Irreducibility

MOPSS

Mathematics Olympiad

Problem Solving Sessions

Department of Mathematics
IISER Bhopal

https://jpsaha.github.io/MOTP/MOPSS/

Suggested readings

- Evan Chen's advice On reading solutions, available at https://blog.evanchen.cc/2017/03/06/on-reading-solutions/.
- Evan Chen's Advice for writing proofs/Remarks on English, available at https://web.evanchen.cc/handouts/english/english.pdf.
- Notes on proofs by Evan Chen from OTIS Excerpts [**Che25**, Chapter 1].
- Tips for writing up solutions by Edward Barbeau, available at https://www.math.utoronto.ca/barbeau/writingup.pdf.
- Evan Chen discusses why math olympiads are a valuable experience for high schoolers in the post on Lessons from math olympiads, available at https://blog.evanchen.cc/2018/01/05/lessons-from-math-olympiads/.

List of problems and examples

1.1 Example 2
1.2 Example 3
1.3 Example 4
1.4 Example 6
1.5 Example 7
1.6 Example 7
1.7 Example 7

§1 Irreducibility

Example 1.1. [**WH96**, Problem 27] Let $p_1, \ldots, p_n$ denote $n \geq 1$ distinct integers. Show that the polynomial

$$(x - p_1)^2 (x - p_2)^2 \cdots (x - p_n)^2 + 1$$

cannot be expressed as the product of two non-constant polynomials with integral coefficients.

Solution 1. On the contrary, let us assume that the polynomial

$$P(x) := (x - p_1)^2 (x - p_2)^2 \cdots (x - p_n)^2 + 1$$

can be expressed as the product of two non-constant polynomials $f(x), g(x)$ with integral coefficients.

Let us first establish the following Claims.

> **Claim** — Replacing f, g by $-f, -g$ respectively (if necessary), we may assume that f, g take positive values at all real arguments.

Proof of the Claim. Note that the polynomial $P(x)-1$ vanishes at $x = p_1, \ldots, p_n$. Since the product of the leading coefficients of $f(x)$ and $g(x)$ is equal to the leading coefficient of $P(x)$, we may replace $f(x), g(x)$ by $-f(x), -g(x)$ respectively (if necessary) to assume that the leading coefficients of $f(x), g(x)$ are positive. Since $P = fg$ and P does not have a real root, it follows that the polynomials f, g do not have any real roots. At large enough real arguments, the polynomials f, g take positive values. Since f, g have no real roots, we conclude that they take positive values at all real arguments. □

> **Claim** — The polynomials f, g are of degree n. Moreover, these polynomials are equal.

Proof of the Claim. On the contrary, let us asssume that the degrees of f, g are not equal. Interchanging f, g if necessary, we assume that $\deg(f) < \deg(g)$. Since the sum of the degrees of f, g is equal to $2n$, it follows that $\deg(f) < n$.

For any $1 \leq i \leq n$, the integers $f(p_i), g(p_i)$ are equal to 1 or -1. Since f, g take positive values at all real arguments, we obtain $f(p_i) = 1$ for any $1 \leq i \leq n$. This shows that the polynomial $f - 1$ has at least n distinct roots. Using $\deg(f) < n$, we conclude that $f - 1$ is the zero polynomial, which is impossible since f is a non-constant polynomial. Therefore, the hyothesis that the degrees of f, g are not equal is not tenable. This completes the proof of the first part of the Claim.

Note that f, g are polynomials of degree n with equal leading coefficients. This shows that the polynomial $f(x) - g(x)$ has degree less than n and it vanishes at the n distinct points $p_1, \dots, p_n$. It follows that $f = g$.

