

Talteori, Föreläsning 4

Polynom, kongruenser, Hensel-lyft

Jan Snellman¹

¹Matematiska Institutionen
Linköpings Universitet

Föreläsningsanteckningar på kurshemsidan <http://courses.mai.liu.se/GU/TATA54/>



TEKNISKA HÖGSKOLAN
LINKÖPING UNIVERSITET

Polynom med koefficienter i \mathbb{Z}_p

Definition, grad

Divisionsalgoritmen

Lagrange

Wilson's theorem

Hensel-lyft

Polynomiella kongruenser

Polynomiella kongruenser modulo

primpotens

Formell derivata

Hensels lemma

Faktorisering

Tillämpning: inverser

Definition

- ▶ p primtal
- ▶ $\mathbb{Z}_p[x]$ ringen av polynom med koefficienter i \mathbb{Z}_p
- ▶ Allmänt sådant

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

med $a_j \in \mathbb{Z}_p$, $a_n \neq 0$.

- ▶ $n = \deg(f(x))$.
- ▶ $\text{lc}(f(x)) = a_n$, $\text{lm}(f(x)) = x^n$
- ▶ Nollpolynomet har grad $-\infty$

Lemma

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

Exempel

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

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

Definition

Om $f(x) = \sum_{j=0}^n c_j x^j$, $a \in \mathbb{Z}_p$, så är evalueringen av $f(x)$ vid $x = a$ definierad som

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

Exempel

- ▶ $p = 2$
 - ▶ $f(x) = 1$ (konstant polynom)
 - ▶ $g(x) = x^4 + x^2 + 1$
 - ▶ $f(0) = f(1) = 1$
 - ▶ $g(0) = g(1) = 1$
 - ▶ Så f och g definierar samma
- polynomiella funktion $\mathbb{Z}_2 \rightarrow \mathbb{Z}_2$, men är olika som polynom
- ▶ Två polynom ger samma funktion om de skiljer sig åt med en polynomiell multipel av $x^2 + x$

Definition

Om $f(x) = \sum_{j=0}^n c_j x^j$, $a \in \mathbb{Z}_p$, så är evalueringen av $f(x)$ vid $x = a$ definierad som

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

Exempel

- ▶ $p = 2$
- ▶ $f(x) = 1$ (konstant polynom)
- ▶ $g(x) = x^4 + x^2 + 1$
- ▶ $f(0) = f(1) = 1$
- ▶ $g(0) = g(1) = 1$
- ▶ Så f och g definierar samma

- polynomiella funktion $\mathbb{Z}_2 \rightarrow \mathbb{Z}_2$, men är olika som polynom
- ▶ Två polynom ger samma funktion om de skiljer sig åt med en polynomiell multipel av $x^2 + x$

Definition

Om $f(x) = \sum_{j=0}^n c_j x^j$, $a \in \mathbb{Z}_p$, så är evalueringen av $f(x)$ vid $x = a$ definierad som

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

Exempel

- ▶ $p = 2$
- ▶ $f(x) = 1$ (konstant polynom)
- ▶ $g(x) = x^4 + x^2 + 1$
- ▶ $f(0) = f(1) = 1$
- ▶ $g(0) = g(1) = 1$
- ▶ Så f och g definierar samma

- polynomiella funktion $\mathbb{Z}_2 \rightarrow \mathbb{Z}_2$, men är olika som polynom
- ▶ Två polynom ger samma funktion om de skiljer sig åt med en polynomiell multipel av $x^2 + x$

Definition

Om $f(x) = \sum_{j=0}^n c_j x^j$, $a \in \mathbb{Z}_p$, så är evalueringen av $f(x)$ vid $x = a$ definierad som

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

Exempel

- ▶ $p = 2$
- ▶ $f(x) = 1$ (konstant polynom)
- ▶ $g(x) = x^4 + x^2 + 1$
- ▶ $f(0) = f(1) = 1$
- ▶ $g(0) = g(1) = 1$
- ▶ Så f och g definierar samma

- polynomiella funktion $\mathbb{Z}_2 \rightarrow \mathbb{Z}_2$, men är olika som polynom
- ▶ Två polynom ger samma funktion om de skiljer sig åt med en polynomiell multipel av $x^2 + x$

Definition

Om $f(x) = \sum_{j=0}^n c_j x^j$, $a \in \mathbb{Z}_p$, så är evalueringen av $f(x)$ vid $x = a$ definierad som

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

Exempel

- ▶ $p = 2$
- ▶ $f(x) = 1$ (konstant polynom)
- ▶ $g(x) = x^4 + x^2 + 1$
- ▶ $f(0) = f(1) = 1$
- ▶ $g(0) = g(1) = 1$
- ▶ Så f och g definierar samma

- polynomiella funktion $\mathbb{Z}_2 \rightarrow \mathbb{Z}_2$, men är olika som polynom
- ▶ Två polynom ger samma funktion omm de skiljer sig åt med en polynomiell multipel av $x^2 + x$

Definition

Om $f(x) = \sum_{j=0}^n c_j x^j$, $a \in \mathbb{Z}_p$, så är evalueringen av $f(x)$ vid $x = a$ definierad som

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

Exempel

- ▶ $p = 2$
- ▶ $f(x) = 1$ (konstant polynom)
- ▶ $g(x) = x^4 + x^2 + 1$
- ▶ $f(0) = f(1) = 1$
- ▶ $g(0) = g(1) = 1$
- ▶ Så f och g definierar samma

- polynomiella funktion $\mathbb{Z}_2 \rightarrow \mathbb{Z}_2$, men är olika som polynom
- ▶ Två polynom ger samma funktion om de skiljer sig åt med en polynomiell multipel av $x^2 + x$

Definition

Om $f(x) = \sum_{j=0}^n c_j x^j$, $a \in \mathbb{Z}_p$, så är evalueringen av $f(x)$ vid $x = a$ definierad som

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

Exempel

- ▶ $p = 2$
- ▶ $f(x) = 1$ (konstant polynom)
- ▶ $g(x) = x^4 + x^2 + 1$
- ▶ $f(0) = f(1) = 1$
- ▶ $g(0) = g(1) = 1$
- ▶ Så f och g definierar samma

- polynomiella funktion $\mathbb{Z}_2 \rightarrow \mathbb{Z}_2$, men är olika som polynom
- ▶ Två polynom ger samma funktion om de skiljer sig åt med en polynomiell multipel av $x^2 + x$

Teorem (Divisionsalgoritmen)

Antag $f(x), g(x) \in \mathbb{Z}_p[x]$, $g(x)$ ej nollpolynom. De finns unika $k(x), r(x) \in \mathbb{Z}_p[x]$,

$$f(x) = k(x)g(x) + r(x), \quad \deg(r(x)) < \deg(g(x)) \quad (*)$$

Bevis.

Kan anta $n = \deg(f(x)) \geq \deg(g(x)) = m$. Sätt

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

och sätt

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

Då $\deg(f_2) < \deg(f)$, fortsätt med induktion. □

Beviset fungerar för koefficienter i en godtycklig kropp (e.g. \mathbb{Q}, \mathbb{R}) men inte för \mathbb{Z} .

Exempel

- ▶ $p = 2$
- ▶ $f(x) = x^5 + x^2 + x + 1$, $g(x) = x^2 + x$
- ▶

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

Teorem (Faktorsatsen)

$f(x) \in \mathbb{Z}_p[x]$, $a \in \mathbb{Z}_p$. Då $f(a) = 0$ omm $f(x) = k(x)(x - a)$ för något $k(x)$, i.e., resten vid division med $(x - a)$ är noll.

Bevis.

Om $f(x) = k(x)(x - a)$, så $\text{RHS}(a) = 0$, så $f(a) = 0$.

Om $f(a) = 0$, utför division med rest:

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

Så $r(x) = r$, en konstant. Evaluera vid $x = a$:

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

varför $r = 0$.



Teorem (Lagrange)

$f(x) \in \mathbb{Z}_p[x]$, $\deg(f(x)) = n$. Då har $f(x)$ högst n nollställen i \mathbb{Z}_p .

Bevis.

Om $a \in \mathbb{Z}_p$, $f(a) = 0$, så $f(x) = (x - a)g(x)$. Om $f(b) = 0$, $b \neq a$, så $0 = (b - a)g(b)$, och $g(b) = 0$. Eftersom $\deg(g(x)) = n - 1 < n$ och $g(x)$ innehåller de återstående nollställena till $f(x)$, följer utsagan med induktion. \square

Exempel

$f(x) = [2]_4x + [2]_4 \in \mathbb{Z}_4[x]$ men $f([1]_4) = [2]_4 + [2]_4 = [0]_4$,
 $f([3]_4) = [6]_4 + [2]_4 = [0]_4$. Vad är det för fel på \mathbb{Z}_4 ?

Teorem (Wilson)

p primtal. Då $(p - 1)! \equiv -1 \pmod{p}$.

Bevis

$p = 2$: OK.

$p > 2$: Sätt $f(x) = x^{p-1} - 1$. Fermat: $f(k) \equiv 0 \pmod{p}$ för $k \in \{1, 2, \dots, p-1\}$.

$p - 1$ nollställen in $\mathbb{Z}_p[x]$. Lagrange: inga fler nollställen.

Faktorsatsen:

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

återstående nollställen i $q(x)$, så

$$q(k) \equiv 0 \pmod{p}, \quad k \in \{2, 3, \dots, p-1\}$$

Bevis.

Det följer att

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

Evaluera vid $x = 0$:

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

Med andra ord,

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

Men p är udda, så $(-1)^{p-1} = 1$.



- ▶ $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- ▶ $m, n, r \in \mathbb{Z}_+, c \in \mathbb{Z}, p$ primtal
- ▶ $f(c) = 0$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ $f(c) \equiv 0 \pmod{mn}$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ “Lyft”:
 - ▶ $f(c) \equiv 0 \pmod{p^r}$
 - ▶ $c \equiv c + tp^r \pmod{p^r}$ men inte $\pmod{p^{r+1}}$ för $1 \leq t \leq p-1$, olika
 - ▶ Kanske $f(c + tp^r) \equiv 0 \pmod{p^{r+1}}$ för något t
- ▶ “Kombinera”:
 - ▶ $\gcd(m, n) = 1$
 - ▶ $f(c) \equiv 0 \pmod{m}$
 - ▶ $f(c) \equiv 0 \pmod{n}$
 medför $f(c) \equiv 0 \pmod{mn}$ (Kinesiska Restsatsen)

- ▶ $f(x) = a_\ell x^\ell + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$
- ▶ $m, n, r \in \mathbb{Z}_+, c \in \mathbb{Z}, p$ primtal
- ▶ $f(c) = 0$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ $f(c) \equiv 0 \pmod{mn}$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ “Lyft” :
 - ▶ $f(c) \equiv 0 \pmod{p^r}$
 - ▶ $c \equiv c + tp^r \pmod{p^r}$ men inte $\pmod{p^{r+1}}$ för $1 \leq t \leq p-1$, olika
 - ▶ Kanske $f(c + tp^r) \equiv 0 \pmod{p^{r+1}}$ för något t
- ▶ “Kombinera” :
 - ▶ $\gcd(m, n) = 1$
 - ▶ $f(c) \equiv 0 \pmod{m}$
 - ▶ $f(c) \equiv 0 \pmod{n}$
 medför $f(c) \equiv 0 \pmod{mn}$ (Kinesiska Restsatsen)

- ▶ $f(x) = a_\ell x^\ell + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$
- ▶ $m, n, r \in \mathbb{Z}_+, c \in \mathbb{Z}, p$ primtal
- ▶ $f(c) = 0$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ $f(c) \equiv 0 \pmod{mn}$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ “Lyft”:
 - ▶ $f(c) \equiv 0 \pmod{p^r}$
 - ▶ $c \equiv c + tp^r \pmod{p^r}$ men inte $\pmod{p^{r+1}}$ för $1 \leq t \leq p-1$, olika
 - ▶ Kanske $f(c + tp^r) \equiv 0 \pmod{p^{r+1}}$ för något t
- ▶ “Kombinera”:
 - ▶ $\gcd(m, n) = 1$
 - ▶ $f(c) \equiv 0 \pmod{m}$
 - ▶ $f(c) \equiv 0 \pmod{n}$
 medför $f(c) \equiv 0 \pmod{mn}$ (Kinesiska Restsatsen)

- ▶ $f(x) = a_\ell x^\ell + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$
- ▶ $m, n, r \in \mathbb{Z}_+, c \in \mathbb{Z}, p$ primtal
- ▶ $f(c) = 0$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ $f(c) \equiv 0 \pmod{mn}$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ “Lyft”:
 - ▶ $f(c) \equiv 0 \pmod{p^r}$
 - ▶ $c \equiv c + tp^r \pmod{p^r}$ men inte $\pmod{p^{r+1}}$ för $1 \leq t \leq p-1$, olika
 - ▶ Kanske $f(c + tp^r) \equiv 0 \pmod{p^{r+1}}$ för något t
- ▶ “Kombinera”:
 - ▶ $\gcd(m, n) = 1$
 - ▶ $f(c) \equiv 0 \pmod{m}$
 - ▶ $f(c) \equiv 0 \pmod{n}$
 medför $f(c) \equiv 0 \pmod{mn}$ (Kinesiska Restsatsen)

- ▶ $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- ▶ $m, n, r \in \mathbb{Z}_+, c \in \mathbb{Z}, p$ primtal
- ▶ $f(c) = 0$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ $f(c) \equiv 0 \pmod{mn}$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ “Lyft”:
 - ▶ $f(c) \equiv 0 \pmod{p^r}$
 - ▶ $c \equiv c + tp^r \pmod{p^r}$ men inte $\pmod{p^{r+1}}$ för $1 \leq t \leq p-1$, olika
 - ▶ Kanske $f(c + tp^r) \equiv 0 \pmod{p^{r+1}}$ för något t
- ▶ “Kombinera”:
 - ▶ $\gcd(m, n) = 1$
 - ▶ $f(c) \equiv 0 \pmod{m}$
 - ▶ $f(c) \equiv 0 \pmod{n}$
 medför $f(c) \equiv 0 \pmod{mn}$ (Kinesiska Restsatsen)

- ▶ $f(x) = a_\ell x^\ell + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$
- ▶ $m, n, r \in \mathbb{Z}_+, c \in \mathbb{Z}, p$ primtal
- ▶ $f(c) = 0$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ $f(c) \equiv 0 \pmod{mn}$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ “Lyft”:
 - ▶ $f(c) \equiv 0 \pmod{p^r}$
 - ▶ $c \equiv c + tp^r \pmod{p^r}$ men inte $\pmod{p^{r+1}}$ för $1 \leq t \leq p-1$, olika
 - ▶ Kanske $f(c + tp^r) \equiv 0 \pmod{p^{r+1}}$ för något t
- ▶ “Kombinera”:
 - ▶ $\gcd(m, n) = 1$
 - ▶ $f(c) \equiv 0 \pmod{m}$
 - ▶ $f(c) \equiv 0 \pmod{n}$
 medför $f(c) \equiv 0 \pmod{mn}$ (Kinesiska Restsatsen)

- ▶ $f(x) = a_\ell x^\ell + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$
- ▶ $m, n, r \in \mathbb{Z}_+, c \in \mathbb{Z}, p$ primtal
- ▶ $f(c) = 0$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ $f(c) \equiv 0 \pmod{mn}$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ “Lyft”:
 - ▶ $f(c) \equiv 0 \pmod{p^r}$
 - ▶ $c \equiv c + tp^r \pmod{p^r}$ men inte $\pmod{p^{r+1}}$ för $1 \leq t \leq p - 1$, olika
 - ▶ Kanske $f(c + tp^r) \equiv 0 \pmod{p^{r+1}}$ för något t
- ▶ “Kombinera”:
 - ▶ $\gcd(m, n) = 1$
 - ▶ $f(c) \equiv 0 \pmod{m}$
 - ▶ $f(c) \equiv 0 \pmod{n}$
 medför $f(c) \equiv 0 \pmod{mn}$ (Kinesiska Restsatsen)

- ▶ $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- ▶ $m, n, r \in \mathbb{Z}_+, c \in \mathbb{Z}, p$ primtal
- ▶ $f(c) = 0$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ $f(c) \equiv 0 \pmod{mn}$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ “Lyft”:
 - ▶ $f(c) \equiv 0 \pmod{p^r}$
 - ▶ $c \equiv c + tp^r \pmod{p^r}$ men inte $\pmod{p^{r+1}}$ för $1 \leq t \leq p - 1$, olika
 - ▶ Kanske $f(c + tp^r) \equiv 0 \pmod{p^{r+1}}$ för något t
- ▶ “Kombinera”:
 - ▶ $\gcd(m, n) = 1$
 - ▶ $f(c) \equiv 0 \pmod{m}$
 - ▶ $f(c) \equiv 0 \pmod{n}$
 medför $f(c) \equiv 0 \pmod{mn}$ (Kinesiska Restsatsen)

- ▶ $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- ▶ $m, n, r \in \mathbb{Z}_+, c \in \mathbb{Z}, p$ primtal
- ▶ $f(c) = 0$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ $f(c) \equiv 0 \pmod{mn}$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ “Lyft”:
 - ▶ $f(c) \equiv 0 \pmod{p^r}$
 - ▶ $c \equiv c + tp^r \pmod{p^r}$ men inte $\pmod{p^{r+1}}$ för $1 \leq t \leq p - 1$, olika
 - ▶ Kanske $f(c + tp^r) \equiv 0 \pmod{p^{r+1}}$ för något t
- ▶ “Kombinera”:
 - ▶ $\gcd(m, n) = 1$
 - ▶ $f(c) \equiv 0 \pmod{m}$
 - ▶ $f(c) \equiv 0 \pmod{n}$
 medför $f(c) \equiv 0 \pmod{mn}$ (Kinesiska Restsatsen)

- ▶ $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- ▶ $m, n, r \in \mathbb{Z}_+, c \in \mathbb{Z}, p$ primtal
- ▶ $f(c) = 0$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ $f(c) \equiv 0 \pmod{mn}$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ “Lyft”:
 - ▶ $f(c) \equiv 0 \pmod{p^r}$
 - ▶ $c \equiv c + tp^r \pmod{p^r}$ men inte $\pmod{p^{r+1}}$ för $1 \leq t \leq p - 1$, olika
 - ▶ Kanske $f(c + tp^r) \equiv 0 \pmod{p^{r+1}}$ för något t
- ▶ “Kombinera”:
 - ▶ $\gcd(m, n) = 1$
 - ▶ $f(c) \equiv 0 \pmod{m}$
 - ▶ $f(c) \equiv 0 \pmod{n}$
 medför $f(c) \equiv 0 \pmod{mn}$ (Kinesiska Restsatsen)

- ▶ $f(x) = a_\ell x^\ell + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$
- ▶ $m, n, r \in \mathbb{Z}_+, c \in \mathbb{Z}, p$ primtal
- ▶ $f(c) = 0$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ $f(c) \equiv 0 \pmod{mn}$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ “Lyft”:
 - ▶ $f(c) \equiv 0 \pmod{p^r}$
 - ▶ $c \equiv c + tp^r \pmod{p^r}$ men inte $\pmod{p^{r+1}}$ för $1 \leq t \leq p - 1$, olika
 - ▶ Kanske $f(c + tp^r) \equiv 0 \pmod{p^{r+1}}$ för något t
- ▶ “Kombinera”:
 - ▶ $\gcd(m, n) = 1$
 - ▶ $f(c) \equiv 0 \pmod{m}$
 - ▶ $f(c) \equiv 0 \pmod{n}$
 medför $f(c) \equiv 0 \pmod{mn}$ (Kinesiska Restsatsen)

- ▶ $f(x) = a_\ell x^\ell + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$
- ▶ $m, n, r \in \mathbb{Z}_+, c \in \mathbb{Z}, p$ primtal
- ▶ $f(c) = 0$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ $f(c) \equiv 0 \pmod{mn}$ medför $f(x) \equiv 0 \pmod{m}$, ej omvänt
- ▶ “Lyft”:
 - ▶ $f(c) \equiv 0 \pmod{p^r}$
 - ▶ $c \equiv c + tp^r \pmod{p^r}$ men inte $\pmod{p^{r+1}}$ för $1 \leq t \leq p - 1$, olika
 - ▶ Kanske $f(c + tp^r) \equiv 0 \pmod{p^{r+1}}$ för något t
- ▶ “Kombinera”:
 - ▶ $\gcd(m, n) = 1$
 - ▶ $f(c) \equiv 0 \pmod{m}$
 - ▶ $f(c) \equiv 0 \pmod{n}$
 medför $f(c) \equiv 0 \pmod{mn}$ (Kinesiska Restsatsen)

Exempel

$$x^2 + x + 5 \equiv 0 \pmod{77}$$

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:

$$0 \equiv x^2 - 10x + 5 \equiv (x-5)^2 - 25 + 5 \equiv (x-5)^2 - 9 \equiv (x-5+3)(x-5-3) \equiv (x-2)(x-8)$$

Kombinera med Restsatsen:

$$\left. \begin{array}{l} x \equiv 1 \pmod{7} \\ x \equiv 2 \pmod{11} \end{array} \right\} \iff x \equiv 57 \pmod{77}$$

Tre lösningar till, hitta dem!

Exempel

$f(x) = x^2 + x + 5$, sök nollställens modulo 7^2 .

Märk: om $f(a) \equiv 0 \pmod{49}$, så $f(a) \equiv 0 \pmod{7}$, men inte omvänt nödvändigtvis

Nollställen modulo 7: 1,5. Kan vi "lyfta" dem till nollställen modulo 49?

$a \equiv 1 \pmod{7}$ ger $a = 1 + 7s$. Så "lyften" är 1, 8, 15, 22, 29, 36, 43. Är någon av dem nollställe modulo 49?

$f(a) = a^2 + a + 5 \equiv (1 + 7s)^2 + (1 + 7s) + 5 \equiv 1 + 14s + 49s^2 + 1 + 7s + 5 \pmod{7^2}$, så

$$f(a) \equiv 21s + 7 \pmod{49}$$

För nollställe, lös

Exempel (fortsättning)

$$21s \equiv -7 \pmod{49}$$

$$3s \equiv -1 \pmod{7}$$

$$s \equiv 2 \pmod{7}$$

varför

$$a = 1 + 7s \equiv 1 + 7 * 2 \equiv 15 \pmod{49}$$

Datorn kontrollerar:

```
R.<t> = Integers(49) []
```

```
f=t^2+t+5
```

hittar

$$f(15) = ??$$

Exempel (cont)

Är det enda nollstället?

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

hittar

```
myroots = ??
```

Aha, så "lyftet" av nollstället $x \equiv 5 \pmod{7}$ till $x = 5 + 7 * 4$ fungerar.

Definition

- ▶ $f(x) = \sum_j a_j x^j \in K[x]$
- ▶ K någon koefficientring
- ▶ Den formella derivatan är $f'(x) = \sum_j j a_j x^{j-1}$

Exempel

$$f(x) = 1 + x + x^2 + x^3 + x^4 + x^5 \in \mathbb{Z}_2[x],$$

då blir

$$f'(x) = 1 + 2x + 3x^2 + 4x^3 + 5x^4 = 1 + 3x^2 + 5x^4.$$

Koefficienterna räknas modulo två, inte exponenterna!

Lemma

$f(x + y) \in K[x, y]$, polynomringen i två variabler. Då gäller att

$$f(x + y) = f(x) + f'(x)y + g(x, y)y^2 \quad (1)$$

för något $g(x, y) \in K[x, y]$.

Vi kan identifiera $K[x, y]$ med $K[x][y] \subset K(x)[y]$ och skriva

$$f(x + y) = f(x) + f'(x)y + \mathcal{O}(y^2)$$

Exempel

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

$$\begin{aligned} f(x + y) &= (x + y)^3 - (x + y) + 2 \\ &= x^3 + 3x^2y + 3xy^2 + y^3 - x - y + 2 \\ &= (x^3 - x + 2) + (3x^2 - 1)y + 3xy^2 + y^3. \end{aligned}$$

Bevis.

Binomialsatsen:

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

Därför:

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



Hensels lemma

- ▶ p primtal
- ▶ $f(x) \in \mathbb{Z}[x]$
- ▶ $c \in \mathbb{Z}, f(c) \equiv 0 \pmod{p^r}$
- ▶ Substituera $x = c, y = p^r s$ i $f(x + y) = f(x) + f'(x)y + g(x, y)y^2$
- ▶ Får $f(c + sp^r) = f(c) + f'(c)p^r s + g * (p^r s)^2$, så

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

- ▶ Om $f'(c) \not\equiv 0 \pmod{p}$ så $f'(c) \not\equiv 0 \pmod{p^{r+1}}$ och vi kan lösa

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

unikt. Dela med p^r för att erhålla

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

Hensels lemma

- ▶ p primtal
- ▶ $f(x) \in \mathbb{Z}[x]$
- ▶ $c \in \mathbb{Z}, f(c) \equiv 0 \pmod{p^r}$
- ▶ Substituera $x = c, y = p^r s$ i $f(x + y) = f(x) + f'(x)y + g(x, y)y^2$
- ▶ Får $f(c + sp^r) = f(c) + f'(c)p^r s + g * (p^r s)^2$, så

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

- ▶ Om $f'(c) \not\equiv 0 \pmod{p}$ så $f'(c) \not\equiv 0 \pmod{p^{r+1}}$ och vi kan lösa

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

unikt. Dela med p^r för att erhålla

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

Hensels lemma

- ▶ p primtal
- ▶ $f(x) \in \mathbb{Z}[x]$
- ▶ $c \in \mathbb{Z}, f(c) \equiv 0 \pmod{p^r}$
- ▶ Substituera $x = c, y = p^r s$ i $f(x + y) = f(x) + f'(x)y + g(x, y)y^2$
- ▶ Får $f(c + sp^r) = f(c) + f'(c)p^r s + g * (p^r s)^2$, så

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

- ▶ Om $f'(c) \not\equiv 0 \pmod{p}$ så $f'(c) \not\equiv 0 \pmod{p^{r+1}}$ och vi kan lösa

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

unikt. Dela med p^r för att erhålla

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

Hensels lemma

- ▶ p primtal
- ▶ $f(x) \in \mathbb{Z}[x]$
- ▶ $c \in \mathbb{Z}, f(c) \equiv 0 \pmod{p^r}$
- ▶ Substituera $x = c, y = p^r s$ i $f(x + y) = f(x) + f'(x)y + g(x, y)y^2$
- ▶ Får $f(c + sp^r) = f(c) + f'(c)p^r s + g * (p^r s)^2$, så

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

- ▶ Om $f'(c) \not\equiv 0 \pmod{p}$ så $f'(c) \not\equiv 0 \pmod{p^{r+1}}$ och vi kan lösa

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

unikt. Dela med p^r för att erhålla

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

Hensels lemma

- ▶ p primtal
- ▶ $f(x) \in \mathbb{Z}[x]$
- ▶ $c \in \mathbb{Z}, f(c) \equiv 0 \pmod{p^r}$
- ▶ Substituera $x = c, y = p^r s$ i $f(x + y) = f(x) + f'(x)y + g(x, y)y^2$
- ▶ Får $f(c + sp^r) = f(c) + f'(c)p^r s + g * (p^r s)^2$, så

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

- ▶ Om $f'(c) \not\equiv 0 \pmod{p}$ så $f'(c) \not\equiv 0 \pmod{p^{r+1}}$ och vi kan lösa

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

unikt. Dela med p^r för att erhålla

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

Hensels lemma

- ▶ p primtal
- ▶ $f(x) \in \mathbb{Z}[x]$
- ▶ $c \in \mathbb{Z}, f(c) \equiv 0 \pmod{p^r}$
- ▶ Substituera $x = c, y = p^r s$ i $f(x + y) = f(x) + f'(x)y + g(x, y)y^2$
- ▶ Får $f(c + sp^r) = f(c) + f'(c)p^r s + g * (p^r s)^2$, så

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

- ▶ Om $f'(c) \not\equiv 0 \pmod{p}$ så $f'(c) \not\equiv 0 \pmod{p^{r+1}}$ och vi kan lösa

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

unikt. Dela med p^r för att erhålla

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

Lemma (Hensels lemma)

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

Då finns unikt $t \pmod{p}$ så att

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

Detta t är den unika lösningen till ekvationen

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

Lemma (Hensels lemma)

1. p primtal

2. $f(x) \in \mathbb{Z}[x]$

3. $f(c) \equiv 0 \pmod{p}$

4. $f'(c) \not\equiv 0 \pmod{p}$

Då finns c_2, c_3, c_4, \dots så att

1. $c_j \equiv c \pmod{p}$ (det är ett lyft av c)

2. $c_j \equiv c_{j-1} \pmod{p^{j-1}}$ (lyft av c_{j-1})

3. $f(c_j) \equiv 0 \pmod{p^j}$ (lösning mod p^j)

4. c_j är unik mod p^j

- ▶ Lyft c_j till c_{j+1} genom att sätta $c_{j+1} = c_j + tp^j$, lös för $t \pmod{p^{j+1}}$
- ▶ Om $f'(c) \equiv 0 \pmod{p}$ så första lyftet icke-existerande eller ej unikt

Exempel

- ▶ $p = 5$
- ▶ $f(x) = x^3 + 2$
- ▶ f saknar nollställen i \mathbb{Z} eller \mathbb{Q} , men ett nollställe i \mathbb{R} , och 3 nollställen i \mathbb{C}
- ▶ $f(2) \equiv 0 \pmod{5}$
- ▶ $f'(x) = 3x^2$, $f'(2) = 12 \not\equiv 0 \pmod{5}$
- ▶ Hensel: lyfter unikt till alla potenser av 5
- ▶ ??

