Supplementary material for Eisenstein criterion

Theorem (Eisenstein) Let $a_0, a_1, \ldots, a_n$ be integers. **Eisenstein's Criterion** states that the polynomial

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

cannot be factored into the product of two non-constant polynomials if:

1. p is a prime that divides each of $a_0, a_1, \ldots, a_{n-1}$;

2. a_n is not divisible by p;

3. a_0 is not divisible by p^2.

Problem (Optional) Prove Eisenstein's Criterion.

Problem (Optional) Show that there are irreducible polynomials which Eisenstein's criterion cannot detect. More precisely, find an irreducible polynomial $f(x)$ for which Eisenstein's criterion fails for all primes p, and for all shifts $f(x-a)$.

Example (A very important example you may encounter in future) We shall use Eisenstein's Criterion to prove that $f(x,y,z) = x^2 + y^2 + z^2$ is irreducible over $\mathbb{C}[x,y,z]$.

> Consider the (UFD) ring $\mathbb{A} = \mathbb{C}[y,z]$ and the expression
>
> $$x^2 + (y+iz)(y-iz) \in \mathbb{A}[x].$$
>
> Since:
>
> 1. $(y+iz)$ is prime in $\mathbb{A}$ and divides $a_1 = 0$;
>
> 2. $a_n = 1$ is not divisible by $(y+iz)$;
>
> 3. $a_0 = y^2 + z^2$ is not divisible by $(y+iz)^2$,
>
> we conclude that f is irreducible over $\mathbb{C}[x,y,z]$.

Theorem (Eisenstein, extended) Let $a_0, a_1, \ldots, a_n$ be integers. **Extended Eisenstein's Criterion** states that

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

has an irreducible factor with $\deg > k$ if:

1. p is a prime that divides each of $a_0, a_1, \ldots, a_k$;

2. a_{k+1} is not divisible by p;

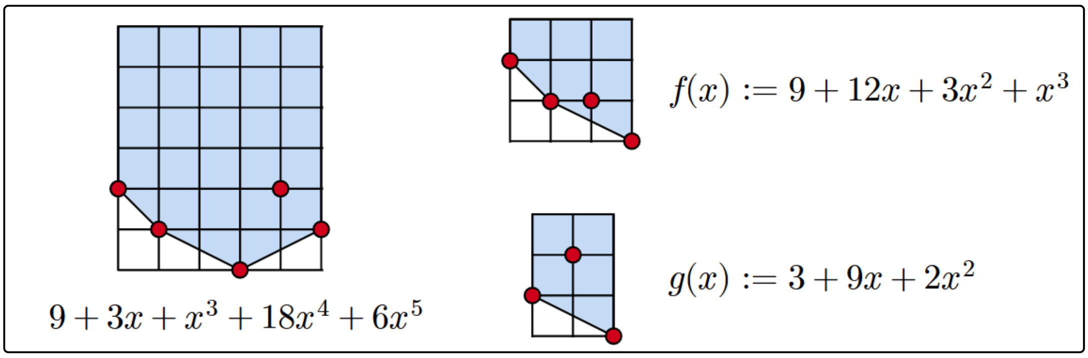
3. a_0 is not divisible by p^2.

Problem (Optional) Prove Extended Eisenstein's Criterion.

Example (IMO 1993) Given an integer $n \geq 1$, consider the polynomial $f(x) = x^n + 5x^{n-1} + 3$. Show that f is irreducible in $\mathbb{Z}[x]$.

> Taking $p = 3$ and $k = n-2$ in Extended Eisenstein's Criterion, we see that f has some irreducible factor g with $\deg g > (n-2)$.
>
> We are done when $\deg g = n$.
>
> When $\deg g = n-1$, there exists some $d \in \mathbb{Z}$ such that $(x-d) \cdot g(x) = f(x)$. We learn from middle school that $d \in \{\pm 1, \pm 3\}$. As a result, $f(d)$ is an odd number (absurd).

Definition I call it $\bmod 3$-convex hull of polynomials, guess what it means?



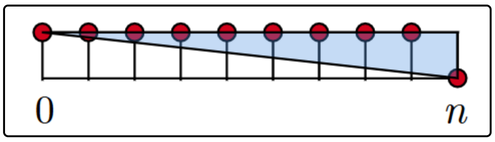
Problem (optional) Create the corresponding $\bmod 3$-convex hull for the product polynomial $f(x) \cdot g(x)$, and count the number of integer points where the **bottom polygonal chain** passes through.

Theorem (Eisenstein, diagrammatic) Let f be a polynomial with $f(0) \neq 0$. If there exists some prime p, such that

- the bottom polygonal chain is straight and passes through none of the integral points,

then the polynomial is irreducible in $\mathbb{Q}[x]$.

Problem (optional) Prove Eisenstein Criterion **without words**.



Example (某年南开 (?) 考研压轴题) Create a criterion (Eisenstein-analogue) according to the following diagram, and make the problem difficult: