Talteori, Föreläsning 4

Polynom, kongruenser, Hensel-lyft

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet
Föreläsningsanteckningar på kurshemsidan `http://courses.mai.liu.se/GU/TATA54/`

Sammanfattning

Polynom med koefficienter i $\mathbb{Z}_p$

- Definition, grad
- Divisionsalgoritmen
- Lagrange
- Wilsons theorem

Hensel-lyft

- Polynomiella kongruenser
- Polynomiella kongruenser modulo primpotens
- Formell derivata
- Hensels lemma
- Faktorisering
- Tillämpning: inverser

Sammanfattning

Polynom med koefficienter i $\mathbb{Z}_p$

- Definition, grad
- Divisionsalgoritmen
- Lagrange
- Wilsons theorem

Hensel-lyft

- Polynomiella kongruenser
- Polynomiella kongruenser modulo primpotens
- Formell derivata
- Hensels lemma
- Faktorisering
- Tillämpning: inverser

"Lyft"

$$\mathbb{Z}_{mn} \twoheadrightarrow \mathbb{Z}_n$$

$$[a]_{mn} \mapsto [a]_n$$

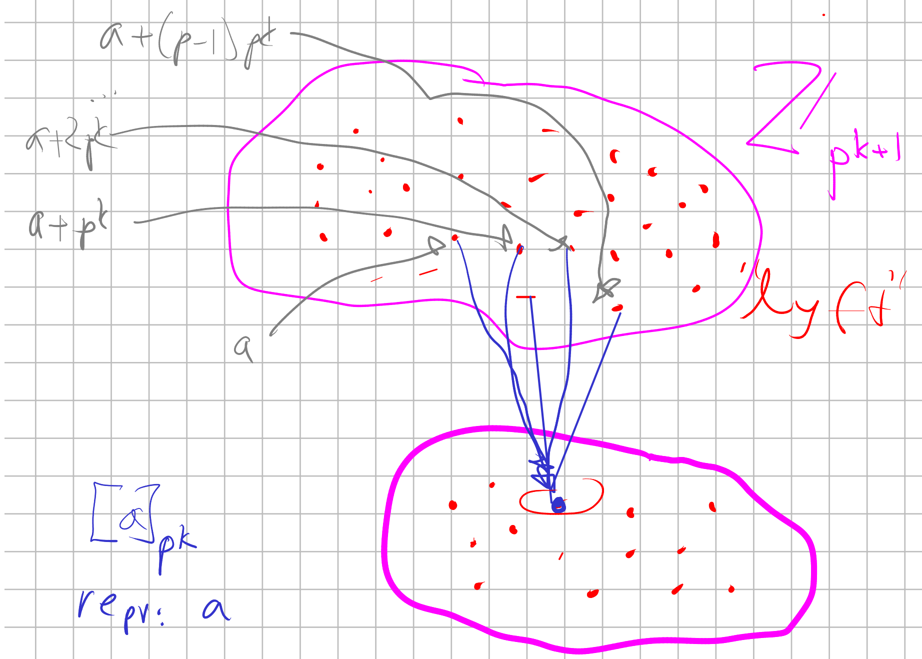
väldef

Speciellt: p primtal

$$\mathbb{Z}_p \twoheadleftarrow \mathbb{Z}_{p^2} \twoheadleftarrow \mathbb{Z}_{p^3} \twoheadleftarrow \cdots$$