Exempel

- ▶ $p = 3$
- ▶ $f(x) = x^3 + 2$
- ▶ $f(1) \equiv 0 \pmod{3}$
- ▶ $f'(x) = 3x^2, f'(1) = 3 \equiv 0 \pmod{3}$
- ▶ Hensel: om det lyfter, så ej unikt
- ▶ I själva verket inga lösningar modulo 9

Exempel

- ▶ $p = 3$
- ▶ $f(x) = ??$
- ▶ $f(2) = ?? \equiv 0 \pmod{3}$
- ▶ $f'(x) = ??$
- ▶ $f'(2) = ?? \equiv 0 \pmod{3}$
- ▶ Hensel: om lyfter, så ej unikt
- ▶ Lyfter på varjehanda sätt:

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

- ▶ Motsäger verkligen inte Lagranges fina resultat

Exempel

- ▶ Vi lyfter “manuellt”
- ▶ $0 \equiv f(2 + 3t) \equiv f(2) + f'(2)3t \pmod{9}$
- ▶ $f(2)$ råkar bli 0 mod 9
- ▶ $f'(2) \equiv 3 \pmod{9}$
- ▶ $3 * 3 * t \equiv 0 \pmod{9}$, t är vadsomhelst
- ▶ $2 + 0 * 3$, $2 + 1 * 3$, $2 + 2 * 3$ alla giltiga lyft

Tillämpning: faktorisera heltal

- ▶ Antag q_1, q_2 primtal, $N = q_1 q_2$
- ▶ $N \equiv q_1 q_2 \pmod{p^j}$
- ▶ Om $x_j y_j \equiv N \pmod{p^j}$, sätt $x_{j+1} = x_j + sp^j$, $y_{j+1} = y_j + tp^j$,
- ▶ Vill ha $x_{j+1} y_{j+1} \equiv N \pmod{p^{j+1}}$
- ▶ $N \equiv (x_j + sp^j)(y_j + tp^j) \equiv x_j y_j + tp^j x_j + sp^j y_j + sp^j tp^j \pmod{p^{j+1}}$
- ▶ $N - x_j y_j \equiv tp^j x_j + sp^j y_j \pmod{p^{j+1}}$
- ▶ Allt delbart med p^j , så
- ▶ $(N - x_j y_j)/p^j \equiv sy_j + tx_j \pmod{p}$
- ▶ p lösningar, om s fixt så kan t lösas ut

Exempel (Hackman)

- ▶ $a \in \mathbb{Z}$ har invers $b \pmod{p^n}$, så $ab \equiv 1 \pmod{p^n}$
- ▶ Så $a \not\equiv 0 \pmod{p}$
- ▶ Vill lyfta b till invers $\pmod{p^{n+1}}$
- ▶ $f(x) = ax - 1$, $f(b) \equiv 0 \pmod{p^n}$, $f'(b) = a \not\equiv 0 \pmod{p}$
- ▶ $f(b + tp^n) \equiv f(b) + f'(b)tp^n \equiv ab - 1 + atp^n \equiv 0 \pmod{p^{n+1}}$
- ▶ Dela med p^n
- ▶ $\frac{ab-1}{p^n} + at \equiv 0 \pmod{p}$

Exempel (fortsättning)

- ▶ $a = 8, p = 5$
- ▶ $8 * 2 \equiv 1 \pmod{5}$
- ▶ Ekvation $(8 * 2 - 1)/5 + 8t \equiv 0 \pmod{5}$ blir $3 + 8t \equiv 0 \pmod{5}$, unik lösning $t = 4$
- ▶ Så $2 + 4 * 5 = 22$ invers mod 25
- ▶ $8 * 22 = 176 \equiv 1 \pmod{25}$