Comment: Your course grade before the final exam is in red on your test. Your course grade cannot be lower than what is indicated there if you do or don't take the final exam provided you show up to the last two weeks of classes. For emergency situations, you may also get permission from your instructor to miss a class during these last two weeks.

Test Grades:

100
100
100
98
98
95
95
93
93
92
90
78
59
57
40

Theorem 2.1.1. **(The Schönemann-Eisenstein Criterion)** ***Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ where n is a positive integer. Suppose there exists a prime p such that $p \nmid a_n$, $p | a_j$ for all $j < n$, and $p^2 \nmid a_0$. Then $f(x)$ is irreducible over $\mathbb{Q}$.***

Examples.

Theorem 2.1.1 $\implies$ $2x^6 + 6x^4 + 6$ is irreducible over $\mathbb{Q}$ (but not over $\mathbb{Z}$)

Theorem 2.1.1 $\implies$ $3x^8 + 14x + 10$ is irreducible over $\mathbb{Z}$

Theorem 2.1.1. (The Schönemann-Eisenstein Criterion) *Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ where n is a positive integer. Suppose there exists a prime p such that $p \nmid a_n$, $p | a_j$ for all $j < n$, and $p^2 \nmid a_0$. Then $f(x)$ is irreducible over $\mathbb{Q}$.*

Examples.

$$\text{Theorem 2.1.1} \implies 2x^6 + 6x^4 + 6 \text{ is irreducible over } \mathbb{Q}$$
$$\text{(but not over } \mathbb{Z}\text{)}$$

$$\text{Theorem 2.1.1} \implies 3x^8 + 14x + 10 \text{ is irrreducible over } \mathbb{Z}$$

$$\text{Theorem 2.1.1} \implies x^2 + x + 1 \text{ is irreducible over } \mathbb{Q}$$

Theorem 2.1.1. (The Schönemann-Eisenstein Criterion) *Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ where n is a positive integer. Suppose there exists a prime p such that $p \nmid a_n$, $p | a_j$ for all $j < n$, and $p^2 \nmid a_0$. Then $f(x)$ is irreducible over $\mathbb{Q}$.*

A polynomial $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ is in *Eisenstein form* (with respect to the prime p) if there is a prime p such that $p \nmid a_n$, $p | a_j$ for $j < n$, and $p^2 \nmid a_0$.

An *Eisenstein polynomial* is an $f(x) \in \mathbb{Z}[x]$ for which there is an integer a and a prime p such that $f(x+a)$ is in Eisenstein form with respect to the prime p. In this case, we say $f(x)$ is *Eisenstein with respect to the prime p*.

A polynomial $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ is in ***Eisenstein form*** (with respect to the prime p) if there is a prime p such that $p \nmid a_n$, $p | a_j$ for $j < n$, and $p^2 \nmid a_0$.

An ***Eisenstein polynomial*** is an $f(x) \in \mathbb{Z}[x]$ for which there is an integer a and a prime p such that $f(x+a)$ is in Eisenstein form with respect to the prime p. In this case, we say $f(x)$ is ***Eisenstein with respect to the prime*** p.

Examples.

$x^2 + x + 1$ is Eisenstein with respect to the prime 3

$x^6 + 2x^5 + 2x + 9$ is an Eisenstein polynomial

$$(x+3)^6 + 2(x+3)^5 + 2(x+3) + 9$$
$$= x^6 + 20x^5 + 165x^4 + 720x^3 + 1755x^2 + 2270x + 1230$$

How do we know if a given polynomial is Eisenstein?

Background

$$f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{C}[x], \quad g(x) = \sum_{j=0}^{r} b_j x^j \in \mathbb{C}[x]$$

$$n \geq 1, \quad r \geq 1, \quad a_n b_r \neq 0$$

The resultant of $f(x)$ and $g(x)$, denoted $R(f, g)$, can be defined in terms of an $(n+r) \times (n+r)$ determinant called the Sylvester determinant of $f(x)$ and $g(x)$.

