Irreducibility of Polynomials
Aditya Ghosh

Warm-up Problems

1. Suppose that $A(x) = \sum_{k=0}^{n} a_k x^k$, $B(x) = \sum_{k=0}^{m} b_k x^k$ and $C(x) = \sum_{k=0}^{n-m} c_k x^k$. If $A(x) = B(x)C(x)$ holds for all $x \in \mathbb{R}$ (or, for at least $n+1$ many $x \in \mathbb{R}$) then show that for each $0 \leq k \leq n$, we must have $a_k = \sum_{i+j=k} b_i c_j$, where the sum is over all integers $0 \leq i \leq m$ and $0 \leq j \leq n-m$ such that $i + j = k$.

2. Prove that a quadratic or cubic polynomial with integer coefficients having no rational root (e.g. $3x^2 - 15x - 11$ or $2x^3 - 4x + 1$) cannot be factorised into non-constant polynomials with integer coefficients.

3. Show that there do not exist two non-constant polynomials $p(x)$ and $q(x)$ each having integer coefficients such that $p(x)q(x) = x^5 + 2x + 1$. (Hint? See the footnote\(^1\).)

Playing with Roots & Degree

Our goal is to show that a given polynomial $f(x)$ cannot be factorised as a product of two non-constant polynomials with integer coefficients. We begin with the assumption that $f(x) = p(x)q(x)$. Then we use specific values of $x$ (may be zeros of $f$ or $p, q$) that eventually leads to a contradiction. We might construct a new polynomial (using $p, q$) which has more zeros than its degree, play with their coefficients, bound the modulus of a root, use triangle inequality etc.

Example. Suppose $n$ is an odd natural number and $a_1, \ldots, a_n$ are distinct integers. Show that the polynomial $f(x) = (x-a_1)(x-a_2) \cdots (x-a_n)+1$ cannot be factorised as the product of two non-constant polynomials with integer coefficients.

Solution. Let, if possible, $f(x) = p(x)q(x)$ where $p(x), q(x)$ are polynomials with integer coefficients. Putting $x = a_i$ in the equation $p(x)q(x) = (x-a_1)(x-a_2) \cdots (x-a_n)+1$, we get $p(a_i)q(a_i) = 1$. Since $p(a_i), q(a_i)$ are integers, this implies that $p(a_i) = q(a_i) = \pm 1$ for each $1 \leq i \leq n$. Now we play a little trick: we consider $h(x) = p(x) - q(x)$. We require $p(x)$ and $q(x)$ to be non-constant, which forces each of them to have degree $< n$. So $\deg h(x)$ is at most $n-1$. But we have $h(a_i) = 0$ for each $1 \leq i \leq n$ and the $a_i$’s are all distinct. Therefore

\(^1\)Hint: First show that none of $p$ or $q$ can be linear. Then compare coefficients.
10. Let \( a \)

11. Let \( a, b \)

12. Show that for \( n \) is even?

13. Find all pairs of integers \( a, b \) for which there exists a polynomial \( P(x) \in \mathbb{Z}[x] \) such that 

\( h \) has more roots than its degree, which is possible only when \( h \) is the zero polynomial. But then \( p(x) = q(x) \), which implies \((x - a_1) \cdots (x - a_n) + 1 = p(x)^2 \). Note that the RHS is a polynomial of even degree, whereas the degree of the LHS is odd, a contradiction. \( \square \)

**Notation.** We shall write \( p(x) \in \mathbb{Z}[x] \) to denote that \( p(x) \) is a polynomial with integer coefficients. If \( p(x) \) cannot be factorised as a product of two non-constant polynomials with integer coefficients, we say that \( p(x) \) is irreducible over \( \mathbb{Z}[x] \).

Now try out the following problems.

4. Does the conclusion of the above example hold if \( n \) is even?

5. Let \( n \) be any natural number and \( a_1, a_2, \ldots, a_n \) be distinct integers. Prove that the polynomial \( f(x) = (x - a_1)(x - a_2) \cdots (x - a_n) - 1 \) is irreducible over \( \mathbb{Z}[x] \).

6. Suppose \( p(x) \) is a polynomial of degree 2019 having integer coefficients satisfying \( p(a_i) \in \{-1, +1\} \) for 2019 distinct integers \( a_1, \ldots, a_{2019} \). Show that \( p(x) \) is irreducible over \( \mathbb{Z}[x] \).

7. Let \( a_1, \ldots, a_n \) be distinct integers. Show that \( f(x) = (x - a_1)^2(x - a_2)^2 \cdots (x - a_n)^2 + 1 \) is irreducible over \( \mathbb{Z}[x] \).

8. Show that the polynomial \( P(x) = x^n + 4 \) is irreducible over \( \mathbb{Z}[x] \) if and only if \( 4 \mid n \).

9. If \( \alpha \) is a root of the polynomial \( p(x) = a_0 + a_1x + \cdots + a_nx^n \) with real coefficients \( (a_n \neq 0) \), then show that \( |\alpha| \leq 1 + \max_{0 \leq k \leq n-1} \left| \frac{a_k}{a_n} \right| \).

10. Let \( a_0 + 10a_1 + \cdots + 10^na_n \) be the decimal representation of a prime number such that \( a_n \geq 2, n > 1 \). Prove that the polynomial \( p(x) = a_0 + a_1x + \cdots + a_nx^n \) cannot be written as a product of two non-constant polynomials with integer coefficients.

11. Let \( P(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \) be a polynomial with integer coefficients such that \( |a_0| \) is prime and \( |a_0| > |a_1| + |a_2| + \cdots + |a_n| \). Prove that \( P(x) \) is irreducible over \( \mathbb{Z}[x] \).

(Hint: If \( r \in \mathbb{C} \) is a zero of \( P(x) \) then show that \( |r| > 1 \). Assuming \( P(x) = Q(x)R(x) \), deduce that at least one among \( |Q(0)| \) and \( |R(0)| \) is 1. Now use Vieta’s formulae.)

12. Show that for \( n \geq 2 \), the polynomial \( x^n + x^{n-1} + 3 \) is irreducible in \( \mathbb{Z}[x] \).

13. Find all pairs of integers \( a, b \) for which there exists a polynomial \( P(x) \in \mathbb{Z}[x] \) such that product \( (x^2 + ax + b) \cdot P(x) \) is a polynomial of a form \( x^n + c_{n-1}x^{n-1} + \cdots + c_1x + c_0 \) where each of \( c_0, c_1, \ldots, c_{n-1} \) is equal to 1 or \(-1\).
Eisenstein’s Criterion

The following criterion allows us to prove irreducibility of polynomials of a certain kind.

**Theorem.** (Eisenstein’s Criterion) Let \( A(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \) be a polynomial with integer coefficients and \( p \) be a prime dividing \( a_0, a_1, \cdots, a_{n-1} \), such that \( p \nmid a_n \) and \( p^2 \nmid a_0 \). Then \( A(x) \) is irreducible over \( \mathbb{Z}[x] \).

**Proof.** Let, if possible, \( A(x) = B(x)C(x) \) for some non-constant polynomials \( B(x), C(x) \) with integer coefficients. Suppose that \( B(x) = \sum_{k=0}^{m} b_k x^k \) and \( C(x) = \sum_{k=0}^{n-m} c_k x^k \). Since \( A(x) = B(x)C(x) \) holds for all \( x \in \mathbb{R} \), it must hold for each \( 0 \leq k \leq n \) that \( a_k = \sum_{i+j=k} b_i c_j \), where the sum is over all integers \( 0 \leq i \leq m \) and \( 0 \leq j \leq n-m \) such that \( i + j = k \). Let us start with \( a_0 = b_0c_0 \). Since \( p \mid a_0 \) but \( p^2 \nmid a_0 \), we can say that exactly one among \( b_0 \) and \( c_0 \) is divisible by \( p \). W.l.o.g assume that \( p \mid b_0 \) and \( p \nmid c_0 \). Next, \( a_1 = b_0c_1 + b_1c_0 \). Since \( p \mid a_1, p \mid b_0 \) but \( p \nmid c_0 \), we get \( p \mid b_1 \). What does the next relation \( a_2 = b_0c_2 + b_1c_1 + b_2c_0 \) give? It gives \( p \mid b_2 \). Continuing in this manner, we eventually get from \( a_m = b_0c_m + \cdots + b_mc_0 \) that \( p \mid b_m \). (Note that here we have \( p \mid a_m \) because \( m < n \).) But now that we have shown \( p \mid b_i \) for each \( i \), we can see that \( a_n = \sum_{i+j=n} b_i c_j \) implies \( p \mid a_n \), which is a contradiction. \( \square \)

