Integer Polynomials

June 29, 2007

Yufei Zhao

yufeiz@mit.edu

We will use $\mathbb{Z}[x]$ to denote the ring of polynomials with integer coefficients. We begin by summarizing some of the common approaches used in dealing with integer polynomials.

- Looking at the coefficients
  - Bound the size of the coefficients
  - Modulos reduction. In particular, $a - b \mid P(a) - P(b)$ whenever $P(x) \in \mathbb{Z}[x]$ and a, b are distinct integers.
- Looking at the roots
  - Bound their location on the complex plane.
  - Examine the algebraic degree of the roots, and consider field extensions. Minimal polynomials.

Many problems deal with the irreducibility of polynomials. A polynomial is *reducible* if it can be written as the product of two nonconstant polynomials, both with rational coefficients. Fortunately, if the original polynomial has integer coefficients, then the concepts of (ir)reducibility over the integers and over the rationals are equivalent. This is due to **Gauss' Lemma**.

Theorem 1 (Gauss)**.** If a polynomial with integer coefficients is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.

Thus, it is generally safe to talk about the reducibility of integer polynomials without being pedantic about whether we are dealing with $\mathbb{Q}$ or $\mathbb{Z}$.

Modulo Reduction

It is often a good idea to look at the coefficients of the polynomial from a number theoretical standpoint. The general principle is that any polynomial equation can be reduced mod m to obtain another polynomial equation whose coefficients are the residue classes mod m.

Many criterions exist for testing whether a polynomial is irreducible. Unfortunately, none are powerful enough to be universal. One of the most well-known criteria is **Eisenstein's criterion**.

Theorem 2 (Eisenstein)**.** 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 $p \mid a_i$ for $0 \le i \le n-1$, $p \nmid a_n$ and $p^2 \nmid a_0$. Then $f(x)$ is irreducible.

Proof. Suppose that $f = gh$, where g and h are nonconstant integer polynomials. Consider the reduction mod p (i.e., apply the ring homomorphism $\mathbb{Z}[x] \to \mathbb{F}_p[x]$), and let $\bar{f}, \bar{g}, \bar{h}$ denote the residues of f, g, h (i.e. the coefficients are residues mod p). We have $\bar{f}(x) = a_0 x^n$. Since $\mathbb{F}_p[x]$ is a unique factorization domain, we see that the only possibilities for $\bar{g}$ and $\bar{h}$ are cx^k for some integers c and $k \ge 1$. Then, the constant terms of g and h are both divisible by p, so $p^2 \mid a_0$. Contradiction. □

The most typical example for the application of Eisenstein's criterion is to show that the cyclotomic polynomial $\Phi_p(x)$ is irreducible for prime p:

Problem 1. Let p be a prime number. Show that $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible.

Solution. The polynomial $f(x)$ is irreducible if and only if $f(x+1)$ is irreducible. We have

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1)-1} = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-2}x + p.$$

Note that $f(x+1)$ fails the Eisenstein criterion for the prime p. Therefore $f(x)$ is irreducible. □

Note that the proof of Eisenstein's criterion extends to other rings with similar properties. For instance, to show that $x^4 + 2x + 2$ is irreducible over the Gaussian integers $\mathbb{Z}[i]$, we can simply apply Eisenstein with the Gaussian prime $1 + i$.

The proof of Eisenstein's Criterion can be slightly generalized to the following. The proof is more or less the same, and so it's left as exercise.

Theorem 3 (Extended Eisenstein)**.** 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 $p \mid a_i$ for $0 \le i \le n-k$, $p \nmid a_k$ and $p^2 \nmid a_0$. Then $f(x)$ has an irreducible factor of degree greater than k.

We give one more result that relates to looking at the modulo reduction of polynomials, known as **Hensel's lemma**.

Theorem 4 (Hensel)**.** Let $a_0, a_1, \ldots, a_k$ be integers, and let $P(x) = a_n x^k + \cdots a_1 x + a_0$, and let $P'(x)$ denote the derivative of $P(x)$. Suppose that x_1 is an integer such that $P(x_1) \equiv 0 \pmod{p}$ and $P'(x_1) \not\equiv 0 \pmod{p}$. Then, for any positive integer k, there exists an unique residue $x \pmod{p^k}$, such that $P(x_k) \equiv 0 \pmod{p^k}$ and $x \equiv x_1 \pmod{p}$.

The proof of Hensel's lemma closely mimics Newton's method of finding roots. We work up the powers of p, and find the a zero of $P(x) \mod p^k$ for $k = 2, 3, \ldots$. The details of the proof are omitted here.

Root Hunting

When working with integer polynomials, it is often not enough to stay in $\mathbb{Z}$. We have to think outside the box and move our scope to the complex numbers. A lot can be a said about a polynomial if we know something about its complex zeros. Many irreducibility problems hinge on placing bounds on the zeros of the polynomial in the complex plane. We begin with a familiar example.

Problem 2. Let $f(x) = a_n x^n + a_{n-1}x^n + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients, such that $|a_0|$ is prime and

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

Show that $f(x)$ is irreducible.

Solution. Let α be any complex zero of f. Suppose that $|\alpha| \le 1$, then

$$|a_0| = |a_1\alpha + \cdots + a_n\alpha^n| \le |a_1| + \cdots + |a_n|,$$

a contradiction. Therefore, all the zeros of f satisfies $|\alpha| > 1$.

Now, suppose that $f(x) = g(x)h(x)$, where g and g are nonconstant integer polynomials. Then $a_0 = f(0) = g(0)h(0)$. Since $|a_0|$ is prime, one of $|g(0)|, |h(0)|$ equals 1. Say $|g(0)| = 1$, and let b be the leading coefficient of g. If $\alpha_1, \ldots, \alpha_k$ are the roots of g, then $|\alpha_1\alpha_2 \cdots \alpha_k| = 1/|b| \le 1$. However, $\alpha_1, \ldots, \alpha_k$ are also zeros of f, and so each has an magnitude greater than 1. Contradiction. Therefore, f is irreducible. □

Next, we present a **Perron's criterion**, which has a similar statement but a much more difficult proof compared with the previous result.

Theorem 5 (Perron)**.** Let $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with $a_0 \ne 0$ and

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

Then $P(x)$ is irreducible.

Again, the idea is to put bounds on the modulus of the roots of f. The key lies in the following lemma.

Lemma 1. Let $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ be a polynomial with

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

Then exactly one zero of P satisfies $|z| > 1$, and the other $n-1$ zeros of P satisfy $|z| < 1$.

Let us see how we can prove Perron's criterion if we have this lemma. Suppose that $P(x) = f(x)g(x)$, where f and g are integer polynomials. Since P has only one zero with modulus not less than 1, one of the polynomials f, g, has all its zeros strictly inside the unit circle. Suppose that $z_1, \ldots, z_k$ are the zeros of f, and $|z_1|, \ldots, |z_k| < 1$. Note that $f(0)$ is a nonzero integer, and $|f(0)| = |z_1 \cdots z_k| < 1$, contradiction. Therefore, f is irreducible.

Now, let us prove Lemma 1. We offer two proofs. The first proof is an elementary proof that uses only the triangle inequality. The second proof invokes theorems from complex analysis, but it is much more intuitive and instructive.

First proof of the Lemma 1. (due to Laurentiu Panaitopol) Let us suppose wolog that $a_0 \neq 0$ since we can remove any factors of the form x^k . Let's first prove that there is no root α of $P(x)$ with $|\alpha| = 1$. Suppose otherwise, then we have that

$$-a_{n-1}\alpha^{n-1} = \alpha^n + a_{n-2}\alpha^{n-2} + \cdots + a_1\alpha + a_0,$$

thus

$$\begin{aligned} |a_{n-1}| = |a_{n-1}\alpha^{n-1}| &= |\alpha^n + a_{n-2}\alpha^{n-2} + \cdots + a_1\alpha + a_0| \\ &\leq |\alpha^n| + |a_{n-2}\alpha^{n-2}| + \cdots + |a_1\alpha| + |a_0| \\ &= 1 + |a_{n-2}| + \cdots + |a_1| + |a_0|. \end{aligned}$$

This contradicts the given inequality. Therefore, no zero of $f(x)$ lies on the unit circle.

Let's denote with α_1, α_2, …, α_n be the zeros of P. Since $|\alpha_1\alpha_2 \cdots \alpha_n| = a_0$, it follows that at least one of the roots is larger than 1 in absolute value. Suppose that $|\alpha_1| > 1$ and let

$$Q(x) = x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1x + b_0$$

be the polynomial with roots α_2, α_3, …, α_n. Then,

$$P(x) = (x - \alpha_1)Q(x) = x^n + (b_{n-2} - \alpha_1)x^{n-1} + (b_{n-3} - b_{n-2}\alpha_1)x^{n-2} + \cdots + (b_0 - b_1\alpha_1)x - b_0\alpha_1$$

It follows that $b_{n-1} = 1$, $a_0 = -b_0\alpha_1$, and $a_k = b_{k-1} - b_k\alpha_1$ for all $1 \leq k \leq n-1$. Then, using the given inequality, we have

$$\begin{aligned} |b_{n-2} - \alpha_1| = |a_{n-1}| &> 1 + |a_{n-2}| + \cdots + |a_1| + |a_0| \\ &= 1 + |b_{n-3} - b_{n-2}\alpha_1| + \cdots + |b_0\alpha_1| \\ &\geq 1 + |b_{n-2}||\alpha_1| - |b_{n-3}| + |b_{n-3}||\alpha_1| - |b_{n-4}| + \cdots + |b_1||x_1| - |b_0| + |b_0||x_1| \\ &= 1 + |b_{n-2}| + (|\alpha_1| - 1)\left(|b_{n-2}| + |b_{n-3}| + \cdots + |b_1| + |b_0|\right). \end{aligned}$$

On the other hand, $|b_{n-2} - \alpha_1| \leq |b_{n-2}| + |\alpha_1|$, so

$$|b_{n-2}| + |\alpha_1| > 1 + |b_{n-2}| + (|\alpha_1| - 1)\left(|b_{n-2}| + |b_{n-3}| + \cdots + |b_1| + |b_0|\right)$$

and therefore

$$|b_{n-2}| + |b_{n-3}| + \cdots + |b_1| + |b_0| < 1.$$

Then, for any complex number α with $|\alpha| \geq 1$, we have

$$\begin{aligned}
|Q(\alpha)| &= |\alpha^{n-1} + b_{n-2}\alpha^{n-2} + b_{n-3}\alpha^{n-3} + \cdots + b_1\alpha + b_0| \\
&\geq |\alpha^{n-1}| - |b_{n-2}\alpha^{n-2}| - |b_{n-3}\alpha^{n-3}| - \cdots - |b_1\alpha| - |b_0| \\
&\geq |\alpha|^{n-1} - |\alpha|^{n-1}\left(|b_{n-2}| + |b_{n-3}| + \cdots + |b_1| + |b_0|\right) \\
&= |\alpha|^{n-1}\left(1 - |b_{n-2}| - |b_{n-3}| - \cdots - |b_1| - |b_0|\right) \\
&> 0
\end{aligned}$$

And so α cannot be a root. It follows that all the zeros of Q lie strictly inside the unit circle. This completes the proof of the lemma. □

In the polynomial P, the second term x^{n-1} is "dominating," in the sense that the absolute value of its coefficient is greater than the sum of the absolute values of all the other coefficients. In the above proof, we managed to construct a new polynomial Q, whose leading term is dominating. While exactly one zero of P is outside the unit circle, none of the zeros of Q is outside the unit circle. This observation generalizes to the following result.

Proposition 6. Let $P(z) = a_n z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$ be a polynomial with complex coefficients, and such that

$$|a_k| > |a_0| + |a_1| + \cdots + |a_{k-1}| + |a_{k+1}| + \cdots + |a_n|$$

for some $0 \leq k \leq n$. Then exactly k zeros of P lie strictly inside the unit circle, and the other $n-k$ zeros of P lie strictly outside the unit circle.

This is indeed true. The easiest way to prove this result is to invoke a well-known theorem in complex analysis, known as **Rouché's theorem**.

Theorem 7 (Rouché)**.** Let f and g be analytic functions on and inside a simple closed curve $\mathcal{C}$. Suppose that $|f(z)| > |g(z)|$ for all points z on $\mathcal{C}$. Then f and $f+g$ have the same number of zeros (counting multiplicities) interior to $\mathcal{C}$.

The proof of Rouché's theorem uses the argument principle. It can be found in any standard complex analysis textbook.

In practice, for polynomials, Rouché's theorem is generally applied to some circle, and is useful when one term is very big compared to the other terms.