□

Using the above Claim, note that

$$f(x)^2 - ((x - p_1)(x - p_2)\cdots(x - p_n))^2 = 1,$$

or equivalently,

$$\big(f(x) + (x - p_1)(x - p_2)\cdots(x - p_n)\big)\big(f(x) - (x - p_1)(x - p_2)\cdots(x - p_n)\big) \\ = 1,$$

which implies that the polynomials

$$f(x) + (x - p_1)(x - p_2)\cdots(x - p_n), f(x) - (x - p_1)(x - p_2)\cdots(x - p_n)$$

are constant polynomials, and both of them are equal. Consequently, the polynomial $(x-p_1)(x-p_2)\cdots(x-p_n)$ is the zero polynomial, which is impossible. This shows that the hypothesis that the given polynomial can be expressed as the product of two non-constant polynomials with integral coefficients is not tenable. This completes the proof. ■

Example 1.2. Let n be a positive integer. Show that the polynomial

$$(x - 1)(x - 2)\cdots(x - n) - 1$$

is irreducible over the field of rational numbers.

Solution 2. Note that the given polynomial is irreducible if $n = 1$. It suffices to consider the case $n \geq 2$. On the contrary, let us assume that the polynomial is reducible over the rationals. Then, by Gauss's lemma, it is also reducible over the integers. Thus, there exist non-constant polynomials $f(x), g(x)$ with integer coefficients such that

$$(x - 1)(x - 2)\cdots(x - n) - 1 = f(x)g(x).$$

Note that for any integer $1 \leq k \leq n$, we have

$$f(k)g(k) = -1.$$

This implies that both $f(k)$ and $g(k)$ are non-zero integers whose product is equal to -1. Hence, for any integer $1 \leq k \leq n$, the pair $(f(k), g(k))$ is either $(-1, 1)$ or $(1, -1)$. This shows that the polynomial $f(x) + g(x)$, which has degree less than n, has at least n distinct roots. Hence, $f(x) + g(x)$ is the zero polynomial, which yields

$$(x-1)(x-2)\cdots(x-n) - 1 = f(x)g(x) = -f(x)^2.$$

This is a contradiction since the leading coefficient of the polynomial on the left-hand side is positive. This completes the proof. ■

Example 1.3. Let n be a positive integer with $n \neq 4$. Show that the polynomial

$$(x-1)(x-2)\cdots(x-n) + 1$$

is irreducible over the field of rational numbers.

Solution 3. Note that the given polynomial is irreducible if $n = 1$. If $n = 2$, then the given polynomial is equal to

$$x^2 - 3x + 3,$$

which has no rational root, and hence is irreducible over the rationals. It suffices to consider the case $n \geq 3$ with $n \neq 4$. On the contrary, let us assume that the given polynomial is reducible over the rationals. Then, by Gauss's lemma, it is also reducible over the integers. Thus, there exist non-constant polynomials $f(x), g(x)$ with integer coefficients such that

$$(x-1)(x-2)\cdots(x-n) + 1 = f(x)g(x).$$

Note that for any integer $1 \leq k \leq n$, we have

$$f(k)g(k) = 1.$$

This shows that the polynomial $f(x) - g(x)$, which has degree less than n, has at least n distinct roots. Hence, $f(x) - g(x)$ is the zero polynomial, which yields

$$(x-1)(x-2)\cdots(x-n) + 1 = f(x)g(x) = f(x)^2.$$

This implies that n is an even positive integer. Since $n \neq 4$, it follows that $n \geq 6$. Note that

$$f\left(n - \frac{1}{2}\right)^2$$

$$
\begin{aligned}
&= \left(n - \frac{1}{2} - 1\right)\left(n - \frac{1}{2} - 2\right)\cdots\left(n - \frac{1}{2} - (n-1)\right)\left(n - \frac{1}{2} - n\right) + 1 \\
&= -\frac{1}{2}\left(1 - \frac{1}{2}\right)\left(2 - \frac{1}{2}\right)\cdots\left((n-1) - \frac{1}{2}\right) + 1 \\
&< 1 - \frac{1}{4}\left(2 - \frac{1}{2}\right)\cdots\left((n-1) - \frac{1}{2}\right) \\
&\leq 1 - \frac{1}{4}\left(2 - \frac{1}{2}\right)\left(3 - \frac{1}{2}\right)\left(4 - \frac{1}{2}\right) \qquad \text{(since } n \geq 6\text{)} \\
&= 1 - \frac{3 \cdot 5 \cdot 7}{32} \\
&< 0,
\end{aligned}
$$

which is impossible. This shows that the given polynomial is irreducible over the rationals. ■

Remark. After obtaining

$$(x-1)(x-2)\cdots(x-n) + 1 = (f(x))^2,$$

one can also argue as follows to complete the proof. Note that n is an even positive integer. For $i \in \{1, -1\}$, let

$$S_i = \{k \in \{1, 2, \ldots, n\} : f(k) = i\}.$$

Note that both S_1 and S_{-1} are disjoint subsets of $\{1, 2, \ldots, n\}$ whose union is equal to $\{1, 2, \ldots, n\}$. Moreover, each of the sets S_1 and S_{-1} contain at most $\frac{n}{2}$ elements since $f(x)$ is a non-constant polynomial. This shows that both S_1 and S_{-1} contain exactly $\frac{n}{2}$ elements.

Note that some element of one of the sets S_1, S_{-1} differs from some element of the other set at least by 3. Indeed, if S_i contains 1, then using that S_i contains $\frac{n}{2}$ elements and

$$1 + (n-3) > \frac{n}{2}$$

holds for $n \geq 6$, it follows that S_{-i} must contain an element greater than or equal to 4. This shows that there exist elements $a \in S_1$ and $b \in S_{-1}$ such that $|a - b| \geq 3$. This yields

$$f(a) - f(b) = 2$$

is divisible by $|a - b|$, which is impossible.

Remark. Note that

$$(x-1)(x-2)(x-3)(x-4)+1 = (x^2-5x+4)(x^2-5x+6)+1 = (x^2-5x+5)^2,$$

which is reducible over the rationals.

Example 1.4. Let p be an odd prime number. Show that the polynomial

$$P(x) = x^p - x + p$$

is irreducible over the field of rational numbers.

Solution 4. On the contrary, let us assume that the polynomial $P(x)$ is reducible over the rationals. Then, by Gauss's lemma, it is also reducible over the integers. Thus, there exist non-constant polynomials $f(x), g(x) \in \mathbb{Z}[x]$ such that

$$P(x) = f(x)g(x).$$

Since the leading coefficient of $P(x)$ is 1, by multiplying $f(x), g(x)$ by -1 if necessary, we may assume that both $f(x)$ and $g(x)$ are monic polynomials. Since p is a prime number, by reordering $f(x), g(x)$ if necessary, we may assume that $|f(0)| = p$. Let $\alpha_1, \ldots, \alpha_k$ denote the roots of $f(x)$ over the complex numbers (counted with multiplicities). Since f is a monic polynomials, by Viete's formulas, we have

$$|\alpha_1 \cdots \alpha_k| = |f(0)| = p.$$

In particular, at least one of the roots, say α, satisfies

$$|\alpha| \geq p^{1/k}.$$

Since $P(\alpha) = 0$, we have

$$\alpha^p - \alpha + p = 0,$$

which implies

$$p \geq |\alpha|^p - |\alpha| = |\alpha|(|\alpha|^{p-1} - 1) \geq p^{1/k}(p^{(p-1)/k} - 1) \geq p^{1/(p-1)}(p-1).$$

This shows that

$$p^{1/(p-1)} \leq 1 + \frac{1}{p-1},$$

which gives

$$p \leq \left(1 + \frac{1}{p-1}\right)^{p-1} < 3.$$

Since p is a prime number, we have $p = 2$. This is a contradiction since p is odd. This completes the proof. ■

Theorem 1 (Eisenstein's criterion)
Let
$$f(x) = a_n x^n + \cdots + a_1 + a_0$$
be a polynomial with integer coefficients. Let p be a prime number and assume that
$$\begin{aligned} a_n &\not\equiv 0 \bmod p, \\ a_{n-1}, \dots, a_0 &\equiv 0 \bmod p, \\ a_0 &\not\equiv 0 \bmod p^2 \end{aligned}$$
holds. Then $f(x)$ cannot be expressed as a product of two non-constant polynomials with rational coefficients.