Background

$$f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{C}[x], \quad g(x) = \sum_{j=0}^{r} b_j x^j \in \mathbb{C}[x]$$

$$n \geq 1, \quad r \geq 1, \quad a_n b_r \neq 0$$

$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & a_n & \dots & a_2 & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_r & b_{r-1} & b_{r-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_r & b_{r-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & b_r & \dots & b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \end{vmatrix}$$

Background

$$f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{C}[x], \quad g(x) = \sum_{j=0}^{r} b_j x^j \in \mathbb{C}[x]$$

$$n \geq 1, \quad r \geq 1, \quad a_n b_r \neq 0$$

$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & a_n & \dots & a_2 & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_r & b_{r-1} & b_{r-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_r & b_{r-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & b_r & \dots & b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} r \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ rows} \end{matrix}$$

$$
R(f,g) = \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & a_n & \dots & a_2 & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_r & b_{r-1} & b_{r-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_r & b_{r-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & b_r & \dots & b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} r \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ rows} \end{matrix}
$$

Example.

$$
f(x) = x^3 + 5x^2 + 2x - 1 \quad \text{and} \quad g(x) = 3x^2 + 10x + 2
$$

$$R(f,g) = \left|\begin{matrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & a_n & \dots & a_2 & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_r & b_{r-1} & b_{r-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_r & b_{r-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & b_r & \dots & b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \end{matrix}\right| \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} r \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ rows} \end{matrix}$$

Example.

$$f(x) = x^3 + 5x^2 + 2x - 1 \quad \text{and} \quad g(x) = 3x^2 + 10x + 2$$

$$R(f,g) = \begin{vmatrix} 1 & 5 & 2 & -1 & 0 \\ 0 & 1 & 5 & 2 & -1 \\ 3 & 10 & 2 & 0 & 0 \\ 0 & 3 & 10 & 2 & 0 \\ 0 & 0 & 3 & 10 & 2 \end{vmatrix}$$

$$R(f,g) = \left|\begin{matrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & a_n & \dots & a_2 & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_r & b_{r-1} & b_{r-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_r & b_{r-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & b_r & \dots & b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \end{matrix}\right| \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} r \text{ rows} \\ \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} n \text{ rows} \end{matrix}$$

Example.

$$f(x) = x^3 + 5x^2 + 2x - 1 \quad \text{and} \quad g(x) = 3x^2 + 10x + 2$$

$$R(f,g) = \begin{vmatrix} 1 & 5 & 2 & -1 & 0 \\ 0 & 1 & 5 & 2 & -1 \\ 3 & 10 & 2 & 0 & 0 \\ 0 & 3 & 10 & 2 & 0 \\ 0 & 0 & 3 & 10 & 2 \end{vmatrix} = \begin{vmatrix} 1 & 5 & 2 & -1 & 0 \\ 0 & 1 & 5 & 2 & -1 \\ 0 & -5 & -4 & 3 & 0 \\ 0 & 0 & -5 & -4 & 3 \\ 0 & 0 & 3 & 10 & 2 \end{vmatrix}$$

$$\boldsymbol{R(f,g)} = \begin{vmatrix} \mathbf{1} & \mathbf{5} & \mathbf{2} & \mathbf{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{5} & \mathbf{2} & \mathbf{-1} \\ \mathbf{3} & \mathbf{10} & \mathbf{2} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{3} & \mathbf{10} & \mathbf{2} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{3} & \mathbf{10} & \mathbf{2} \end{vmatrix} = \begin{vmatrix} \mathbf{1} & \mathbf{5} & \mathbf{2} & \mathbf{-1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{5} & \mathbf{2} & \mathbf{-1} \\ \mathbf{0} & \mathbf{-5} & \mathbf{-4} & \mathbf{3} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{-5} & \mathbf{-4} & \mathbf{3} \\ \mathbf{0} & \mathbf{0} & \mathbf{3} & \mathbf{10} & \mathbf{2} \end{vmatrix}$$

$$= \begin{vmatrix} \mathbf{1} & \mathbf{5} & \mathbf{2} & \mathbf{-1} \\ \mathbf{-5} & \mathbf{-4} & \mathbf{3} & \mathbf{0} \\ \mathbf{0} & \mathbf{-5} & \mathbf{-4} & \mathbf{3} \\ \mathbf{0} & \mathbf{3} & \mathbf{10} & \mathbf{2} \end{vmatrix}$$

$$R(f,g)=\begin{vmatrix}1&5&2&-1&0\\0&1&5&2&-1\\3&10&2&0&0\\0&3&10&2&0\\0&0&3&10&2\end{vmatrix}=\begin{vmatrix}1&5&2&-1&0\\0&1&5&2&-1\\0&-5&-4&3&0\\0&0&-5&-4&3\\0&0&3&10&2\end{vmatrix}$$

$$=\begin{vmatrix}1&5&2&-1\\-5&-4&3&0\\0&-5&-4&3\\0&3&10&2\end{vmatrix}=\begin{vmatrix}1&5&2&-1\\0&21&13&-5\\0&-5&-4&3\\0&3&10&2\end{vmatrix}$$

$$=\begin{vmatrix}21&13&-5\\-5&-4&3\\3&10&2\end{vmatrix}=21(-38)-13(-19)+(-5)(-38)$$

$$=19(-42+13+10)$$

$$R(f,g)=\begin{vmatrix}1&5&2&-1&0\\0&1&5&2&-1\\3&10&2&0&0\\0&3&10&2&0\\0&0&3&10&2\end{vmatrix}=\begin{vmatrix}1&5&2&-1&0\\0&1&5&2&-1\\0&-5&-4&3&0\\0&0&-5&-4&3\\0&0&3&10&2\end{vmatrix}$$

$$=\begin{vmatrix}1&5&2&-1\\-5&-4&3&0\\0&-5&-4&3\\0&3&10&2\end{vmatrix}=\begin{vmatrix}1&5&2&-1\\0&21&13&-5\\0&-5&-4&3\\0&3&10&2\end{vmatrix}$$

$$=\begin{vmatrix}21&13&-5\\-5&-4&3\\3&10&2\end{vmatrix}=21(-38)-13(-19)+(-5)(-38)$$

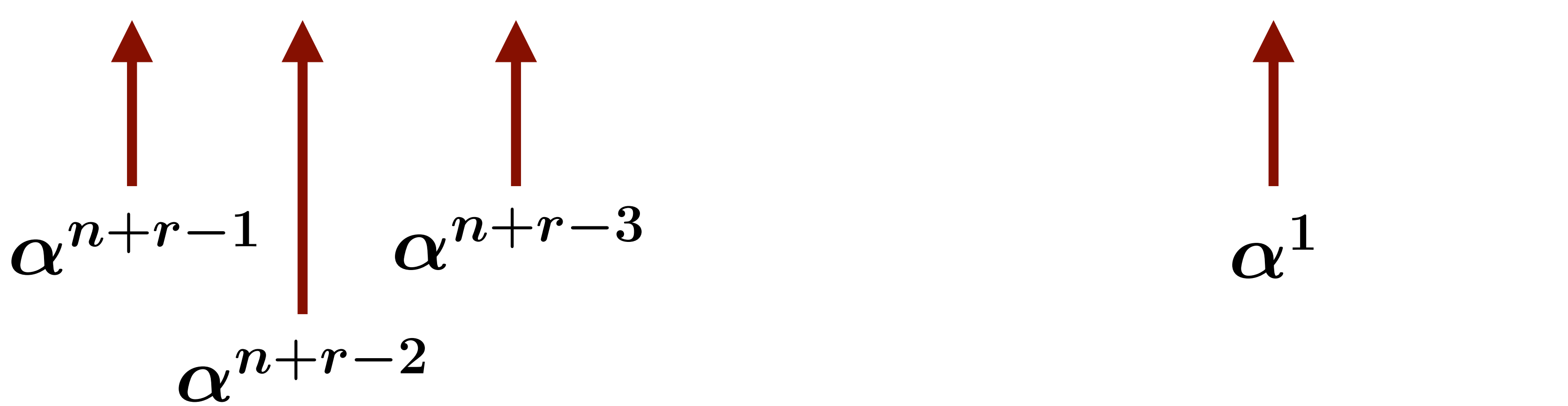
$$=19(-42+13+10)=-19^2$$

Lemma 2.2.1. *Let $f(x)$ and $g(x) \in \mathbb{C}[x]$, and suppose that there is an α such that $f(\alpha) = g(\alpha) = 0$. Then $R(f, g) = 0$.*

$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & a_n & \dots & a_2 & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_r & b_{r-1} & b_{r-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_r & b_{r-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & b_r & \dots & b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} r \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ rows} \end{matrix}$$

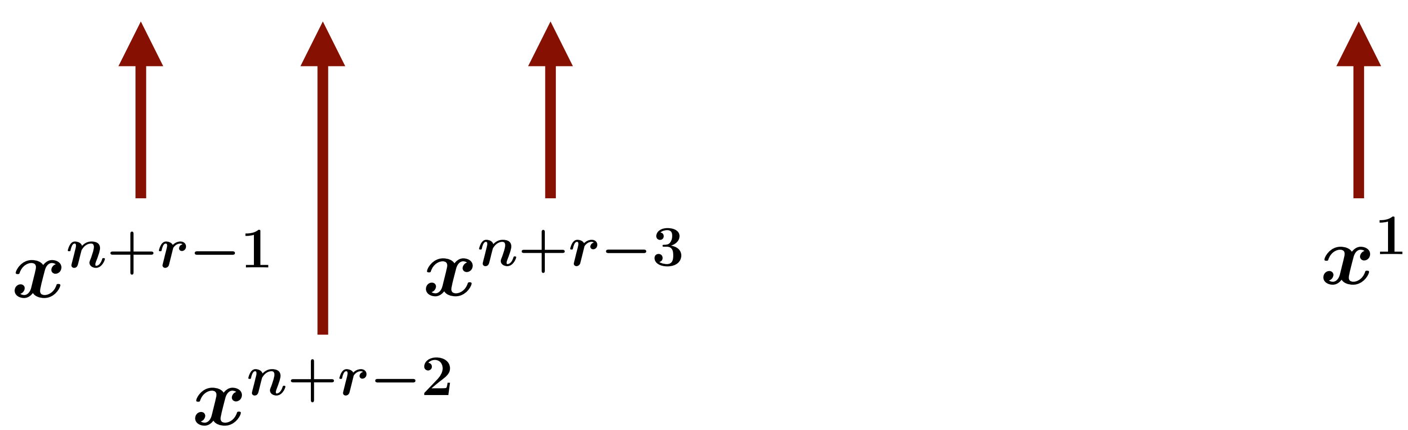
Lemma 2.2.1. *Let $f(x)$ and $g(x) \in \mathbb{C}[x]$, and suppose that there is an α such that $f(\alpha) = g(\alpha) = 0$. Then $R(f,g) = 0$.*

$$R(f,g) = \left| \begin{matrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & a_n & \dots & a_2 & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_r & b_{r-1} & b_{r-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_r & b_{r-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & b_r & \dots & b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \end{matrix} \right| \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} r \text{ rows} \\ \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \end{matrix}}\right\} n \text{ rows} \end{matrix}$$



Lemma 2.2.1. *Let $f(x)$ and $g(x) \in \mathbb{C}[x]$, and suppose that there is an α such that $f(\alpha) = g(\alpha) = 0$. Then $R(f,g) = 0$.*

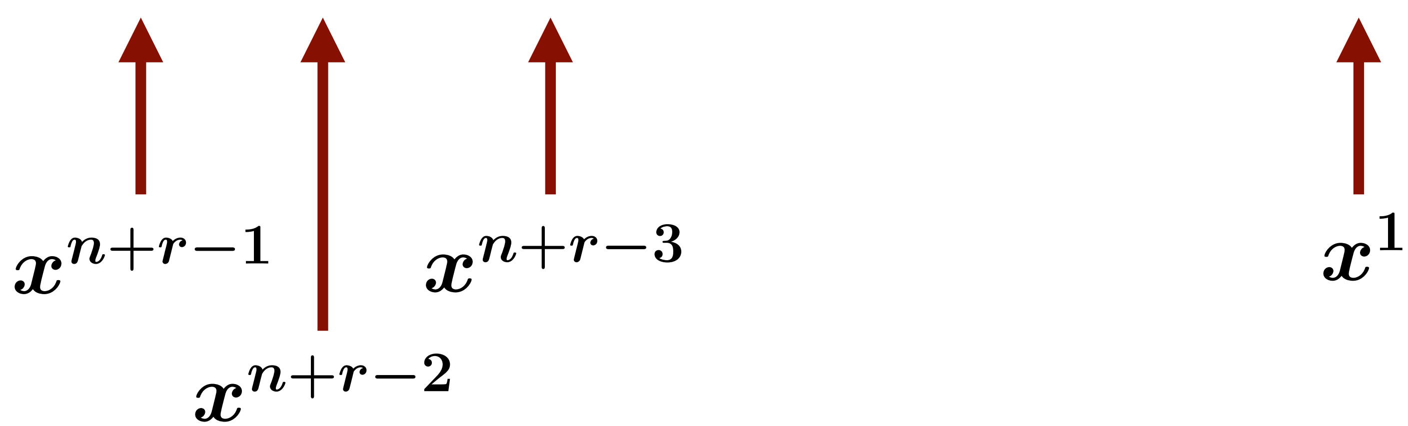
$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & a_n & \dots & a_2 & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_r & b_{r-1} & b_{r-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_r & b_{r-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & b_r & \dots & b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \end{vmatrix} \begin{array}{l} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} r \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ rows} \end{array}$$



Claim. *Given $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$, there exist $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ with $\deg u < \deg g$ and $\deg v < \deg f$ satisfying*

$$f(x)u(x) + g(x)v(x) = R(f,g).$$

$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & a_n & \dots & a_2 & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_r & b_{r-1} & b_{r-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_r & b_{r-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & b_r & \dots & b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} r \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ rows} \end{matrix}$$



Claim. *Given $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$, there exist $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ with $\deg u < \deg g$ and $\deg v < \deg f$ satisfying*

$$(*) \qquad f(x)u(x) + g(x)v(x) = R(f, g).$$

$$w(x) = u(x)g(x)+v(x)h(x), \quad w(x) \text{ monic}, \quad \deg w \text{ minimal}$$

$$u(x) \in F[x], \quad v(x) \in F[x]$$

Is $|R(f, g)|$ the minimal positive integer for which $(*)$ holds?

No

Claim. *Given $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$, there exist $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ with $\deg u < \deg g$ and $\deg v < \deg f$ satisfying*

$$(*) \qquad f(x)u(x) + g(x)v(x) = R(f, g).$$

Lemma 2.2.2. *Let $f(x)$ and $g(x)$ be two non-constant polynomials in the field F where $F = \mathbb{Q}$ or $F = \mathbb{F}_p$. If $R(f, g) = 0$ in F, then $f(x)$ and $g(x)$ have an irreducible factor in common in $F[x]$. If further $\deg g < \deg f$, then $f(x)$ is reducible over F.*

Lemma 2.2.1. *Let $f(x)$ and $g(x) \in \mathbb{C}[x]$, and suppose that there is an α such that $f(\alpha) = g(\alpha) = 0$. Then $R(f, g) = 0$.*

Claim. *Given $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$, there exist $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ with $\deg u < \deg g$ and $\deg v < \deg f$ satisfying*

$$(*) \qquad f(x)u(x) + g(x)v(x) = R(f,g).$$

$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & a_n & \dots & a_2 & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_r & b_{r-1} & b_{r-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_r & b_{r-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & b_r & \dots & b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} r \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ rows} \end{matrix}$$

$\uparrow$ x^{n+r-1} $\quad$ $\uparrow$ x^{n+r-2} $\quad$ $\uparrow$ x^{n+r-3} $\quad \dots \quad$ $\uparrow$ x^1

Claim. *Given $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$, there exist $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ with $\deg u < \deg g$ and $\deg v < \deg f$ satisfying*

$$(*) \qquad f(x)u(x) + g(x)v(x) = R(f, g).$$

$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & a_n & \dots & a_2 & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_r & b_{r-1} & b_{r-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_r & b_{r-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & b_r & \dots & b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \end{vmatrix} \begin{matrix} \left.\right\} r \text{ rows} \\ \left.\right\} n \text{ rows} \end{matrix}$$

Row labels: c_1, c_2, c_3, c_{r+1}, c_{r+2}, c_{r+n}

Column labels: x^{n+r-1}, x^{n+r-2}, x^{n+r-3}, x^1

Claim. *Given $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$, there exist $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ with $\deg u < \deg g$ and $\deg v < \deg f$ satisfying*

$$(*) \qquad f(x)u(x) + g(x)v(x) = R(f, g).$$

c_1, c_2, c_3, c_{r+1}, c_{r+2}, c_{r+n}

$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & a_n & \dots & a_2 & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_r & b_{r-1} & b_{r-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_r & b_{r-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & b_r & \dots & b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \end{vmatrix}$$

r rows

n rows

x^{n+r-1}

x^{n+r-}

$$u(x) = c_1x^{r-1} + c_2x^{r-2} + \cdots + c_r$$

$$v(x) = c_{r+1}x^{n-1} + c_{r+2}x^{n-2} + \cdots + c_{r+n}$$

Claim. *Given $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$, there exist $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ with $\deg u < \deg g$ and $\deg v < \deg f$ satisfying*

$$(*) \qquad f(x)u(x) + g(x)v(x) = R(f, g).$$

Lemma 2.2.2. *Let $f(x)$ and $g(x)$ be two non-constant polynomials in the field F where $F = \mathbb{Q}$ or $F = \mathbb{F}_p$. If $R(f, g) = 0$ in F, then $f(x)$ and $g(x)$ have an irreducible factor in common in $F[x]$. If further $\deg g < \deg f$, then $f(x)$ is reducible over F.*

Lemma 2.2.1. *Let $f(x)$ and $g(x) \in \mathbb{C}[x]$, and suppose that there is an α such that $f(\alpha) = g(\alpha) = 0$. Then $R(f, g) = 0$.*

Background

$$f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{C}[x], \quad g(x) = \sum_{j=0}^{r} b_j x^j \in \mathbb{C}[x]$$

$$n \geq 1, \quad r \geq 1, \quad a_n b_r \neq 0$$

$$R(f,g) = \left| \begin{matrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & a_n & \dots & a_2 & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_r & b_{r-1} & b_{r-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_r & b_{r-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & b_r & \dots & b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \end{matrix} \right| \begin{matrix} \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} r \text{ rows} \\ \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} n \text{ rows} \end{matrix}$$

$$f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{C}[x], \quad g(x) = \sum_{j=0}^{r} b_j x^j \in \mathbb{C}[x]$$

$$n \geq 1, \quad r \geq 1, \quad a_n b_r \neq 0$$

$$R(f,g) = \left| \begin{matrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & a_n & \dots & a_2 & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_r & b_{r-1} & b_{r-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_r & b_{r-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & b_r & \dots & b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \end{matrix} \right| \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} r \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ rows} \end{matrix}$$

Comment: If $\alpha_1, \dots, \alpha_n$ are the roots of $f(x)$, then

$$R(f,g) = a_n^r \, g(\alpha_1) \cdots g(\alpha_n).$$

$$f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{C}[x], \quad g(x) = \sum_{j=0}^{r} b_j x^j \in \mathbb{C}[x]$$

$$n \geq 1, \quad r \geq 1, \quad a_n b_r \neq 0$$

Comment: If $\alpha_1, \ldots, \alpha_n$ are the roots of $f(x)$, then

$$R(f, g) = a_n^r g(\alpha_1) \cdots g(\alpha_n).$$

Lemma 2.2.1. *Let $f(x)$ and $g(x) \in \mathbb{C}[x]$, and suppose that there is an α such that $f(\alpha) = g(\alpha) = 0$. Then $R(f, g) = 0$.*

$$f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{C}[x], \quad g(x) = \sum_{j=0}^{r} b_j x^j \in \mathbb{C}[x]$$

$$n \geq 1, \quad r \geq 1, \quad a_n b_r \neq 0$$

Comment: If $\alpha_1, \ldots, \alpha_n$ are the roots of $f(x)$, then

$$R(f, g) = a_n^r g(\alpha_1) \cdots g(\alpha_n).$$

Lemma 2.2.1. *Let $f(x)$ and $g(x)$ be two non-constant polynomials in the field F where $F = \mathbb{Q}$ or $F = \mathbb{F}_p$. If $R(f, g) = 0$ in F, then $f(x)$ and $g(x)$ have an irreducible factor in common in $F[x]$. If further $\deg g < \deg f$, then $f(x)$ is reducible over F.*

Algorithm: Given $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 2$, determine whether $f(x)$ is an Eisenstein polynomial.

A polynomial $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ is in *Eisenstein form* (with respect to the prime p) if there is a prime p such that $p \nmid a_n$, $p | a_j$ for $j < n$, and $p^2 \nmid a_0$.

An *Eisenstein polynomial* is an $f(x) \in \mathbb{Z}[x]$ for which there is an integer a and a prime p such that $f(x+a)$ is in Eisenstein form with respect to the prime p. In this case, we say $f(x)$ is *Eisenstein with respect to the prime p*.

Algorithm: Given $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 2$, determine whether $f(x)$ is an Eisenstein polynomial.

Steps:

Algorithm: Given $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 2$, determine whether $f(x)$ is an Eisenstein polynomial.

Steps:

- **Calculate $R(f, f')$.**

Algorithm: Given $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 2$, determine whether $f(x)$ is an Eisenstein polynomial.

Steps:

- **Calculate $R(f, f')$.**

  $\rightarrow$ If $R(f, f') = 0$, then $f(x)$ is not Eisenstein with respect to any prime.

Lemma 2.2.1. *Let $f(x)$ and $g(x)$ be two non-constant polynomials in the field F where $F = \mathbb{Q}$ or $F = \mathbb{F}_p$. If $R(f, g) = 0$ in F, then $f(x)$ and $g(x)$ have an irreducible factor in common in $F[x]$. If further $\deg g < \deg f$, then $f(x)$ is reducible over F.*

Algorithm: Given $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 2$, determine whether $f(x)$ is an Eisenstein polynomial.

Steps:

- **Calculate $R(f, f')$.**

  $\rightarrow$ **If $R(f, f') = 0$, then $f(x)$ is not Eisenstein with respect to any prime.**

  $\rightarrow$ **If $R(f, f') \neq 0$, then proceed as follows.**

Algorithm: Given $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 2$, determine whether $f(x)$ is an Eisenstein polynomial.

Steps:

- **Calculate $R(f, f')$.**
  - $\rightarrow$ **If $R(f, f') = 0$, then $f(x)$ is not Eisenstein with respect to any prime.**
  - $\rightarrow$ **If $R(f, f') \neq 0$, then proceed as follows.**
    - ▶ **Factor $R(f, f')$.**

Algorithm: Given $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 2$, determine whether $f(x)$ is an Eisenstein polynomial.

