Homework: **(due November 9 by class time)**
Page 20, the one Homework problem there
Page 22, Problem (1) and (2)

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 $\mathbb{F}_p[x]$.

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

$$x^{(j-1)p} \bmod \mathrm{d}\ (p, f(x)).$$

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

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

Suppose $\vec{v} = \langle b_1, b_2, \dots, b_n \rangle$ 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.

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

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*

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

$$g(x)^p - g(x) \equiv \prod_{s=0}^{p-1} (g(x) - s) \pmod{p}$$

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

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

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***

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

$$g(x)^p - g(x) \equiv \prod_{s=0}^{p-1} (g(x) - s) \pmod{p}$$

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

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

$$\prod_{s=0}^{p-1} (g(x) - s) \equiv f(x)u(x) \pmod{p}$$

Etc.

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***

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

Comments:

- **If $g(x)$ isn't constant, then $1 \le \deg(g(x) - s) < \deg f(x)$ for each s, so we get a non-trivial factorization of $f(x)$ in $\mathbb{F}_p[x]$.**
- **The above will NOT necessarily completely factor $f(x)$ modulo p.**

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*

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

Comments:

- One can completely factor $f(x)$ by taking the product of the greatest common divisors of each factor of $f(x)$ obtained above with $h(x) - s$ (with $0 \le s \le p-1$) where $h(x)$ is obtained from another of the k vectors spanning the null space of B. This will obtain a new non-trivial factor of $f(x)$ in $\mathbb{F}_p[x]$. Continuing to use all k vectors will produce a complete factorization of $f(x)$ in $\mathbb{F}_p[x]$.

Hensel Lifting

The method takes a factorization of $f(x)$ modulo a prime p and produces a factorization of $f(x)$ modulo p^k for an arbitrary positive integer k.

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

We only consider $f(x)$ monic and $u(x)$ and $v(x)$ relatively prime in $\mathbb{F}_p[x]$.

Hensel Lifting

The method takes a factorization of $f(x)$ modulo a prime p and produces a factorization of $f(x)$ modulo p^k for an arbitrary positive integer k.

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

We only consider $f(x)$ monic and $u(x)$ and $v(x)$ relatively prime to be monic.

$$\boxed{\deg u_k(x) = \deg u(x),\ \deg v_k(x) = \deg v(x)}$$

Hensel Lifting will produce, for any positive integer k, monic polynomials $u_k(x)$ and $v_k(x)$ in $\mathbb{Z}[x]$ satisfying

$$u_k(x) \equiv u(x) \pmod{p}, \quad v_k(x) \equiv v(x) \pmod{p},$$

and

$$f(x) \equiv u_k(x)v_k(x) \pmod{p^k}.$$

Hensel Lifting will produce, for any positive integer k, monic polynomials $u_k(x)$ and $v_k(x)$ in $\mathbb{Z}[x]$ satisfying

$$u_k(x) \equiv u(x) \pmod{p}, \quad v_k(x) \equiv v(x) \pmod{p},$$

and

$$f(x) \equiv u_k(x)v_k(x) \pmod{p^k}.$$

We start with $u_1(x) = u(x)$ and $v_1(x) = v(x)$.

Hensel Lifting will produce, for any positive integer k, monic polynomials $u_k(x)$ and $v_k(x)$ in $\mathbb{Z}[x]$ satisfying

$$u_k(x) \equiv u(x) \pmod{p}, \quad v_k(x) \equiv v(x) \pmod{p},$$

and

$$f(x) \equiv u_k(x)v_k(x) \pmod{p^k}.$$

We start with $u_1(x) = u(x)$ and $v_1(x) = v(x)$. Now, given $u_k(x)$ and $v_k(x)$, we explain how to obtain $u_{k+1}(x)$ and $v_{k+1}(x)$. Compute

$$w_k(x) \equiv \frac{1}{p^k}\left(f(x) - u_k(x)v_k(x)\right) \pmod{p}.$$

Observe that $\deg w_k(x) < \deg f(x)$ and

$$p^k w_k(x) \equiv f(x) - u_k(x)v_k(x) \pmod{p^{k+1}}.$$

We start with $u_1(x) = u(x)$ and $v_1(x) = v(x)$. Now, given $u_k(x)$ and $v_k(x)$, we explain how to obtain $u_{k+1}(x)$ and $v_{k+1}(x)$. Compute

$$w_k(x) \equiv \frac{1}{p^k}\left(f(x) - u_k(x)v_k(x)\right) \pmod{p}.$$

Observe that $\deg w_k(x) < \deg f(x)$ and

$$p^k w_k(x) \equiv f(x) - u_k(x)v_k(x) \pmod{p^{k+1}}.$$

Since $u(x)$ and $v(x)$ are relatively prime in $\mathbb{F}_p[x]$, we can find $a(x)$ and $b(x)$ in $\mathbb{F}_p[x]$ (depending on k) such that

$$a(x)u(x) + b(x)v(x) \equiv w_k(x) \pmod{p}.$$

One can take $\deg a(x) < \deg v(x)$ and $\deg b(x) < \deg u(x)$.

Set

$$u_{k+1}(x) = u_k(x) + b(x)p^k \quad \text{and} \quad v_{k+1}(x) = v_k(x) + a(x)p^k.$$

Observe that $\deg w_k(x) < \deg f(x)$ **and**

$$p^k w_k(x) \equiv f(x) - u_k(x)v_k(x) \pmod{p^{k+1}}.$$

Since $u(x)$ **and** $v(x)$ **are relatively prime in** $\mathbb{F}_p[x]$**, we can find** $a(x)$ **and** $b(x)$ **in** $\mathbb{F}_p[x]$ **(depending on** k**) such that**

$$a(x)u(x) + b(x)v(x) \equiv w_k(x) \pmod{p}.$$

One can take $\deg a(x) < \deg v(x)$ **and** $\deg b(x) < \deg u(x)$**.**

Set

$$u_{k+1}(x) = u_k(x) + b(x)p^k \quad \text{and} \quad v_{k+1}(x) = v_k(x) + a(x)p^k.$$

Observe that $\deg w_k(x) < \deg f(x)$ and

$$p^k w_k(x) \equiv f(x) - u_k(x)v_k(x) \pmod{p^{k+1}}.$$

Since $u(x)$ and $v(x)$ are relatively prime in $\mathbb{F}_p[x]$, we can find $a(x)$ and $b(x)$ in $\mathbb{F}_p[x]$ (depending on k) such that

$$a(x)u(x) + b(x)v(x) \equiv w_k(x) \pmod{p}.$$

One can take $\deg a(x) < \deg v(x)$ and $\deg b(x) < \deg u(x)$. Set

$$u_{k+1}(x) = u_k(x) + b(x)p^k \quad \text{and} \quad v_{k+1}(x) = v_k(x) + a(x)p^k.$$

Then $u_{k+1}(x)$ and $v_{k+1}(x)$ are monic and (modulo p^{k+1})

$$u_{k+1}(x)v_{k+1}(x) \equiv \big(u_k(x) + b(x)p^k\big)\big(v_k(x) + a(x)p^k\big)$$

Observe that $\deg w_k(x) < \deg f(x)$ and

$$p^k w_k(x) \equiv f(x) - u_k(x)v_k(x) \pmod{p^{k+1}}.$$

Since $u(x)$ and $v(x)$ are relatively prime in $\mathbb{F}_p[x]$, we can find $a(x)$ and $b(x)$ in $\mathbb{F}_p[x]$ (depending on k) such that

$$a(x)u(x) + b(x)v(x) \equiv w_k(x) \pmod{p}.$$

One can take $\deg a(x) < \deg v(x)$ and $\deg b(x) < \deg u(x)$. Set

$$u_{k+1}(x) = u_k(x) + b(x)p^k \quad \text{and} \quad v_{k+1}(x) = v_k(x) + a(x)p^k.$$

Then $u_{k+1}(x)$ and $v_{k+1}(x)$ are monic and (modulo p^{k+1})

$$\begin{aligned} u_{k+1}(x)v_{k+1}(x) &\equiv \big(u_k(x) + b(x)p^k\big)\big(v_k(x) + a(x)p^k\big) \\ &\equiv u_k(x)v_k(x) + p^k\big(a(x)u(x) + b(x)v(x)\big) \end{aligned}$$

Observe that $\deg w_k(x) < \deg f(x)$ and

$$p^k w_k(x) \equiv f(x) - u_k(x)v_k(x) \pmod{p^{k+1}}.$$

Since $u(x)$ and $v(x)$ are relatively prime in $\mathbb{F}_p[x]$, we can find $a(x)$ and $b(x)$ in $\mathbb{F}_p[x]$ (depending on k) such that

$$a(x)u(x) + b(x)v(x) \equiv w_k(x) \pmod{p}.$$

One can take $\deg a(x) < \deg v(x)$ and $\deg b(x) < \deg u(x)$. Set

$$u_{k+1}(x) = u_k(x) + b(x)p^k \quad \text{and} \quad v_{k+1}(x) = v_k(x) + a(x)p^k.$$

Then $u_{k+1}(x)$ and $v_{k+1}(x)$ are monic and (modulo p^{k+1})

$$\begin{aligned} u_{k+1}(x)v_{k+1}(x) &\equiv \big(u_k(x) + b(x)p^k\big)\big(v_k(x) + a(x)p^k\big) \\ &\equiv u_k(x)v_k(x) + p^k\big(a(x)u(x) + b(x)v(x)\big) \\ &\equiv u_k(x)v_k(x) + p^k w_k(x) \end{aligned}$$