The proof was straightforward. Let us now look at a few examples.

**Example.** Consider the polynomial \( P(x) = 3x^4 + 15x^2 + 10 \). In order for Eisenstein’s criterion to apply for a prime number \( p \) it must divide both non-leading coefficients 15 and 10, which means only \( p = 5 \) could work, and indeed it does since 5 does not divide the leading coefficient 3, and its square 25 does not divide the constant coefficient 10. We therefore conclude that \( P(x) \) is irreducible over \( \mathbb{Z}[x] \).

**Example.** Consider \( P(x) = 3x^9 + 18x^3 - 60x + 6 \). Here \( p = 3 \) won’t do, because it divides the leading coefficient. However, \( p = 2 \) does the job. Eisenstein’s criterion with \( p = 2 \) tells us that \( P(x) \) must be irreducible over \( \mathbb{Z}[x] \).

Try to do the following problems now.

14. Show that the polynomial \( f(x) = (2^5 - 1) + (2^{10} - 1)x^2 + (2^{15} - 1)x^3 + (2^{18} - 1)x^4 \) is irreducible over \( \mathbb{Z}[x] \).

15. Show that for any positive integer \( n \), there are infinitely many irreducible polynomial of degree \( n \) having integer coefficients.
Often Eisenstein’s criterion does not apply directly, but it applies (for some prime number) to the polynomial obtained after substituting \(x + a\) for \(x\) (for some integer \(a\)). The fact that the polynomial after the substitution is irreducible then allows us to conclude that the original polynomial is irreducible as well. This idea is known as applying a shift.

**Trick 1.** If \(f(x) \in \mathbb{Z}[x]\) is irreducible over \(\mathbb{Z}[x]\), then so is the polynomial \(f(x + a)\) for any \(a \in \mathbb{Z}\).

**Proof.** If \(f(x + a)\) can be factorised as \(p(x)q(x)\), then \(f(x)\) can be written as \(p(x - a)q(x - a)\). And if a polynomial \(p(x)\) has integer coefficients then so does \(p(x - a)\). □

**Example.** Consider \(P(x) = x^3 - 3x^2 + 5\). Note that Eisenstein’s criterion does not apply directly to \(P\). But if one substitutes \(x + 1\) for \(x\) in \(P\), one obtains the polynomial \(Q(x) = P(x + 1) = (x + 1)^3 - 3(x + 1)^2 + 5 = x^3 - 3x + 3\) which satisfies Eisenstein’s criterion for the prime number 3. Thus \(Q(x)\) is irreducible over \(\mathbb{Z}[x]\), which proves that \(P(x)\) must also be irreducible.

Another possibility to transform a polynomial so as to satisfy the criterion (which may be combined with applying a shift), is reversing the order of its coefficients, provided its constant term is nonzero (without which it would be divisible by \(x\) anyway).

**Trick 2.** Suppose that \(a_0, \ldots, a_n \in \mathbb{Z}\) such that \(f(x) = \sum_{k=0}^{n} a_k x^k\) is irreducible over \(\mathbb{Z}[x]\). Then the polynomial \(\hat{f}(x) = \sum_{k=0}^{n} a_{n-k} x^k\), obtained by reversing the coefficients of \(f(x)\), must also be irreducible.