Steps:

- **Calculate $R(f, f')$.**
  - → **If $R(f, f') = 0$, then $f(x)$ is not Eisenstein with respect to any prime.**
  - → **If $R(f, f') \neq 0$, then proceed as follows.**
    - ▶ **Factor $R(f, f')$.**
    - ▶ **For each prime p dividing $R(f, f')$ and each $a \in \{0, 1, ..., p - 1\}$, check if $f(x + a)$ is in Eisenstein form with respect p.**

Algorithm: Given $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 2$, determine whether $f(x)$ is an Eisenstein polynomial.

Steps:

- **Calculate $R(f, f')$.**
  - → **If $R(f, f') = 0$, then $f(x)$ is not Eisenstein with respect to any prime.**
  - → **If $R(f, f') \neq 0$, then proceed as follows.**
    - ▶ **Factor $R(f, f')$.**
    - ▶ **For each prime p dividing $R(f, f')$ and each $a \in \{0, 1, ..., p-1\}$, check if $f(x+a)$ is in Eisenstein form with respect p.**
      - ≻ **If it is for some such p, then $f(x)$ is an Eisenstein polyomial (with respect to p).**

Algorithm: Given $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 2$, determine whether $f(x)$ is an Eisenstein polynomial.

Steps:

- Calculate $R(f, f')$.
  - $\rightarrow$ If $R(f, f') = 0$, then $f(x)$ is not Eisenstein with respect to any prime.
  - $\rightarrow$ If $R(f, f') \neq 0$, then proceed as follows.
    - ▶ Factor $R(f, f')$.
    - ▶ For each prime p dividing $R(f, f')$ and each $a \in \{0, 1, ..., p-1\}$, check if $f(x+a)$ is in Eisenstein form with respect p.
      - $\succ$ If it is for some such p, then $f(x)$ is an Eisenstein polyomial (with respect to p).
      - $\succ$ If it is not for every such p, then $f(x)$ is not an Eisenstein polynomial. ∎

Comment: If for some integer a we have that $f(x+a)$ is in Eisenstein form with respect to the prime p, then $f(x) \equiv a_n(x-a)^n \pmod{p}$.

Idea for most of Algorithm. Show that if there is a prime p such that

$$f(x) \equiv g(x)^2 h(x) \pmod{p}, \quad \text{where } \deg g \geq 1,$$

then $p | R(f, f')$.

Is the matrix below nonsingular?

$$\begin{pmatrix} 119 & 532 & 289 \\ 873 & 112 & 567 \\ 222 & 633 & 650 \end{pmatrix}$$

$$
R(f,g) = \begin{vmatrix}
a_n & a_{n-1} & a_{n-2} & \ldots & a_0 & 0 & 0 & \ldots & 0 \\
0 & a_n & a_{n-1} & \ldots & a_1 & a_0 & 0 & \ldots & 0 \\
0 & 0 & a_n & \ldots & a_2 & a_1 & a_0 & \ldots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
b_r & b_{r-1} & b_{r-2} & \ldots & b_0 & 0 & 0 & \ldots & 0 \\
0 & b_r & b_{r-1} & \ldots & b_1 & b_0 & 0 & \ldots & 0 \\
0 & 0 & b_r & \ldots & b_2 & b_1 & b_0 & \ldots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots
\end{vmatrix}
\begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} r \text{ rows} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ rows} \end{matrix}
$$

Comment: If for some integer a we have that $f(x+a)$ is in Eisenstein form with respect to the prime p, then $f(x) \equiv a_n(x-a)^n \pmod{p}$.

Idea for most of Algorithm. Show that if there is a prime p such that

$$f(x) \equiv g(x)^2 h(x) \pmod{p}, \quad \text{where } \deg g \geq 1,$$

then $p | R(f, f')$.

Algorithm: Given $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 2$, determine whether $f(x)$ is an Eisenstein polynomial.

Steps:

- **Calculate $R(f, f')$.**
  - $\rightarrow$ **If $R(f, f') = 0$, then $f(x)$ is not Eisenstein with respect to any prime.**
  - $\rightarrow$ **If $R(f, f') \neq 0$, then proceed as follows.**
    - ▶ **Factor $R(f, f')$.**
    - ▶ **For each prime p dividing $R(f, f')$ and each $a \in \{0, 1, ..., p-1\}$, check if $f(x+a)$ is in Eisenstein form with respect p.**
      - $\succ$ **If it is for some such p, then $f(x)$ is an Eisenstein polyomial (with respect to p).**
      - $\succ$ **If it is not for every such p, then $f(x)$ is not an Eisenstein polynomial.**

Comment: If for some integer a we have that $f(x+a)$ is in Eisenstein form with respect to the prime p, then $f(x) \equiv a_n(x-a)^n \pmod{p}$.