Proposition 6 becomes very easy to prove with the aid of Rouché's theorem. Indeed, let us apply Rouché's theorem to the functions $a_k z^k$ and $P(z) - a_k z^k$ with the curve being the unit circle. The given inequality implies that $|a_k z^k| > |P(z) - a_k z^k|$ for all $|z| = 1$. It follows that P has the same number of zeros as $a_k z^k$ inside the unit circle. It follows that P has exactly k zeros inside the unit circle. Also, it is not hard to show that P has no zeros on the unit circle (c.f. first proof of Lemma 1). Thus we have proved Proposition 6.

Second proof of Lemma 1. Apply Proposition 6 to $k = n-1$. □

While we're at it, let's look at couple of neat applications of Rouché's theorem, just for fun. These are not integer polynomial problems, but they contain useful ideas.

Problem 3. (Romania ??) Let $f \in \mathbb{C}[x]$ be a monic polynomial. Prove that we can find a $z \in \mathbb{C}$ such that $|z| = 1$ and $|f(z)| \geq 1$.

Solution. Let $\deg P = n$. Suppose that $|f(z)| < 1$ for all z on the unit circle. Then $|f(z)| < |z^n|$ for all z on the unit circle. So, by Rouché's theorem, $f(z) - z^n$ has n roots inside the unit circle, which is impossible, since $f(z) - z^n$ has degree $n-1$. □

The Fundamental Theorem of Algebra is also an easy consequence of Rouché's theorem.

Theorem 8 (Fundamental Theorem of Algebra)**.** Any polynomial $P(x) \in \mathbb{C}[x]$ of degree n has exactly n complex zeros.

Proof. Let $P(x) = a_n x^n + \cdots + a_1 x + a_0$. For a sufficiently large real number R, we have

$$|a_n|R^n > |a_{n-1}|R^{n-1} + \cdots + |a_1|R + a_0.$$

Apply Rouché's theorem to the functions $a_n x^n$ and $P(x) - a_n x^n$ on the circle $|z| = R$, we find that $P(x)$ has exactly n zeros inside the circle. Also, since we may choose R arbitrarily large, so there are no additional zeros. □

Note that the above proof also gives a bound (although rather weak) for the zeros of a polynomial. This bound is attributed to Cauchy.

Finally, the following result is a slightly stronger version of Rouché's theorem.

Theorem 9 (Extended Rouché)**.** Let f and g be analytic functions on and inside a simple closed curve $\mathcal{C}$. Suppose that

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

for all points z on $\mathcal{C}$. Then f and g have the same number of zeros (counting multiplicities) interior to $\mathcal{C}$.

There are many ways of bounding polynomial zeros on the complex plane. The following result is worth mentioning, as it has proven useful quite a few times.

Proposition 10. Let $P(x) = a_0 + a_1 x + \cdots + a_n x^n$, where $0 < a_0 \le a_1 \le \cdots \le a_n$ are real numbers, then any complex zero of the polynomial satisfies $|z| \le 1$.

Proof. If $|z| > 1$, then, since z is a zero of $(1-x)P(x)$, we get

$$a_0 + (a_1 - a_0)z + \cdots + (a_n - a_{n-1})z^n - a_n z^n = 0.$$

Thus,

$$\begin{aligned} |a_n z^n| &= |a_0 + (a_1 - a_0)z + \cdots + (a_n - a_{n-1})z^n| \\ &\le a_0 + (a_1 - a_0)|z| + \cdots + (a_n - a_{n-1})|z^n| \\ &< a_0|z|^n + (a_1 - a_0)|z|^n + \cdots + (a_n - a_{n-1})|z|^n \\ &= a_0|z|^n - a_0|z|^n + a_1|z|^n - a_1|z|^n + \cdots + a_n|z|^n \\ &= |a_n z^n| \end{aligned}$$

contradiction. Therefore, $|z| \le 1$. □

It follows as a simple corollary that for any polynomial with positive real coefficients, $P(x) = a_0 + a_1 x + \cdots + a_n x^n$, all its zeros lie in the annulus

$$\min_{1 \le k \le n} \frac{a_{k-1}}{a_k} \le |z| \le \max_{1 \le k \le n} \frac{a_{k-1}}{a_k}$$

Finally, we present one more irreducibility criterion, known as **Cohn's criterion**. Essentially, it says that if $f(x)$ has nonnegative integer coefficients, and $f(n)$ is prime for some n greater than all the coefficients, then f is irreducible.

Theorem 11 (Cohn's Criterion)**.** Let p be a prime number, and $b \ge 2$ an integer. Suppose that $\overline{p_n p_{n-1} \cdots p_1 p_0}$ is the base-b representation of p, with $0 \le p_i < b$ for each i and $p_n \ne 0$, then the polynomial

$$f(x) = p_n x^n + p_{n-1} x^n + \cdots + p_1 x + p_0$$

is irreducible.

The following proof is due to M. Ram Murty[1].

As before, we begin with a lemma bounding the complex zeros of the polynomial.

[1] M. Ram Murty, Prime Numbers and Irreducible Polynomials, *Amer. Math. Monthly.* 109 (2002) 452–458

Lemma 2. Let $f(x) = a_n x^n + a_{n-1}x^{n-2} + \cdots + a_1 x + a_0$ belong to $\mathbb{Z}[x]$. Suppose that $a_n \geq 1$, $a_{n-1} \geq 0$, and $|a_i| \leq H$ for $i = 0, 1, \ldots, n-2$, where H is some positive constant. Then any complex zero α of $f(x)$ either has nonpositive real part, or satisfies

$$|\alpha| < \frac{1 + \sqrt{1+4H}}{2}$$

Proof. If $|z| > 1$ and $\operatorname{Re} z > 0$, we observe that

$$\begin{aligned}\left|\frac{f(z)}{z^n}\right| &\geq \left|a_n + \frac{a_{n-1}}{z}\right| - H\left(\frac{1}{|z|^2} + \cdots \frac{1}{|z|^n}\right) \\ &> \operatorname{Re}\left(a_n + \frac{a_{n-1}}{z}\right) - \frac{H}{|z|^2 - |z|} \\ &\geq 1 - \frac{H}{|z|^2 - |z|} = \frac{|z|^2 - |z| - H}{|z|^2 - |z|} \geq 0\end{aligned}$$

whenever

$$|z| \geq \frac{1 + \sqrt{1+4H}}{2}.$$

It follows that α cannot be a zero of f if $|\alpha| \geq \frac{1+\sqrt{1+4H}}{2}$ and $\operatorname{Re}\alpha > 0$. □

To prove Theorem 11 for the case $b \geq 3$, we notice that Lemma 2 implies if α is a zero of $f(x)$, then $|b - \alpha| > 1$. Suppose that $f(x) = g(x)h(x)$, where g and h are nonconstant integer polynomials. Since $f(b)$ is prime, one of $|g(b)|, |h(b)|$ is 1. Say $|g(b)| = 1$, and the zeros of g are $\alpha_1, \ldots, \alpha_k$. We have $|g(b)| = |b - \alpha_1| \cdots |b - \alpha_k| > 1$, contradiction. Therefore, f is irreducible.

The $b = 2$ case is special, and requires more analysis.

Lemma 3. Let $f(x) = x^n + a_{n-1}x^{n-2} + \cdots + a_1 x + a_0$ with $a_i \in \{0, 1\}$ for each i. Then all the zeros of f lie in the half plane $\operatorname{Re} z < \frac{3}{2}$.

Proof. The cases $n = 1$ and 2 can be verified by hand. Assume that $n \geq 3$. Then, for $z \neq 0$, we have

$$\left|\frac{f(z)}{z^n}\right| \geq \left|1 + \frac{a_{m-1}}{z} + \frac{a_{m-2}}{z^2}\right| - \left(\frac{1}{|z|^3} + \cdots + \frac{1}{|z|^m}\right) > \left|1 + \frac{a_{m-1}}{z} + \frac{a_{m-2}}{z^2}\right| - \frac{1}{|z|^2(|z|-1)}.$$

If z satisfies $|\arg z| \leq \pi/4$, then we have $\operatorname{Re}(1/z^2) \geq 0$, and we get

$$\left|\frac{f(z)}{z^n}\right| > 1 - \frac{1}{|z|^2(|z|-1)}.$$

If $|z| \geq \frac{3}{2}$, then $|z|^2(|z|-1) \geq \left(\frac{3}{2}\right)^2\left(\frac{3}{2} - 1\right) = \frac{9}{8} > 1$, and so $f(z) \neq 0$. On the other hand, if z is a zero of f with $|\arg z| > \pi/4$, and suppose that $\operatorname{Re} z > 0$, then from Lemma 2 we have $|z| < \frac{1+\sqrt{5}}{2}$, and thus $\operatorname{Re} z < \frac{1+\sqrt{5}}{2\sqrt{2}} < \frac{3}{2}$. It follows that all zeros of f lie in the half-plane $\operatorname{Re} z < \frac{3}{2}$. □