Observe that $\deg w_k(x) < \deg f(x)$ **and**

$$p^k w_k(x) \equiv f(x) - u_k(x)v_k(x) \pmod{p^{k+1}}.$$

Since $u(x)$ **and** $v(x)$ **are relatively prime in** $\mathbb{F}_p[x]$, **we can find** $a(x)$ **and** $b(x)$ **in** $\mathbb{F}_p[x]$ **(depending on** k**) such that**

$$a(x)u(x) + b(x)v(x) \equiv w_k(x) \pmod{p}.$$

One can take $\deg a(x) < \deg v(x)$ **and** $\deg b(x) < \deg u(x)$. **Set**

$$u_{k+1}(x) = u_k(x) + b(x)p^k \quad \text{and} \quad v_{k+1}(x) = v_k(x) + a(x)p^k.$$

Then $u_{k+1}(x)$ **and** $v_{k+1}(x)$ **are monic and (modulo** p^{k+1}**)**

$$\begin{aligned} u_{k+1}(x)v_{k+1}(x) &\equiv \big(u_k(x) + b(x)p^k\big)\big(v_k(x) + a(x)p^k\big) \\ &\equiv u_k(x)v_k(x) + p^k\big(a(x)u(x) + b(x)v(x)\big) \\ &\equiv u_k(x)v_k(x) + p^k w_k(x) \\ &\equiv u_k(x)v_k(x) + \big(f(x) - u_k(x)v_k(x)\big) \end{aligned}$$

Observe that $\deg w_k(x) < \deg f(x)$ and

$$p^k w_k(x) \equiv f(x) - u_k(x)v_k(x) \pmod{p^{k+1}}.$$

Since $u(x)$ and $v(x)$ are relatively prime in $\mathbb{F}_p[x]$, we can find $a(x)$ and $b(x)$ in $\mathbb{F}_p[x]$ (depending on k) such that

$$a(x)u(x) + b(x)v(x) \equiv w_k(x) \pmod{p}.$$

One can take $\deg a(x) < \deg v(x)$ and $\deg b(x) < \deg u(x)$. Set

$$u_{k+1}(x) = u_k(x) + b(x)p^k \quad \text{and} \quad v_{k+1}(x) = v_k(x) + a(x)p^k.$$

Then $u_{k+1}(x)$ and $v_{k+1}(x)$ are monic and

$$\begin{aligned}
u_{k+1}(x)v_{k+1}(x) &\equiv \big(u_k(x) + b(x)p^k\big)\big(v_k(x) + a(x)p^k\big) \\
&\equiv u_k(x)v_k(x) + p^k\big(a(x)u(x) + b(x)v(x)\big) \\
&\equiv u_k(x)v_k(x) + p^k w_k(x) \\
&\equiv u_k(x)v_k(x) + \big(f(x) - u_k(x)v_k(x)\big) \\
&\equiv f(x) \pmod{p^{k+1}}.
\end{aligned}$$

Hensel Lifting

Hensel Lifting will produce, for any positive integer k, monic polynomials $u_k(x)$ and $v_k(x)$ in $\mathbb{Z}[x]$ satisfying

$$u_k(x) \equiv u(x) \pmod{p}, \quad v_k(x) \equiv v(x) \pmod{p},$$

and

$$f(x) \equiv u_k(x)v_k(x) \pmod{p^k}.$$

Comment: A complete factorization of $f(x)$ modulo p^k can be obtained from a complete factorization of $f(x)$ modulo p by modifying this idea.

Do MAPLE examples.

An Inequality of Landau

Definitions and Notations. For

$$f(x) = \sum_{j=0}^{n} a_j x^j = a_n \prod_{j=1}^{n} (x - \alpha_j),$$

with $a_n \neq 0$, we set

$$\|f\| = \left(\sum_{j=0}^{n} a_j^2 \right)^{1/2} \quad \text{and} \quad M(f) = |a_n| \prod_{j=1}^{n} \max\{1, |\alpha_j|\},$$

the latter being the Mahler measure of the polynomial $f(x)$.

An Inequality of Landau

Definitions and Notations. For

$$f(x) = \sum_{j=0}^{n} a_j x^j = a_n \prod_{j=1}^{n} (x - \alpha_j),$$

with $a_n \neq 0$, we set

$$\|f\| = \left(\sum_{j=0}^{n} a_j^2 \right)^{1/2} \quad \text{and} \quad M(f) = |a_n| \prod_{j=1}^{n} \max\{1, |\alpha_j|\},$$

the latter being the Mahler measure of the polynomial $f(x)$. We also define the reciprocal of $f(x)$ as

$$\widetilde{f}(x) = x^{\deg f} f(1/x).$$