**Proof.** Observe that \(\hat{f}(1/x) = f(x)/x^n\). Let, if possible, \(\hat{f}(x)\) be factorised as \(p(x)q(x)\). Suppose \(\deg p(x) = k\) and \(\deg q(x) = m\). Clearly, \(k + m = \deg f(x) = n\). Then,

\[
f(x) = x^n \hat{f}(1/x) = x^n p(1/x)q(1/x) = x^k p(1/x) \cdot x^m q(1/x) \text{ for every } x \neq 0.
\]

Since \(p(x), q(x)\) are integer polynomials, so are \(x^k p(1/x)\) and \(x^m q(1/x)\) (their coefficients are same as \(p\) and \(q\), just in reverse order). Thus \(f\) becomes reducible if \(\hat{f}\) is so. □

**Example.** The polynomial \(2x^5 - 4x^2 - 3\) satisfies the criterion for \(p = 2\) after reversing its coefficients, and is therefore irreducible in \(\mathbb{Z}[x]\).
**Example.** Consider the polynomial \( p(x) = 4x^3 + 12x^2 + 3x + 1 \). Note that \( p(x) \) satisfies the requirements of Eisenstein’s criterion neither directly, nor after reversing its coefficients. So we try some shift. First we check \( p(x + 1) \), which simplifies to \( 4x^3 + 24x^2 + 39x + 20 \). Since this does not work, we try with \( p(x - 1) \). Note that 
\[ p(x - 1) = 4x^3 - 9x + 6. \]
Although this does not meet the requirements directly, it does so after reversing the coefficients (with \( p = 3 \)). Hence we conclude that \( p(x) \) is irreducible over \( \mathbb{Z}[x] \).

16. Show that the polynomial \( f(x) = x^4 - 4ax^2 + 1 \) is irreducible over \( \mathbb{Z}[x] \) for any \( a \in \mathbb{Z} \).

17. Suppose \( p \) is a prime number. Show that the polynomial \( 1 + x + x^2 + \cdots + x^{p-1} \) is irreducible over \( \mathbb{Z}[x] \).

18. Prove that \( p(x) = x^4 + x^3 - 3x^2 - 5x + 1 \) is irreducible over \( \mathbb{Z}[x] \).

19. Prove that \( q(x) = 3x^5 - 9x^3 - 2016x + 2018 \) is irreducible over \( \mathbb{Z}[x] \).

20. Show that \( f(x) = 20x^4 - 2018x^3 + 6x^2 - 4x + 1 \) is irreducible over \( \mathbb{Z}[x] \).

21. (Extended Eisenstein’s Criterion) Let \( a_0, a_1, \ldots, a_n \) be integers and \( p \) be a prime such that \( p \) divides each of \( a_0, a_1, a_2, \ldots, a_k \), but \( p \nmid a_{k+1} \) and \( p^2 \nmid a_0 \). Show that the polynomial 
\[ f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \]
has an irreducible factor of degree more than \( k \). That is, if \( f(x) = g(x)h(x) \) then at least one among \( g(x) \) and \( h(x) \) has degree \( \geq k \).

22. For an integer \( n > 1 \), show that \( f(x) = x^n + 5x^{n-1} + 3 \) is irreducible over \( \mathbb{Z}[x] \).

### Rational Coefficients

23. Suppose that \( f(x) \) is a polynomial with rational coefficients. Show that there exists a polynomial \( \tilde{f}(x) \) with integer coefficients such that \( f(x) = \frac{c}{d} \cdot \tilde{f}(x) \) where \( c, d \) are coprime integers and gcd of the coefficients of \( \tilde{f}(x) \) is 1.

24. We call a polynomial \( f(x) \) having integer coefficients to be primitive if the gcd of the coefficients of \( f(x) \) is 1. Show that product of two primitive polynomials is also a primitive polynomial.