To finish off the proof, suppose that $f(x) = g(x)h(x)$, where g and h are integer polynomials. Since $f(2)$ is prime, one of $|g(2)|$, $|h(2)|$ is 1. Say $|g(2)| = 1$. By Lemma 3, all the zeros of f lie in the half plane $\operatorname{Re} z < \frac{3}{2}$, which means that they satisfy $|z - 2| > |z - 1|$. Thus, if $\alpha_1, \ldots, \alpha_k$ are the zeros of g, we have $|g(2)| = |2 - \alpha_1| \cdots |2 - \alpha_k| > |1 - \alpha_1| \cdots |1 - \alpha_k| = |g(1)| \geq 1$. So $|g(2)| > 1$, contradiction.

Problems

1. If q is a rational number and $\cos q\pi$ is also rational, show that $\cos q\pi \in \{0, \pm\frac{1}{2}, \pm 1\}$.

2. Let $P(x)$ be a monic polynomial with integer coefficients such that all its zeros lie on the unit circle. Show that all the zeros of $P(x)$ are roots of unity, i.e., $P(x)|(x^n - 1)^k$ for some $n, k \in \mathbb{N}$.

3. If $P(x)$ is a polynomial that such that $P(n)$ is an integer for every integer n, then show that

$$P(x) = c_n\binom{x}{n} + c_{n-1}\binom{x}{n-1} + \cdots + c_0\binom{x}{0},$$

for some integers $c_n, \ldots, c_0$. (Note that the coefficients of P are not necessarily integers.)

4. Let f be an irreducible polynomial in $\mathbb{Z}[x]$, show that f has no multiple roots.

5. Player A and B play the following game. Player A thinks of a polynomial, $P(x)$, with non-negative integer coefficients. Player B may pick a number a, and ask player A to return the value of $P(a)$, and then player B may choose another number b and ask player A to return the value of $P(b)$. After the two questions, player B must guess $P(x)$. Does player B have a winning strategy?

6. Determine all pairs of polynomials $f, g \in \mathbb{Z}[x]$, such that $f(g(x)) = x^{2007} + 2x + 1$.

7. (a) (USAMO 1974) Let a, b, c be three distinct integers, and let P be a polynomial with integer coefficients. Show that in this case the conditions $P(a) = b$, $P(b) = c$, $P(c) = a$ cannot be satisfied simultaneously.

   (b) Let $P(x)$ be a polynomial with integer coefficients, and let n be an odd positive integer. Suppose that $x_1, x_2, \ldots, x_n$ is a sequence of integers such that $x_2 = P(x_1), x_3 = P(x_2), \ldots, x_n = P(x_{n-1})$, and $x_1 = P(x_n)$. Prove that all the x_i's are equal.[2]

   (c) (Putnam 2000) Let $f(x)$ be a polynomial with integer coefficients. Define a sequence $a_0, a_1, \ldots$ 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 $a_2 = 0$.

   (d) (IMO 2006) Let $P(x)$ be a polynomial of degree $n > 1$ with integer coefficients and let k be a positive integer. Consider the polynomial

$$Q(x) = \underbrace{P(P(\ldots(P(x)\ldots))}_{k\ P's}$$

   Prove that there are at most n integers t such that $Q(t) = t$.

8. (IMO Shortlist 1997) 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 $c = 0, 1, \ldots, k+1$, then $F(0) = F(1) = \cdots = F(k+1)$.

9. Let $f(x) = x^4 + 6x^2 + 1$. Show that for any prime p, $f(x)$ is reducible over $\mathbb{F}_p$, but $f(x)$ is irreducible over $\mathbb{Z}$.

10. Let m, n, and a be positive integers and p a prime number less than $a - 1$. Prove that the polynomial $f(x) = x^m(x-a)^n + p$ is irreducible.

