Factoring Polynomials

Notation. Let p be a prime, and let $f(x) \in \mathbb{Z}[x]$ with $f(x) \not\equiv 0 \pmod{p}$. We say

$$u(x) \equiv v(x) \pmod{p,\ f(x)}$$

where $u(x)$ and $v(x)$ are in $\mathbb{Z}[x]$, if there exist $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ such that $u(x) = v(x) + f(x)g(x) + p\,h(x)$.

Properties:

- **If**

$$u(x) \equiv v(x) \pmod{p,\ f(x)} \text{ and } v(x) \equiv w(x) \pmod{p,\ f(x)},$$

  then $u(x) \equiv w(x) \pmod{p,\ f(x)}$.

- **If**

$$u_1(x) \equiv v_1(x) \pmod{p,\ f(x)} \text{ and } u_2(x) \equiv v_2(x) \pmod{p,\ f(x)},$$

  then $u_1(x) \pm u_2(x) \equiv v_1(x) \pm v_2(x) \pmod{p,\ f(x)}$.

- **If**

$$u_1(x) \equiv v_1(x) \pmod{p,\ f(x)} \text{ and } u_2(x) \equiv v_2(x) \pmod{p,\ f(x)},$$

  then $u_1(x)u_2(x) \equiv v_1(x)v_2(x) \pmod{p,\ f(x)}$.

- **If** $u(x) \equiv v(x) \pmod{p}$ **or** $u(x) \equiv v(x) \pmod{f(x)}$, **then** $u(x) \equiv v(x) \pmod{p,\ f(x)}$.

- **We have** $u(x) \equiv 0 \pmod{p,\ f(x)}$ **if and only if** $f(x)$ **is a factor of** $u(x)$ **modulo** p.

- If the leading coefficient of $f(x) \in \mathbb{Z}[x]$ is a mod p (i.e., a is the coefficient of the highest degree term in $f(x)$ which is non-zero modulo p), then $f(x) \equiv a\,g(x) \pmod{p}$ for some monic $g(x) \in \mathbb{Z}[x]$. Then

$$u(x) \equiv v(x) \text{ (mod } p,\ f(x)) \iff u(x) \equiv v(x) \text{ (mod } p,\ g(x)).$$

Suppose now that $f(x)$ is monic.

- If $u(x) \equiv v(x)$ (mod p, $f(x)$) where $u(x)$ and $v(x)$ are in $\mathbb{Z}[x]$, then there exist unique polynomials $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ with $h(x) \equiv 0$ or $\deg h < \deg f$ such that $u(x) - v(x) = f(x)g(x) + p\,h(x)$.

$$u(x) - v(x) = f(x)g_0(x) + ph_0(x)$$

$$h_0(x) = f(x)q(x) + r(x)$$

$$g(x) = g_0(x) + pq(x), \quad h(x) = r(x)$$

Suppose now that $f(x)$ is monic.

What Makes F a Field?

(i) closed under sums and products

(ii) sums and products commute

(iii) associative laws hold

(iv) identity elements exist

(v) inverses exist $\forall a \in F$ with $a \neq 0$

(vi) the distributive law holds

- If $u(x)$ … $v(x)$ are in $\mathbb{Z}[x]$ … $g(x)$ and $h(x)$ in … such that $u(x) -$ …
- If deg … residue classes … by the polyno… from $\{0, 1, .$ …

Suppose also that $f(x)$ is irreducible modulo p.

- Let $a(x) \in \mathbb{Z}[x]$ with $a(x) \not\equiv 0 \pmod{p,\ f(x)}$. Then $\exists\, b(x) \in \mathbb{Z}[x]$ such that $a(x)b(x) \equiv 1 \pmod{p,\ f(x)}$.
- Arithmetic mod p, $f(x)$ forms a field with p^k elements where $k = \deg f$.

Berlekamp's Method

This algorithm determines the factorization of a polynomial $f(x)$ modulo a prime p.

Berlekamp's Method

This algorithm determines the factorization of a polynomial $f(x)$ modulo a prime p. For simplicity, we suppose $f(x)$ is monic and squarefree in modulo p.

Berlekamp's Method

This algorithm determines the factorization of a polynomial $f(x)$ modulo a prime p. For simplicity, we suppose $f(x)$ is monic and squarefree in modulo p.

Notation. We set $n = \deg f(x)$.

Berlekamp's Method

This algorithm determines the factorization of a polynomial $f(x)$ modulo a prime p. For simplicity, we suppose $f(x)$ is monic and squarefree in modulo p.

Notation. We set $n = \deg f(x)$. We use $\mathbb{F}_p$ to denote the field of arithmetic mod p.

Berlekamp's Method

This algorithm determines the factorization of a polynomial $f(x)$ modulo a prime p. For simplicity, we suppose $f(x)$ is monic and squarefree in modulo p.

Notation. We set $n = \deg f(x)$. We use $\mathbb{F}_p$ to denote the field of arithmetic mod p. For $w(x) \in \mathbb{Z}[x]$, define

$$w(x) \text{ modd } (p, f(x))$$

as the unique $g(x) \in \mathbb{Z}[x]$ satisfying $\deg g \le n-1$, with each coefficient of $g(x)$ in the set $\{0, 1, \ldots, p-1\}$ and $g(x) \equiv w(x) \pmod{p,\ f(x)}$.

Berlekamp's Method

This algorithm determines the factorization of a polynomial $f(x)$ modulo a prime p. For simplicity, we suppose $f(x)$ is monic and squarefree in modulo p.

Notation. We set $n = \deg f(x)$. We use $\mathbb{F}_p$ to denote the field of arithmetic mod p. For $w(x) \in \mathbb{Z}[x]$, define

$$w(x) \text{ modd } (p, f(x))$$

as the unique $g(x) \in \mathbb{Z}[x]$ satisfying $\deg g \leq n-1$, with each coefficient of $g(x)$ in the set $\{0, 1, \ldots, p-1\}$ and $g(x) \equiv w(x) \pmod{p,\ f(x)}$. We can also view $w(x)$ modd $(p, f(x))$ as being in $\mathbb{F}_p[x]$.

Berlekamp's Method

Let A be the matrix with jth column corresponding to the coefficients of

$$x^{(j-1)p} \text{ modd } (p, f(x)).$$

Specifically, write

$$x^{(j-1)p} \text{ modd } (p, f(x)) = \sum_{i=1}^{n} a_{ij} x^{i-1} \qquad \text{for } 1 \le j \le n.$$

Then we set $A = (a_{ij})_{n \times n}$.

Observations

- **The vector $\langle 1, 0, 0, \ldots, 0 \rangle$ will be an eigenvector for A associated with the eigenvalue 1.**

Let A be the matrix with jth column corresponding to the coefficients of

$$x^{(j-1)p} \text{ modd } (p, f(x)).$$

Specifically, write

$$x^{(j-1)p} \text{ modd } (p, f(x)) = \sum_{i=1}^{n} a_{ij} x^{i-1} \qquad \text{for } 1 \le j \le n.$$

Then we set $A = (a_{ij})_{n \times n}$.

Observations

- The vector $\langle 1, 0, 0, \ldots, 0 \rangle$ will be an eigenvector for A associated with the eigenvalue 1.
- The set of all such vectors is the null space of $B = A - I$.
- This null space is spanned by $k = n - \operatorname{rank}(B)$ linearly independent vectors which can be determined by performing row operations on B.

Example. $f(x) = x^4 + x^3 + x + 1$ and $p = 2$

Let A be the matrix with jth column corresponding to the coefficients of

$$x^{(j-1)p} \text{ modd } (p, f(x)).$$

Specifically, write

$$x^{(j-1)p} \text{ modd } (p, f(x)) = \sum_{i=1}^{n} a_{ij} x^{i-1} \qquad \text{for } 1 \le j \le n.$$

Then we set $A = (a_{ij})$

$$\begin{aligned}
x^0 \text{ modd } (2, f(x)) &= 1 \\
x^2 \text{ modd } (2, f(x)) &= x^2 \\
x^4 \text{ modd } (2, f(x)) &= x^3 + x + 1 \\
x^6 \text{ modd } (2, f(x)) &= x^5 + x^3 + x^2 \text{ modd } (2, f(x)) \\
&= x^4 + x^3 + x \text{ modd } (2, f(x)) = 1
\end{aligned}$$

forming row operations on B.

Example. $f(x) = x^4 + x^3 + x + 1$ and $p = 2$

$$
\begin{aligned}
x^0 \text{ modd } (2, f(x)) &= 1 \\
x^2 \text{ modd } (2, f(x)) &= x^2 \\
x^4 \text{ modd } (2, f(x)) &= x^3 + x + 1 \\
x^6 \text{ modd } (2, f(x)) &= x^5 + x^3 + x^2 \text{ modd } (2, f(x)) \\
&= x^4 + x^3 + x \text{ modd } (2, f(x)) = 1
\end{aligned}
$$

Then we set $A = (a_{ij})_{n \times n}$.

$$
A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}
$$

$\ldots, 0\rangle$ will be an eigenvector for A eigenvalue 1.

ectors is the null space of $B = A - I$.

panned by $k = n - \text{rank}(B)$ linearly which can be determined by performing row operations on B.

