Number Theory, Lecture 4

Polynomials, congruenses, Hensel lifting

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Summary

Summary

Definition

- p prime
- $\mathbb{Z}_p[x]$ the ring of polynomials with coefficients in $\mathbb{Z}_p$
- A general such polynomial is

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

  with $a_j \in \mathbb{Z}_p$, $a_n \neq 0$.
- $n = \deg(f(x))$.
- $\mathrm{lc}(f(x)) = a_n$, $\mathrm{lm}(f(x)) = x^n$
- The zero polynomial has degree $-\infty$

Lemma

- $\deg(fg) = \deg(f) + \deg(g)$,
- $\deg(f+g) \leq \max(\deg(f), \deg(g))$

Example

In $\mathbb{Z}_2[x]$,

- $(x^3+x+1)*(x^4+x+1) = x^7+x^4+x^3+x^5+x^2+x+x^4+x+1 = x^7+x^5+x^3+x^2+1$
- $(x^3+x+1)+(x^3+x^2+1) = x^2+x$

Evaluation

Definition

If $f(x) = \sum_{j=0}^{n} c_j x^j$, $a \in \mathbb{Z}_p$, then the evaluation of $f(x)$ at $x = a$ is

$$f(a) = \sum_{j=0}^{n} c_j a^j$$

Example

- $p = 2$
- $f(x) = 1$ (constant 1 polynomial)
- $g(x) = x^4 + x^2 + 1$
- $f(0) = f(1) = 1$
- $g(0) = g(1) = 1$
- So f and g define the same polynomial functions $\mathbb{Z}_2 \to \mathbb{Z}_2$, but they are different polynomials
- In fact, two polynomials yield same function iff they differ by polynomial multiple of $x^2 + x$

Evaluation

Definition

If $f(x) = \sum_{j=0}^{n} c_j x^j$, $a \in \mathbb{Z}_p$, then the evaluation of $f(x)$ at $x = a$ is

$$f(a) = \sum_{j=0}^{n} c_j a^j$$

Example

- $p = 2$
- $f(x) = 1$ (constant 1 polynomial)
- $g(x) = x^4 + x^2 + 1$
- $f(0) = f(1) = 1$
- $g(0) = g(1) = 1$
- So f and g define the same polynomial functions $\mathbb{Z}_2 \to \mathbb{Z}_2$, but they are different polynomials
- In fact, two polynomials yield same function iff they differ by polynomial multiple of $x^2 + x$

Evaluation

Definition

If $f(x) = \sum_{j=0}^{n} c_j x^j$, $a \in \mathbb{Z}_p$, then the evaluation of $f(x)$ at $x = a$ is

$$f(a) = \sum_{j=0}^{n} c_j a^j$$

Example

- $p = 2$
- $f(x) = 1$ (constant 1 polynomial)
- $g(x) = x^4 + x^2 + 1$
- $f(0) = f(1) = 1$
- $g(0) = g(1) = 1$
- So f and g define the same polynomial functions $\mathbb{Z}_2 \to \mathbb{Z}_2$, but they are different polynomials
- In fact, two polynomials yield same function iff they differ by polynomial multiple of $x^2 + x$

Evaluation

Definition

If $f(x) = \sum_{j=0}^n c_j x^j$, $a \in \mathbb{Z}_p$, then the evaluation of $f(x)$ at $x = a$ is

$$f(a) = \sum_{j=0}^{n} c_j a^j$$

Example

- $p = 2$
- $f(x) = 1$ (constant 1 polynomial)
- $g(x) = x^4 + x^2 + 1$
- $f(0) = f(1) = 1$
- $g(0) = g(1) = 1$
- So f and g define the same polynomial functions $\mathbb{Z}_2 \to \mathbb{Z}_2$, but they are different polynomials
- In fact, two polynomials yield same function iff they differ by polynomial multiple of $x^2 + x$