11. Let p be prime. Show that $f(x) = x^{p-1} + 2x^{p-2} + 3x^{p-3} + \cdots + (p-1)x + p$ is irreducible.

12. (IMO 1993) Let $f(x) = x^n + 5x^{n-1} + 3$, where $n > 1$ is an integer. Prove that $f(x)$ cannot be expressed as the product of two nonconstant polynomials with integer coefficients.

13. (Romania TST 2003) Let $f(x) \in \mathbb{Z}[x]$ be an irreducible monic polynomial with integer coefficients. Suppose that $|f(0)|$ is not a perfect square. Show that $f(x^2)$ is also irreducible.

[2] This problem appeared in Reid Barton's handout in 2005. Compare with the IMO 2006 problem.

14. Let $z_1, z_2, \ldots, z_n \in \mathbb{Z}[i]$ be Gaussian integers (i.e., complex numbers of the form $a+bi$, where $a, b \in \mathbb{Z}$) such that $|z_i - z_1| > 2$ for all $i > 1$. Prove that the polynomial $(x - z_1)(x - z_2)\cdots(x - z_n) + 1$ is irreducible over $\mathbb{Z}[i]$.

15. (Brazil 2006) Let $f(x)$ be an irreducible polynomial, and suppose that it has two roots whose product is 1. Show that the degree of f is even.

16. (MathLinks Contest) Let a be a nonzero integer, and $n \geq 3$ be another integer. Prove that the the following polynomial is irreducible over the integers:

$$P(x) = x^n + ax^{n-1} + ax^{n-2} + \cdots + ax - 1.$$

17. Let $a_1 \geq a_2 \geq \cdots \geq a_n > 0$ be positive integers. Show that the following polynomial is irreducible:

$$P(x) = x^n - a_1x^{n-1} - a_2x^{n-2} - \cdots - a_n$$

18. (MOP 2007) Let $p(x)$ be a polynomial with integer coefficients. Determine if there always exists a positive integer k such that $p(x) - k$ is irreducible.

19. (Iran TST 2007) Does there exist a sequence $a_0, a_1, a_2, \ldots$ in $\mathbb{N}$, such that for each $i \neq j, \gcd(a_i, a_j) = 1$, and for each n, the polynomial $\sum_{i=0}^{n} a_i x^i$ is irreducible in $\mathbb{Z}[x]$?

20. (China TST Quizzes 2006) Let n be a positive integer, and let $A_1, A_2, \ldots, A_k$ be a partition of the set of positive integers. Show that for some $i \in \{1, 2, \ldots, k\}$, there are infinitely many irreducible polynomials of degree n and whose coefficients are distinct elements from A_i.

21. Prove that $x^n - x - 1$ is irreducible over the integers for all $n \geq 2$.

22. (Iran 2003) Let $f_1, f_2, \ldots, f_n$ be polynomials with integer coefficients. Show that there exists a reducible polynomial $g(x) \in \mathbb{Z}[x]$ such that $f_i(x) + g(x)$ is irreducible for $i = 1, 2, \ldots, n$.

23. (IMO Shortlist 1997) Let f be a polynomial with integer coefficients and let p be a prime such that $f(0) = 0$, $f(1) = 1$, and $f(k) \equiv 0$ or $1 \pmod{p}$ for all positive integers k. Show that $\deg f \geq p - 1$.

24. (IMO Shortlist 2005) Find all monic integer polynomials $p(x)$ of degree two for which there exists an integer polynomial $q(x)$ such that $p(x)q(x)$ is a polynomial having all coefficients ± 1.

25. (IMO Shortlist 2005) 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.

26. (IMO 2002) Find all pairs of integers $m, n \geq 3$ such that there exist infinitely many positive integers a for which

$$\frac{a^m + a - 1}{a^n + a^2 - 1}$$

is an integer.

27. (IMO Shortlist 2002) Let $P(x)$ be a cubic polynomial with integer coefficients. Suppose that $xP(x) = yP(y)$ for infinitely many pairs x, y of integers with $x \neq y$. Prove that the equation $P(x) = 0$ has an integer root.

28. (IMO Shortlist 1996) For each positive integer n, show that there exists a positive integer k such that

$$k = f(x)(x + 1)^{2n} + g(x)(x^{2n} + 1)$$

for some polynomials f, g with integer coefficients, and find the smallest such k as a function of n.

29. (Romania TST 1998) show that for any $n \in \mathbb{N}$, the polynomial $P(x) = (x^2 + x)^{2^n} + 1$ is irreducible over the integers.