25. (Gauss’ Lemma) Suppose \( f(x) \) is a polynomial with integer coefficients. Show that \( f(x) \) is irreducible over \( \mathbb{Z}[x] \) if and only if \( f(x) \) is irreducible over \( \mathbb{Q}[x] \), i.e. \( f(x) \) cannot be factorised into non-constant polynomials with rational coefficients.
Hints for the Problems

3. Since \( f \) does not have any rational root, neither of \( p \) or \( q \) can be linear. Assume w.l.o.g that \( p \) is quadratic and \( q \) is cubic. Note that \( p \) and \( q \) may be written (by taking \(-p\) and \(-q\) if needed) as \((x^2 + bx + c)\) and \((x^3 + mx^2 + nx + k)\) respectively. Now compare coefficients to get \( ck = 1 \), \( cn + kb = 2 \), \( k + nb + m = 0 \), \( c + mb + n = 0 \), \( b + m = 0 \). Show that this set of equations has no solution for integers \( c, k, b, m, n \).

4. No. For instance, \((x - 3)(x - 5) + 1 = (x - 4)^2\).

5. Use same idea as in the example preceding it.

6. Suppose that \( p(x) = u(x)v(x) \). Then one of these factors, say \( u(x) \) has degree 1009 or less. Since \( p(a_i) = \pm 1 \) for the 2019 different integers \( a_1, \ldots, a_{2019} \), this forces \( u(a_i) = \pm 1 \) as well. But then for at least 1010 of these \( a_i \), we must have \( u(a_i) \) equaling only one value, say \(-1\). This forces \( u(x) \) to be the constant polynomial \(-1\), contradicting the fact that it is a non-constant polynomial.

7. Let, if possible, \( f(x) = p(x)q(x) \). We must have \( p(a_i) = q(a_i) = \pm 1 \) for each \( 1 \leq i \leq n \). If \( p(a_i) = 1 \) and \( p(a_j) = -1 \) then there exists \( c \) between \( a_i \) and \( a_j \) such that \( p(c) = 0 \). But this is not possible since \( p(c)q(c) = f(c) \geq 1 \). Thus we conclude that all the \( p(a_i) \)'s are equal and same for the \( q(a_i) \)'s. We may assume w.l.o.g that \( p(a_i) = q(a_i) = 1 \) for all \( 1 \leq i \leq n \). Now if any one among \( p \) and \( q \), say \( p \), had degree less than \( n \) then this would imply that \( p \) must be the zero polynomial. But this is not possible, again because \( f(x) \geq 1 \) for all \( x \in \mathbb{R} \). Therefore we conclude that both \( p \) and \( q \) must have degree \( n \). And note that \( p(x)q(x) = (x - a_1)^2 \cdots (x - a_n)^2 + 1 \) implies that the leading coefficients of \( p, q \) must be the same. Hence by considering the polynomial \( p(x) - q(x) \)
we can show that $p(x)$ and $q(x)$ must be identical. Then the equation $f(x) = p(x)^2$ can be written as $((x - a_1) \cdots (x - a_n) - p(x))((x - a_1) \cdots (x - a_n) + p(x)) = 1$. Now the leading coefficients of both the factors above must be zero. If the leading coefficient of $p(x)$ be $s$ then we need $1 - s = 0$ as well as $1 + s = 0$, which is not possible.

8. All zeros of polynomial $P$ have the modulus equal to $2^{2/n}$. If $Q$ and $R$ are polynomials from $\mathbb{Z}[x]$ and $\deg Q = k$, then $|Q(0)|$ is the product of the moduli of $k$ zeros of $P$ and hence equals $2^{2k/n}$. Since this should be an integer, deduce that $n = 2k$. Finally note that if $k$ is odd, polynomial $Q(x)$ has a real zero, but $P(x)$ has none.

9. Note that the bound is trivial if $|\alpha| = 0$ or $1$. Assume now that $|\alpha| \neq 0, 1$. It is given that $\sum_{k=0}^{n} a_k \alpha^k = 0$. We transfer the term $a_n \alpha^n$ to the RHS and use triangle inequality to obtain

$$|a_n \alpha^n| = \left| \sum_{k=0}^{n-1} a_k \alpha^k \right| \leq \sum_{k=0}^{n-1} |a_k||\alpha|^k \leq \max_{0 \leq k \leq n-1} |a_k| \left( \sum_{k=0}^{n-1} |\alpha|^k \right) = \max_{0 \leq k \leq n-1} |a_k| \left( \frac{|\alpha|^n - 1}{|\alpha| - 1} \right).$$

The second inequality above comes from the fact that each $|a_i|$ is less than $\max_{0 \leq k \leq n-1} |a_k|$. Now just cross-multiply to arrive at

$$|\alpha| - 1 \leq \max_{0 \leq k \leq n-1} \left| \frac{a_k}{a_n} \right| \left( \frac{|\alpha|^n - 1}{|\alpha| - 1} \right) \leq \max_{0 \leq k \leq n-1} \left| \frac{a_k}{a_n} \right|.$$

10. Let, if possible, $q(x)$ and $r(x)$ be non-constant polynomials with integer coefficients such that $p(x) = q(x)r(x)$. Let $x_1, \ldots, x_k$ be the zeros of $q(x)$ and $x_{k+1}, \ldots, x_n$ be the zeros of $r(x)$. Since $q(10)r(10) = p(10)$ which is a prime, and $q(10), r(10)$ both are integers, one of them must be $\pm 1$. We can assume w.l.o.g that $q(10) = \pm 1$. Then $|q(10)| = |(10 - x_1)(10 - x_2) \cdots (10 - x_k)| = 1$. On the other hand, the inequality in the last problem tells us that each zero $x_i$ has a modulus less than $1 + 9/2 = 11/2 < 9$, hence $|10 - x_i| > 1$ for each $1 \leq i \leq k$, which contradicts the above equality.

11. Some hints are already given. You may proceed as in problem 9. For full solution, consult Zhao’s note (cited in the references section above).

12. Use the previous problem.

13. The answer is the following: $a = \pm 1$ and $b = \pm 1$, in this case take $P(x) \equiv 1$; $a = 0$ and $b = \pm 1$, in this case take $P(x) \equiv x + 1$; $a = \pm 2$ and $b = 1$; in this case take $P(x) \equiv x - 1$. 

7
The main idea is: any root $z$ of $x^2 + ax + b$ satisfies $|z| \leq 2$.

(Proof. Since $z$ is a root of $(x^2 + ax + b) \cdot P(x)$, we have $|z|^n = \left| \sum_{k=0}^{n-1} c_k z^k \right| \leq \sum_{k=0}^{n-1} |z|^k$ with the last inequality be triangle inequality. So if $|z| \geq 2$, then we get a contradiction.)

Next show that $b = \pm 1$. Now if $|a| \geq 3$, the roots of $x^2 + ax \pm 1$ are $\frac{1}{2}(|a| + \sqrt{|a|^2 \pm 4})$ and one of these is greater than 2. The same is true for $|a| = 2$ and $b = -1$. Thus there are no answers other than the ones we claimed.

14. Use Eisenstein’s criterion.

15. For any prime $p$, the polynomial $x^n + p$ is irreducible.

16. Replace $x$ by $x + 1$.

17. Replace $x$ by $x + 1$.

18. Replace $x$ by $x - 1$.

19. Reverse the coefficients.

20. Reverse the coefficients and then change $x$ to $x + 1$.

21. Mimic the proof of Eisenstein’s criterion.

22. Use the previous problem.

23. Take the lcm of the denominators and then extract out the gcd from the numerator.

24. Use an argument similar to the proof of Eisenstein’s criterion.

25. Let, if possible, $f$ be irreducible over $\mathbb{Z}[x]$ but reducible over $\mathbb{Q}[x]$. Suppose that $f(x) = p(x)q(x)$ where $p, q$ are polynomials having rational coefficients. Use problem 23 to write $f(x) = (a/b)\tilde{p}(x)\tilde{q}(x)$ where $\tilde{p}, \tilde{q}$ are primitive. Now by problem 24, the polynomial $\tilde{p}(x)\tilde{q}(x)$ must also be primitive. Hence deduce from $bf(x) = a\tilde{p}(x)\tilde{q}(x)$ that $b = \pm 1$, which in turn implies that $f$ is reducible (contradiction).