Example. $f(x) = x^4 + x^3 + x + 1$ **and** $p = 2$

$$
\begin{aligned}
x^0 \text{ modd } (2, f(x)) &= 1 \\
x^2 \text{ modd } (2, f(x)) &= x^2 \\
x^4 \text{ modd } (2, f(x)) &= x^3 + x + 1 \\
x^6 \text{ modd } (2, f(x)) &= x^5 + x^3 + x^2 \text{ modd } (2, f(x)) \\
&= x^4 + x^3 + x \text{ modd } (2, f(x)) = 1
\end{aligned}
$$

Then we set $A = (a_{ij})_{n \times n}$.

$$
A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}
$$

genvector for A

ce of $B = A - I$.

rank(B) linearly

ermined by per-

forming row operations on B.

Example. $f(x) = x^4 + x^3 + x + 1$ **and** $p = 2$

$$
\begin{aligned}
x^0 \text{ modd } (2, f(x)) &= 1 \\
x^2 \text{ modd } (2, f(x)) &= x^2 \\
x^4 \text{ modd } (2, f(x)) &= x^3 + x + 1 \\
x^6 \text{ modd } (2, f(x)) &= x^5 + x^3 + x^2 \text{ modd } (2, f(x)) \\
&= x^4 + x^3 + x \text{ modd } (2, f(x)) = 1
\end{aligned}
$$

Then we set $A = (a_{ij})_{n \times n}$.

$$
A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}
$$

forming row operations on B.

Example. $f(x) = x^4 + x^3 + x + 1$ and $p = 2$

$$
\begin{aligned}
x^0 \text{ modd } (2, f(x)) &= 1 \\
x^2 \text{ modd } (2, f(x)) &= x^2 \\
x^4 \text{ modd } (2, f(x)) &= x^3 + x + 1 \\
x^6 \text{ modd } (2, f(x)) &= x^5 + x^3 + x^2 \text{ modd } (2, f(x)) \\
&= x^4 + x^3 + x \text{ modd } (2, f(x)) = 1
\end{aligned}
$$

$$
A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad
B = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \longrightarrow
\begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}
$$

Null space is spanned by $\langle 1, 0, 0, 0 \rangle$ and $\langle 0, 1, 1, 1 \rangle$.

Suppose $\vec{v} = \langle b_1, b_2, \ldots, b_n \rangle$ is in the null space, and set $g(x) = \sum_{j=1}^{n} b_j x^{j-1}$.

Suppose $\vec{v} = \langle b_1, b_2, \ldots, b_n \rangle$ is in the null space, and set $g(x) = \sum_{j=1}^{n} b_j x^{j-1}$. Observe that

$$g(x^p) \equiv g(x) \pmod{p,\ f(x)}.$$

$$g(x^p) \equiv \sum_{j=1}^{n} b_j x^{(j-1)p}$$

Suppose $\vec{v} = \langle b_1, b_2, \ldots, b_n \rangle$ is in the null space, and set $g(x) = \sum_{j=1}^{n} b_j x^{j-1}$. Observe that

$$g(x^p) \equiv g(x) \pmod{p,\ f(x)}.$$

$$g(x^p) \equiv \sum_{j=1}^{n} b_j x^{(j-1)p} \equiv \sum_{j=1}^{n} b_j \sum_{i=1}^{n} a_{ij} x^{i-1}$$

Suppose $\vec{v} = \langle b_1, b_2, \ldots, b_n \rangle$ is in the null space, and set $g(x) = \sum_{j=1}^{n} b_j x^{j-1}$. Observe that

$$g(x^p) \equiv g(x) \pmod{p,\ f(x)}.$$

$$g(x^p) \equiv \sum_{j=1}^{n} b_j x^{(j-1)p} \equiv \sum_{j=1}^{n} b_j \sum_{i=1}^{n} a_{ij} x^{i-1}$$

$$\equiv \sum_{i=1}^{n} \left(\sum_{j=1}^{n} b_j a_{ij} \right) x^{i-1}$$

Suppose $\vec{v} = \langle b_1, b_2, \ldots, b_n\rangle$ is in the null space, and set $g(x) = \sum_{j=1}^{n} b_j x^{j-1}$. Observe that

$$g(x^p) \equiv g(x) \pmod{p,\ f(x)}.$$

$$g(x^p) \equiv \sum_{j=1}^{n} b_j x^{(j-1)p} \equiv \sum_{j=1}^{n} b_j \sum_{i=1}^{n} a_{ij} x^{i-1}$$

$$\equiv \sum_{i=1}^{n} \left(\sum_{j=1}^{n} b_j a_{ij} \right) x^{i-1} \equiv \sum_{i=1}^{n} b_i x^{i-1}$$

Suppose $\vec{v} = \langle b_1, b_2, \ldots, b_n \rangle$ is in the null space, and set $g(x) = \sum_{j=1}^{n} b_j x^{j-1}$. Observe that

$$g(x^p) \equiv g(x) \pmod{p,\ f(x)}.$$

$$\begin{aligned} g(x^p) &\equiv \sum_{j=1}^{n} b_j x^{(j-1)p} \equiv \sum_{j=1}^{n} b_j \sum_{i=1}^{n} a_{ij} x^{i-1} \\ &\equiv \sum_{i=1}^{n} \left(\sum_{j=1}^{n} b_j a_{ij} \right) x^{i-1} \equiv \sum_{i=1}^{n} b_i x^{i-1} \equiv g(x) \end{aligned}$$

Suppose $\vec{v} = \langle b_1, b_2, \ldots, b_n \rangle$ is in the null space, and set $g(x) = \sum_{j=1}^{n} b_j x^{j-1}$. Observe that

$$g(x^p) \equiv g(x) \pmod{p,\ f(x)}.$$

Moreover, the $g(x)$ with this property are precisely the $g(x)$ with coefficients obtained from the components of vectors $\vec{v}$ in the null space of B.

$$\begin{aligned} g(x^p) &\equiv \sum_{j=1}^{n} b_j x^{(j-1)p} \equiv \sum_{j=1}^{n} b_j \sum_{i=1}^{n} a_{ij} x^{i-1} \\ &\equiv \sum_{i=1}^{n} \left(\sum_{j=1}^{n} b_j a_{ij} \right) x^{i-1} \equiv \sum_{i=1}^{n} b_i x^{i-1} \equiv g(x) \end{aligned}$$

Suppose $\vec{v} = \langle b_1, b_2, \ldots, b_n \rangle$ is in the null space, and set $g(x) = \sum_{j=1}^{n} b_j x^{j-1}$. Observe that

$$g(x^p) \equiv g(x) \pmod{p,\ f(x)}.$$

Moreover, the $g(x)$ with this property are precisely the $g(x)$ with coefficients obtained from the components of vectors $\vec{v}$ in the null space of B.

Notation. If $u(x)$ and $v(x)$ are in $\mathbb{Z}[x]$ or $\mathbb{F}_p[x]$, then

$$\gcd{}_p\big(u(x), v(x)\big)$$

denotes the greatest common divisor of $u(x)$ and $v(x)$ when computed over the field $\mathbb{F}_p$.

Definition. The greatest common divisor of two polynomials $g(x)$ and $h(x)$ in $\mathbb{F}_p[x]$, with at least one of $g(x)$ or $h(x)$ non-zero, is the monic polynomial in $\mathbb{F}_p[x]$ of largest degree which divides both $g(x)$ and $h(x)$ and is denoted by $\gcd(g(x), h(x))$.

Suppose $\vec{v} = \langle b_1, b_2, \ldots, b_n \rangle$ is in the null space, and set $g(x) = \sum_{j=1}^{n} b_j x^{j-1}$. Observe that

$$g(x^p) \equiv g(x) \pmod{p,\ f(x)}.$$

Moreover, the $g(x)$ with this property are precisely the $g(x)$ with coefficients obtained from the components of vectors $\vec{v}$ in the null space of B.

Berlekamp's Method

Theorem. *Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$. Suppose $f(x)$ is squarefree in $\mathbb{F}_p[x]$. Let $g(x)$ be a polynomial with coefficients obtained from a vector in the null space of $B = A - I$ as described above. Then*

$$f(x) \equiv \prod_{s=0}^{p-1} \gcd{}_p\big(g(x) - s, f(x)\big) \pmod{p}.$$

Suppose $\vec{v} = \langle b_1, b_2, \ldots, b_n \rangle$ is in the null space, and set $g(x) = \sum_{j=1}^{n} b_j x^{j-1}$. Observe that

$$g(x^p) \equiv g(x) \pmod{p,\ f(x)}.$$

Moreover, the $g(x)$ with this property are precisely the $g(x)$ with coefficients obtained from the components of vectors $\vec{v}$ in the null space of B.

Theorem. *Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$. Suppose $f(x)$ is squarefree in $\mathbb{F}_p[x]$. Let $g(x)$ be a polynomial with coefficients obtained from a vector in the null space of $B = A - I$ as described above. Then*

$$f(x) \equiv \prod_{s=0}^{p-1} \gcd{}_p\big(g(x) - s, f(x)\big) \pmod{p}.$$

Comment: If $\deg g > 0$, then the factorization is non-trivial.

Do MAPLE examples.