Idea for most of Algorithm. Show that if there is a prime p such that

$$f(x) \equiv g(x)^2 h(x) \pmod{p}, \quad \text{where } \deg g \geq 1,$$

then $p | R(f, f')$.

Idea for last part of Algorithm. If $b \in \mathbb{Z}$ satisfies $f(x+b)$ is in Eisenstein form with respect to some prime p, then $f(x+a)$ is also for all $a \equiv b \pmod{p}$.

$$f(x+b) = \sum_{j=0}^{n} a'_j x^j \quad \text{Eisenstein form with respect to } p$$

Comment: If for some integer a we have that $f(x+a)$ is in Eisenstein form with respect to the prime p, then $f(x) \equiv a_n(x-a)^n \pmod{p}$.

Idea for most of Algorithm. Show that if there is a prime p such that

$$f(x) \equiv g(x)^2 h(x) \pmod{p}, \quad \text{where } \deg g \geq 1,$$

then $p | R(f, f')$.

Idea for last part of Algorithm. If $b \in \mathbb{Z}$ satisfies $f(x+b)$ is in Eisenstein form with respect to some prime p, then $f(x+a)$ is also for all $a \equiv b \pmod{p}$.

$$f(x+b) = \sum_{j=0}^{n} a'_j x^j \text{ Eisenstein form with respect to } p$$

$$\Longrightarrow f(kp+b) \equiv kpa'_1 + a'_0 \equiv a'_0 \pmod{p^2}$$

Algorithm: Given $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 2$, determine whether $f(x)$ is an Eisenstein polynomial.

Steps:

- **Calculate $R(f, f')$.**
  - → **If $R(f, f') = 0$, then $f(x)$ is not Eisenstein with respect to any prime.**
  - → **If $R(f, f') \neq 0$, then proceed as follows.**
    - ▶ **Factor $R(f, f')$.**
    - ▶ **For each prime p dividing $R(f, f')$ and each $a \in \{0, 1, ..., p-1\}$, check if $f(x+a)$ is in Eisenstein form with respect p.**
      - ≻ **If it is for some such p, then $f(x)$ is an Eisenstein polyomial (with respect to p).**
      - ≻ **If it is not for every such p, then $f(x)$ is not an Eisenstein polynomial.**

Example.

$$f(x) = x^3 + 5x^2 + 2x - 1 \quad \text{and} \quad g(x) = 3x^2 + 10x + 2$$

$$R(f,g) = \begin{vmatrix} 1 & 5 & 2 & -1 & 0 \\ 0 & 1 & 5 & 2 & -1 \\ 3 & 10 & 2 & 0 & 0 \\ 0 & 3 & 10 & 2 & 0 \\ 0 & 0 & 3 & 10 & 2 \end{vmatrix} = \begin{vmatrix} 1 & 5 & 2 & -1 & 0 \\ 0 & 1 & 5 & 2 & -1 \\ 0 & -5 & -4 & 3 & 0 \\ 0 & 0 & -5 & -4 & 3 \\ 0 & 0 & 3 & 10 & 2 \end{vmatrix}$$

$$= \begin{vmatrix} 1 & 5 & 2 & -1 \\ -5 & -4 & 3 & 0 \\ 0 & -5 & -4 & 3 \\ 0 & 3 & 10 & 2 \end{vmatrix} = \begin{vmatrix} 1 & 5 & 2 & -1 \\ 0 & 21 & 13 & -5 \\ 0 & -5 & -4 & 3 \\ 0 & 3 & 10 & 2 \end{vmatrix}$$

$$= \begin{vmatrix} 21 & 13 & -5 \\ -5 & -4 & 3 \\ 3 & 10 & 2 \end{vmatrix} = 21(-38) - 13(-19) + (-5)(-38)$$

$$= 19(-42 + 13 + 10) = -19^2$$

Example.

$$f(x) = x^3 + 5x^2 + 2x - 1 \quad \text{and} \quad g(x) = 3x^2 + 10x + 2$$

```
> f := x -> x^3 + 5*x^2 + 2*x - 1;
```

$$f := x \to x^3 + 5\,x^2 + 2\,x - 1$$

```
> sort(expand(f(x+11)));
```

$$x^3 + 38\,x^2 + 475\,x + 1957$$

```
> ifactor(475); ifactor(1957);
```

$$(5)^2\,(19)$$

$$(19)\,(103)$$

Note: The prime $p = 19$ is the only p that can "work". From $f(x) \equiv (x - 11)^3 \pmod{19}$ and unique factorization in $\mathbb{F}_{19}[x]$, we get 11 is the only a that can "work".