Example 1.5. [Art91, Chapter 11, Exercise 4.10, p. 444] Let
$$f(x) = a_{2n+1}x^{2n+1} + a_{2n}x^{2n} + \cdots + a_1 x + a_0$$
be a polynomial of degree $2n+1$ with integer coefficients. Let p be a prime number and assume that
$$\begin{aligned} a_{2n+1} &\not\equiv 0 \bmod p, \\ a_0, a_1, \dots, a_n &\equiv 0 \bmod p^2, \\ a_{n+1}, \dots, a_{2n} &\equiv 0 \bmod p, \\ a_0 &\not\equiv 0 \bmod p^3. \end{aligned}$$
Show that $f(x)$ cannot be expressed as a product of two non-constant polynomials with rational coefficients.

Example 1.6. For any prime p, show that there exist non-constant monic polynomials $f_p(x), g_p(x)$ with integer coefficients such that
$$x^4 - 10x^2 + 1 \equiv f_p(x) g_p(x) \bmod p$$
holds. Can the polynomial $x^4 - 10x^2 + 1$ be expressed as the product of two non-constant polynomials with rational coefficients?

Example 1.7. Prove that the polynomial $x^n + 4$ is irreducible over $\mathbb{Z}[x]$ if and only if n is not a multiple of 4.

Solution 5. If n is a multiple of 4, then we can write $n = 4k$ for some positive integer k. In this case, we have
$$x^n + 4 = x^{4k} + 4 = (x^{2k} - 2x^k + 2)(x^{2k} + 2x^k + 2),$$

which shows that $x^n + 4$ is reducible over $\mathbb{Z}[x]$.

Now, suppose that n is not a multiple of 4. We will show that $x^n + 4$ is irreducible over $\mathbb{Z}[x]$. Assume for the sake of contradiction that $x^n + 4$ is reducible over $\mathbb{Z}[x]$. Then we can write

$$x^n + 4 = f(x)g(x),$$

where $f(x), g(x) \in \mathbb{Z}[x]$ are non-constant polynomials with degrees less than n. Since the roots of $x^n + 4$ in $\mathbb{C}$ are of absolute value $4^{1/n}$, the roots of $f(x)$ are also of absolute value $4^{1/n}$. Let the degree of $f(x)$ be d. The absolute value of the constant term of $f(x)$ is then $(4^{1/n})^d = 2^{2d/n}$. Since the constant term of $f(x)$ is an integer, it follows that n divides $2d$. Since $d < n$, we must have that $n = 2d$. Since n is not a multiple of 4, it follows that d is odd. Thus, $f(x)$ is a monic polynomial of odd degree with integer coefficients. Hence, it has a real root, implying that $x^n + 4$ has a real root, which is impossible since n is even. This shows that $x^n + 4$ is irreducible over $\mathbb{Z}[x]$.

This completes the proof. ∎

References

[**Art91**] Michael Artin. *Algebra*. Englewood Cliffs, NJ: Prentice Hall Inc., 1991, pp. xviii+618. isbn: 0-13-004763-5 (cited p. 7)

[**Che25**] Evan Chen. *The OTIS Excerpts*. Available at https://web.evanchen.cc/excerpts.html. 2025, pp. vi+289 (cited p. 1)

[**WH96**] Kenneth S. Williams and Kenneth Hardy. *The Red Book of mathematical problems*. Corrected reprint of the ıt The Red Book: 100 practice problems for undergraduate mathematics competitions [Integer Press, Ottawa, ON, 1988]. Dover Publications, Inc., Mineola, NY, 1996, pp. x+174. isbn: 0-486-69415-1 (cited p. 2)