Evaluation

Definition

If $f(x) = \sum_{j=0}^{n} c_j x^j$, $a \in \mathbb{Z}_p$, then the evaluation of $f(x)$ at $x = a$ is

$$f(a) = \sum_{j=0}^{n} c_j a^j$$

Example

- $p = 2$
- $f(x) = 1$ (constant 1 polynomial)
- $g(x) = x^4 + x^2 + 1$
- $f(0) = f(1) = 1$
- $g(0) = g(1) = 1$
- So f and g define the same polynomial functions $\mathbb{Z}_2 \to \mathbb{Z}_2$, but they are different polynomials
- In fact, two polynomials yield same function iff they differ by polynomial multiple of $x^2 + x$

Evaluation

Definition

If $f(x) = \sum_{j=0}^{n} c_j x^j$, $a \in \mathbb{Z}_p$, then the evaluation of $f(x)$ at $x = a$ is

$$f(a) = \sum_{j=0}^{n} c_j a^j$$

Example

- $p = 2$
- $f(x) = 1$ (constant 1 polynomial)
- $g(x) = x^4 + x^2 + 1$
- $f(0) = f(1) = 1$
- $g(0) = g(1) = 1$
- So f and g define the same polynomial functions $\mathbb{Z}_2 \to \mathbb{Z}_2$, but they are different polynomials
- In fact, two polynomials yield same function iff they differ by polynomial multiple of $x^2 + x$

Evaluation

Definition

If $f(x) = \sum_{j=0}^{n} c_j x^j$, $a \in \mathbb{Z}_p$, then the evaluation of $f(x)$ at $x = a$ is

$$f(a) = \sum_{j=0}^{n} c_j a^j$$

Example

- $p = 2$
- $f(x) = 1$ (constant 1 polynomial)
- $g(x) = x^4 + x^2 + 1$
- $f(0) = f(1) = 1$
- $g(0) = g(1) = 1$
- So f and g define the same polynomial functions $\mathbb{Z}_2 \to \mathbb{Z}_2$, but they are different polynomials
- In fact, two polynomials yield same function iff they differ by polynomial multiple of $x^2 + x$

Theorem (Division algorithm)

Let $f(x), g(x) \in \mathbb{Z}_p[x]$, $g(x)$ not z.p. Then exists unique $k(x), r(x) \in \mathbb{Z}_p[x]$,

$$f(x) = k(x)g(x) + r(x), \qquad \deg(r(x)) < \deg(g(x)) \tag{*}$$

Proof.

WLOG $n = \deg(f(x)) \geq \deg(g(x)) = m$. Put

$$f = a_n x^n + \tilde{f}, \quad g = b_m x^m + \tilde{g}$$

and put

$$f_2 = f - \frac{a_n}{b_m} x^{n-m} g.$$

Then $\deg(f_2) < \deg(f)$, proceed by induction. □

Works for coefficients in any field (e.g. $\mathbb{Q}, \mathbb{R}$) but not for $\mathbb{Z}$.

Example

- $p = 2$
- $f(x) = x^5 + x^2 + x + 1$, $g(x) = x^2 + x$
- $$\begin{aligned} f &= x^3 g + (f - x^3 g) \\ &= x^3 g + (x^4 + x^2 + x + 1) \\ &= (x^3 + x^2) g + (x^4 + x^2 + x + 1 - x^2 g) \\ &= (x^3 + x^2) g + (x^3 + x^2 + x + 1) \\ &= (x^3 + x^2 + x) g + (x^3 + x^2 + x + 1 - x g) \\ &= (x^3 + x^2 + x) g + (x^2 + 1) \\ &= (x^3 + x^2 + x + 1) g + (x^2 + 1 - g) \\ &= (x^3 + x^2 + x + 1) g + (x + 1) \end{aligned}$$

Theorem (Factor theorem)

$f(x) \in \mathbb{Z}_p[x]$, $a \in \mathbb{Z}_p$. Then $f(a) = 0$ iff $f(x) = k(x)(x-a)$ for some $k(x)$, i.e., the remainder when divided by $(x-a)$ is zero.

Proof.

If $f(x) = k(x)(x-a)$, then $\mathrm{RHS}(a) = 0$, so $f(a) = 0$.
If $f(a) = 0$, perform division with remainder:

$$f(x) = k(x)(x-a) + r(x), \quad \deg(r(x)) < \deg((x-a)) = 1$$

So $r(x) = r$, a constant. Evaluate at a:

$$0 = f(a) = k(a)(a-a) + r$$

hence $r = 0$. □

Theorem (Lagrange)

$f(x) \in \mathbb{Z}_p[x]$, $\deg(f(x)) = n$. *Then $f(x)$ has at most n zeroes in $\mathbb{Z}_p$.*

Proof.

If $a \in \mathbb{Z}_p$, $f(a) = 0$, then $f(x) = (x-a)g(x)$. If $f(b) = 0$, $b \neq a$, then $(0 = (b-a)g(b)$, and $g(b) = 0$. Since $\deg(g(x) = n-1 < n$ and $g(x)$ contains the remaining zeroes of $f(x)$, proceed by induction. □

Example

$f(x) = [2]_4 x + [2]_4 \in \mathbb{Z}_4[x]$ has $f([1]_4) = [2]_4 + [2]_4 = [0]_4$,
$f([3]_4) = [6]_4 + [2]_4 = [0]_4$.

Application: Wilson's theorem

Theorem (Wilson)

p prime. Then $(p-1)! \equiv -1 \mod p$.

Proof

$p = 2$: OK.

$p > 2$: Put $f(x) = x^{p-1} - 1$. Fermat: $f(k) \equiv 0 \mod p$ for $k \in \{1, 2, \ldots, p-1\}$.

$p - 1$ roots in $\mathbb{Z}_p[x]$. Lagrange: no more roots.

Factor thm:

$$f(x) = (x-1)q(x) \in \mathbb{Z}_p[x],$$

remaining roots in $q(x)$, so

$$q(k) \equiv 0 \mod p, \qquad k \in \{2, 3, \ldots, p-1\}$$

Proof.

Follows that

$$f(x) = (x-1)(x-2)\cdots(x-(p-1)) \in \mathbb{Z}_p[x]$$

Evaluate at zero:

$$f(0) = (-1)(-2)\cdots(-(p-1)) = (-1)^{p-1}(p-1)!$$

In other words

$$0^{p-1} - 1 \equiv (-1)^{p-1}(p-1)! \mod p$$

But p is odd. □

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, p prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod p^{r+1}, different reps if $0 \le t \le p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some t
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, p prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod p^{r+1}, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some t
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, p prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod p^{r+1}, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some t
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, p prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod p^{r+1}, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some t
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, p prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod p^{r+1}, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some t
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, p prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod p^{r+1}, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some t
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, p prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod p^{r+1}, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some t
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, p prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod p^{r+1}, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some t
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, p prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod p^{r+1}, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some t
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, p prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod p^{r+1}, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some t
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, p prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod p^{r+1}, different reps if $0 \leq t \leq p - 1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some t
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

implies $f(c) \equiv 0 \mod mn$ (CRT)

- $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- $m, n, r \in \mathbb{P}$, $c \in \mathbb{Z}$, p prime
- $f(c) = 0$ implies $f(x) \equiv 0 \mod m$, not conversely
- $f(c) \equiv 0 \mod mn$ implies $f(x) \equiv 0 \mod m$, not conversely
- "Lifting":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ but not (always) mod p^{r+1}, different reps if $0 \leq t \leq p-1$
  - Maybe $f(c + tp^r) \equiv 0 \mod p^{r+1}$ for some t
- "Combining":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  implies $f(c) \equiv 0 \mod mn$ (CRT)

Example

$$x^2 + x + 5 \equiv 0 \mod 77$$

Modulo 7:
$0 \equiv x^2 - 6x + 5 \equiv (x-3)^2 - 9 + 5 \equiv (x-3)^2 - 4 \equiv (x-3+2)(x-3-2) \equiv (x-1)(x-5)$
Modulo 11: $0 \equiv x^2 - 10x + 5 \equiv (x-5)^2 - 25 + 5 \equiv (x-5)^2 - 9 \equiv (x-5+3)(x-5-3) \equiv (x-2)(x-8)$
Combine using CRT:

$$\left.\begin{aligned} x &\equiv 1 \mod 7 \\ x &\equiv 2 \mod 11 \end{aligned}\right\} \iff x \equiv 57 \mod 77$$

Three more solutions, find them as exercise!

Example

$f(x) = x^2 + x + 5$, find roots modulo 7^2.

Note: if $f(a) \equiv 0 \mod 49$, then $f(a) \equiv 0 \mod 7$, but not necessarily conversely.

Roots modulo 7: 1,5. Can we "lift" them to roots modulo 49?

$a \equiv 1 \mod 7$ gives $a = 1 + 7s$. So the "lifts" are $1, 8, 15, 22, 29, 36, 43$. Is one of them a zero modulo 49?

$f(a) = a^2 + a + 5 \equiv (1 + 7s)^2 + (1 + 7s) + 5 \equiv 1 + 14s + 49s^2 + 1 + 7s + 5 \mod 7^2$, so

$$f(a) \equiv 21s + 7 \mod 49$$

For zero, solve

Example (cont)

$$
\begin{aligned}
21s &\equiv -7 \mod 49 \\
3s &\equiv -1 \mod 7 \\
s &\equiv 2 \mod 7
\end{aligned}
$$

hence

$$a = 1 + 7s \equiv 1 + 7 * 2 \equiv 15 \mod 49$$

Computer check:

```
R.<t> = Integers(49)[]
f=t^2+t+5
```

finds

$$f(15) = \textbf{??}$$

Example (cont)

Is it the only root?

```
myroots=f.roots(multiplicities=False)
```

finds

$$\mathtt{myroots} = \mathbf{??}$$

Aha, so the "lift" of the root $x \equiv 5 \mod 7$ that works is $x = 5 + 7 * 4$.

Definition

- $f(x) = \sum_j a_j x^j \in K[x]$
- K some field (or $\mathbb{Z}$)
- The formal derivate is $f'(x) = \sum_j j a_j x^{j-1}$

Lemma

$f(x+y) \in K[x,y]$, the polynomial ring with two variables, and

$$f(x+y) = f(x) + f'(x)y + g(x,y)y^2 \tag{1}$$

for some $g(x,y) \in K[x,y]$

Example

$f(x) = x^3 - x + 2$, $f'(x) = 3x^2 - 1$, $f(x+y) = (x+y)^3 - (x+y) + 2 = x^3 + 3x^2y + 3xy^2 + y^3 - x - y + 2 = (x^3 - x + 2) + (3x^2 - 1)y + 3xy^2 + y^3$

Proof.

Binomial thm:

$$(x+y)^j = x^j + jx^{j-1}y + \binom{j}{2}x^{j-2}y^2 + \cdots + y^j = x^j + jx^{j-1}y + y^2 g_j(x,y)$$

Hence:

$$\begin{aligned} f(x+y) &= \sum_j a_j(x+y)^j \\ &= a_0 + \sum_{j>0} a_j(x^j + jx^{j-1}y + g_j(x,y)y^2) \qquad \text{Binomial thm} \\ &= a_0 + \sum_{j>0} a_j x^j + y\sum_{j>0} a_j j x^{j-1} + y^2 \sum_{j>0} a_j g_j(x,y) \\ &= f(x) + yf'(x) + g(x,y)y^2 \end{aligned}$$

□

- p prime
- $f(x) \in \mathbb{Z}[x]$
- $c \in \mathbb{Z}$, $f(c) \equiv 0 \mod p^r$
- Substitute $x = c$, $y = p^r s$ in $f(x+y) = f(x) + f'(x)y + g(x,y)y^2$
- Get $f(c + sp^r) = f(c) + f'(c)p^r s + g * (p^r s)^2$, hence

$$f(c + sp^r) \equiv f(c) + f'(c)p^r s \mod p^{r+1}$$

- If $f'(c) \not\equiv 0 \mod p$ then $f'(c) \not\equiv 0 \mod p^{r+1}$ and we can solve

$$(f'(c)p^r)s \equiv -f(c) \mod p^{r+1}$$

uniquely. Divide by p^r to get

$$f'(c)s \equiv \frac{-f(c)}{p^r} \mod p$$

- p prime
- $f(x) \in \mathbb{Z}[x]$
- $c \in \mathbb{Z}$, $f(c) \equiv 0 \mod p^r$
- Substitute $x = c$, $y = p^r s$ in $f(x+y) = f(x) + f'(x)y + g(x,y)y^2$
- Get $f(c + sp^r) = f(c) + f'(c)p^r s + g * (p^r s)^2$, hence
$$f(c + sp^r) \equiv f(c) + f'(c)p^r s \mod p^{r+1}$$
- If $f'(c) \not\equiv 0 \mod p$ then $f'(c) \not\equiv 0 \mod p^{r+1}$ and we can solve
$$(f'(c)p^r)s \equiv -f(c) \mod p^{r+1}$$
uniquely. Divide by p^r to get
$$f'(c)s \equiv \frac{-f(c)}{p^r} \mod p$$

- p prime
- $f(x) \in \mathbb{Z}[x]$
- $c \in \mathbb{Z}$, $f(c) \equiv 0 \mod p^r$
- Substitute $x = c$, $y = p^r s$ in $f(x+y) = f(x) + f'(x)y + g(x,y)y^2$
- Get $f(c + sp^r) = f(c) + f'(c)p^r s + g * (p^r s)^2$, hence

$$f(c + sp^r) \equiv f(c) + f'(c)p^r s \mod p^{r+1}$$

- If $f'(c) \not\equiv 0 \mod p$ then $f'(c) \not\equiv 0 \mod p^{r+1}$ and we can solve

$$(f'(c)p^r)s \equiv -f(c) \mod p^{r+1}$$

uniquely. Divide by p^r to get

$$f'(c)s \equiv \frac{-f(c)}{p^r} \mod p$$

- p prime
- $f(x) \in \mathbb{Z}[x]$
- $c \in \mathbb{Z}$, $f(c) \equiv 0 \mod p^r$
- Substitute $x = c$, $y = p^r s$ in $f(x+y) = f(x) + f'(x)y + g(x,y)y^2$
- Get $f(c + sp^r) = f(c) + f'(c)p^r s + g * (p^r s)^2$, hence

$$f(c + sp^r) \equiv f(c) + f'(c)p^r s \mod p^{r+1}$$

- If $f'(c) \not\equiv 0 \mod p$ then $f'(c) \not\equiv 0 \mod p^{r+1}$ and we can solve

$$(f'(c)p^r)s \equiv -f(c) \mod p^{r+1}$$

uniquely. Divide by p^r to get

$$f'(c)s \equiv \frac{-f(c)}{p^r} \mod p$$

- p prime
- $f(x) \in \mathbb{Z}[x]$
- $c \in \mathbb{Z}$, $f(c) \equiv 0 \mod p^r$
- Substitute $x = c$, $y = p^r s$ in $f(x+y) = f(x) + f'(x)y + g(x,y)y^2$
- Get $f(c+sp^r) = f(c) + f'(c)p^r s + g * (p^r s)^2$, hence

$$f(c+sp^r) \equiv f(c) + f'(c)p^r s \mod p^{r+1}$$

- If $f'(c) \not\equiv 0 \mod p$ then $f'(c) \not\equiv 0 \mod p^{r+1}$ and we can solve

$$(f'(c)p^r)s \equiv -f(c) \mod p^{r+1}$$

uniquely. Divide by p^r to get

$$f'(c)s \equiv \frac{-f(c)}{p^r} \mod p$$

- p prime
- $f(x) \in \mathbb{Z}[x]$
- $c \in \mathbb{Z}$, $f(c) \equiv 0 \mod p^r$
- Substitute $x = c$, $y = p^r s$ in $f(x+y) = f(x) + f'(x)y + g(x,y)y^2$
- Get $f(c + sp^r) = f(c) + f'(c)p^r s + g * (p^r s)^2$, hence

$$f(c + sp^r) \equiv f(c) + f'(c)p^r s \mod p^{r+1}$$

- If $f'(c) \not\equiv 0 \mod p$ then $f'(c) \not\equiv 0 \mod p^{r+1}$ and we can solve

$$(f'(c)p^r)s \equiv -f(c) \mod p^{r+1}$$

uniquely. Divide by p^r to get

$$f'(c)s \equiv \frac{-f(c)}{p^r} \mod p$$

Lemma (Hensel's lemma)

1. *p prime*
2. $f(x) \in \mathbb{Z}[x]$
3. $f(c) \equiv 0 \mod p^j$
4. $f'(c) \not\equiv 0 \mod p$

Then there is a unique t (mod p) such that

$$f(c + tp^j) \equiv 0 \mod p^{j+1}$$

This t is the unique solution to

$$tf'(c) \equiv \frac{-f(c)}{p^j} \mod p$$

Lemma (Hensel's lemma)

1. *p prime*
2. $f(x) \in \mathbb{Z}[x]$
3. $f(c) \equiv 0 \mod p$
4. $f'(c) \not\equiv 0 \mod p$

Then exists $c_2, c_3, c_4, \ldots$ such that

1. $c_j \equiv c \mod p$ *(it is a lift)*
2. $c_j \equiv c_{j-1} \mod p^{j-1}$ *(it is a lift)*
3. $f(c_j) \equiv 0 \mod p^j$ *(it is a solution mod p^j*
4. c_j *is unique mod p^j*

- Lift c_j to c_{j+1} by putting $c_{j+1} = c_j + tp^j$, solve for t mod p^{j+1}
- If $f'(c) \equiv 0 \mod p$ then first lift either non-existent or non-unique

Example

- $p = 5$
- $f(x) = x^3 + 2$
- f has no zeroes in $\mathbb{Z}$ or $\mathbb{Q}$, but one in $\mathbb{R}$, and 3 zeroes in $\mathbb{C}$
- $f(2) \equiv 0 \mod 5$
- $f'(x) = 3x^2$, $f'(2) = 12 \not\equiv 0 \mod 5$
- Hensel: lifts uniquely to all powers of 5
- **??**

Example

- $p = 3$
- $f(x) = x^3 + 2$
- $f(1) \equiv 0 \mod 3$
- $f'(x) = 3x^2$, $f'(1) = 3 \equiv 0 \mod 3$
- Hensel: if it lifts, it lifts not uniquely
- In fact no soln modulo 9

Example

- $p = 3$
- $f(x) = \textbf{??}$
- $f(2) = \textbf{??} \equiv 0 \mod 3$
- $f'(x) = \textbf{??}$
- $f'(2) = \textbf{??} \equiv 0 \mod 3$
- Hensel: if it lifts, it lifts not uniquely
- In fact lifts in variegated ways:

moduli	roots
3	**??**
3^2	**??**
3^3	**??**
3^4	**??**

- Not a contradiction to Lagrange

Example

- Let's do the first lift "by hand"
- $0 \equiv f(2+3t) \equiv f(2) + f'(2)3t \mod 9$
- $f(2)$ happens to be 0 mod 9
- $f'(2) \equiv 3 \mod 9$
- $3 * 3 * t \equiv 0 \mod 9$, t is "whatever"
- $2 + 0 * 3$, $2 + 1 * 3$, $2 + 2 * 3$ all valid lifts

Exercise from Hackman

- $a \in Z$ has inverse b mod p^n, so $ab \equiv 1 \mod p^n$
- Then $ab \equiv 1 \mod p$, so $a, b \not\equiv 0 \mod p$
- Want to lift b to inverse mod p^{n+1}
- $f(x) = ax - 1$, $f(b) \equiv 0 \mod p^n$, $f'(b) = ab \not\equiv 0 \mod p$
- $f(b + tp^n) \equiv f(b) + f'(b)tp^n \equiv ab - 1 + abtp^n \equiv 0 \mod p^{n+1}$
- Divide by p^n
- $\frac{ab-1}{p^n} + abt \equiv \frac{ab-1}{p^n} + t \equiv 0 \mod p$

Example

- $7 * 3 = 21 \equiv 1 \mod 5$
- Lift 3 to inverse of 7 mod 25
- $b = 3 + 5t$, $7b \equiv 1 \mod 25$
- $7 * 3 + 35t \equiv 1 \mod 25$
- $7 * 3 - 1 + 35t \equiv 0 \mod 25$
- $20/5 + 7t \equiv 0 \mod 5$
- $t \equiv 3 \mod 5$
- $b \equiv 18 \mod 25$