k + 1$, then $P(0) = P(1) = \cdots = P(k + 1)$.

Polynomials Modulo Primes

We end these notes discussing polynomials modulo primes. Let n be a positive integer. We define the set

$$\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$$

where addition and multiplication are performed modulo n. We can also define polynomials over $\mathbb{Z}_n[x]$. For example, $x^2 - 1 \equiv x^2 + 4 \bmod 5$ since $-1 \equiv 4 \bmod 5$. Formally, we say that two polynomials $f(x), g(x)$ are congruent modulo n if their corresponding coefficients differ by a multiple of n.

We will primarily focus on the case when $n = p$, a prime. An interesting thing occurs when we consider irreducible polynomials modulo p. We know that x^2+1 is irreducible over $\mathbb{Z}[x]$. However, note that we can factor x^2+1 over $\mathbb{Z}_5[x]$. This is because $x^2+1 = x^2-4 = (x-2)(x+2) = (x+3)(x+2)$. (Remember everything is taken modulo 5. So 5 is equal to 0 modulo 5.) In the following exercise, we see the even though irreducible polynomials over $\mathbb{Z}[x]$ can factor over $\mathbb{Z}_p[x]$ for some primes p, it is possible that these polynomials remain irreducible over $\mathbb{Z}_p[x]$ for other primes p.

Exercise 8: Let p be a prime number. Prove that $x^2 + 1$ is irreducible over $\mathbb{Z}_p[x]$ if and only if $p \equiv 3 \bmod 4$.

You may ask at this point why we are more interested in polynomials modulo primes rather than simply positive integers. There are certain properties that make factorization over $\mathbb{Z}_p[x]$ easier if p is prime. For example, a version of the Rational Roots Theorem remain true when factorization is done over $\mathbb{Z}_p[x]$.

Rational Roots Theorem for Polynomials Modulo p: Let p be a prime and f be a polynomial in $\mathbb{Z}_p[x]$. Suppose $f(a) = 0$ for some $a \in \mathbb{Z}_p$. Then $(x - a)$ is a factor of f.

Polynomials factor uniquely over $\mathbb{Z}_p[x]$. We can also say something about the number of roots of a polynomial in $\mathbb{Z}_p[x]$.

Unique Factorization for Polynomials Modulo p: Let p be a prime and f be a polynomial in $\mathbb{Z}_p[x]$. Then f factors uniquely (up to order) into irreducible polynomials over $\mathbb{Z}_p[x]$.

Lagrange's Theorem For Roots of Polynomials Modulo p: Let p be a prime, n be a non-negative integer and f be a non-zero polynomial in $\mathbb{Z}_p[x]$ of degree n. Then f contains at most n roots in $\mathbb{Z}_p$.

Note that Unique Factorization and Lagrange's Theorem does not hold if over $\mathbb{Z}_n[x]$ if n is composite. For example, consider $x^2 - 1$ over $\mathbb{Z}_8[x]$. Note that

$$x^2 - 1 = (x - 1)(x - 7) = (x - 3)(x - 5).$$

Furthermore, note that $x = 1, 3, 5, 7$ are all roots of $x^2 - 1$. So this polynomial has degree 2 but has four roots in $\mathbb{Z}_8$. Make sure you are working over $\mathbb{Z}_p$ before you apply Lagrange's Theorem and

Unique Factorization, the latter fact we often take for granted.

Solve the following exercise and keep Fermat's Little Theorem in mind when you are solving it.

Exercise 9: Let p be a prime number.

(a) What are all p roots of the polynomial $x^p - x$ over $\mathbb{Z}_p[x]$?

(b) What are all $p-1$ roots of the polynomial $x^{p-1} - 1$ over $\mathbb{Z}_p[x]$?

(c) From (b), use a previous exercise to prove **Wilson's Theorem**, i.e. $(p-1)! \equiv -1 \bmod p$.

(d) Given $1 \leq t < p$, prove that $f_t(1, 2, \cdots, p-1)$ is divisible by p. Specifically, prove that the sum of all pairwise products from the set $\{1, 2, \cdots, p-1\}$ is divisible by p.

Exercises:

1. Let p be a prime. Prove the existence of a primitive root modulo p, i.e. there exists a positive integer g such that $p-1$ is the smallest positive integer such that $g^{p-1} \equiv 1 \bmod p$.

2. (USA TST 2005) Let n be a positive integer. Consider the set S of all monic polynomials $f(x)$ of degree n, whose coefficients are chosen from $\{1, 2, 3, , \cdots, n!\}$. Find the number of polynomials in S with the property that for every integer $k > 1$, the sequence $f(1), f(2), f(3), \cdots$ contains infinitely many integers relatively prime to k.

3. (China TST 2009) Let p be an odd prime number. Prove that the number of positive integers n such that p divides $n! + 1$ is at most $cp^{2/3}$ where c is a constant independent of p.

4. (USA TST 2008) Let n be a positive integer. Given a polynomial $f(x)$ with integer coefficients, define its signature modulo n to be the ordered sequence $f(1), f(2), \cdots, f(n)$ modulo n. Of the n^n such n-term sequences modulo n, how many are the signature of some polynomial $f(x)$ if

   (a) n is a prime

   (b) n is a positive integer not divisible by the square of a prime.

   (c) n is a positive integer not divisible by the cube of a prime.