$$[a]_p \leftarrow\!\shortmid [a]_{p^2} \leftarrow\!\shortmid [a]_{p^3}$$

Exempel: $p = 3,\ k = 2$

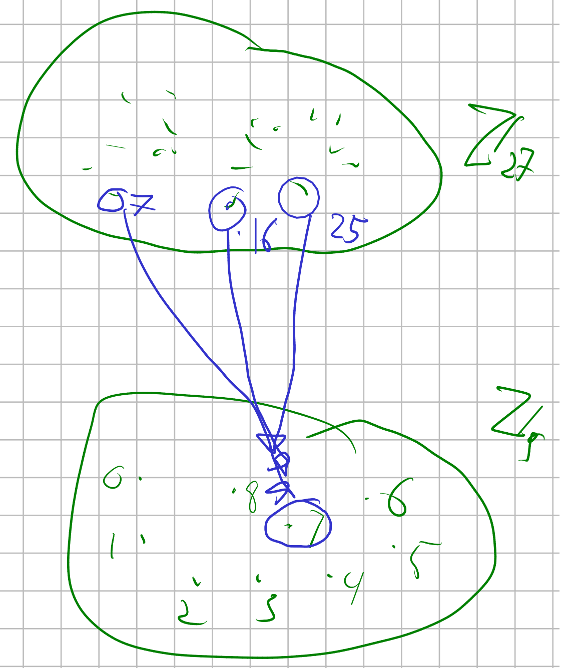


$[a]_{p^k}$

repr: a

p primtal

$\mathbb{Z}/p^k$



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 $a_j \in \mathbb{Z}_p$, $a_n \neq 0$.
- $n = \deg(f(x))$.
- $\mathrm{lc}(f(x)) = a_n$, $\mathrm{lm}(f(x)) = x^n$
- Nollpolynomet har grad $-\infty$

Lemma

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

Exempel

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

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

$x^a \cdot x^b = x^{a+b}$

Evaluering

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

Evaluering

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

Evaluering

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

Evaluering

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

Evaluering

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

Evaluering

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

Evaluering

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

	0	1
1	0	0
2	1	1
3	0	1
4	1	0

0

1

x

$x+1$

0 x^2+x x^3+x^2

- $p = 2$
- $f(x) = 1$ (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 $\mathbb{Z}_2 \to \mathbb{Z}_2$, men är olika som polynom
- Två polynom ger samma funktion omm de skiljer sig åt med en polynomiell multipel av $x^2 + x$

Teorem (Divisionsalgoritmen)

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

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

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

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

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 $\mathrm{RHS}(a) = 0$, 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 $r = 0$. $\square$

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. □

Exempel

$f(x) = [2]_4 x + [2]_4 \in \mathbb{Z}_4[x]$ 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 $\mathbb{Z}_4$?

Tillämpning: Wilsons sats

$p = 5, \quad 1, 2, 3, 4$

Teorem (Wilson)

p primtal. Då $(p-1)! \equiv -1 \mod p$.

Bevis

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

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

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,

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

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 $f(x) \equiv 0 \mod m$, ej omvänt
- $f(c) \equiv 0 \mod mn$ medför $f(x) \equiv 0 \mod m$, ej omvänt
- "Lyft":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ men inte mod p^{r+1} för $1 \leq t \leq p-1$, olika
  - Kanske $f(c + tp^r) \equiv 0 \mod p^{r+1}$ för något t
- "Kombinera":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  medför $f(c) \equiv 0 \mod mn$ (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 $f(x) \equiv 0 \mod m$, ej omvänt
- $f(c) \equiv 0 \mod mn$ medför $f(x) \equiv 0 \mod m$, ej omvänt
- "Lyft":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ men inte mod p^{r+1} för $1 \leq t \leq p-1$, olika
  - Kanske $f(c + tp^r) \equiv 0 \mod p^{r+1}$ för något t
- "Kombinera":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  medför $f(c) \equiv 0 \mod mn$ (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 $f(x) \equiv 0 \mod m$, ej omvänt
- $f(c) \equiv 0 \mod mn$ medför $f(x) \equiv 0 \mod m$, ej omvänt
- "Lyft":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ men inte mod p^{r+1} för $1 \leq t \leq p-1$, olika
  - Kanske $f(c + tp^r) \equiv 0 \mod p^{r+1}$ för något t
- "Kombinera":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  medför $f(c) \equiv 0 \mod mn$ (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 mod 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 $f(x) \equiv 0 \mod m$, ej omvänt
- $f(c) \equiv 0 \mod mn$ medför $f(x) \equiv 0 \mod m$, ej omvänt
- "Lyft":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ men inte mod p^{r+1} för $1 \leq t \leq p-1$, olika
  - Kanske $f(c + tp^r) \equiv 0 \mod p^{r+1}$ för något t
- "Kombinera":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  medför $f(c) \equiv 0 \mod mn$ (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 $f(x) \equiv 0 \mod m$, ej omvänt
- $f(c) \equiv 0 \mod mn$ medför $f(x) \equiv 0 \mod m$, ej omvänt
- "Lyft":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ men inte mod p^{r+1} för $1 \leq t \leq p-1$, olika
  - Kanske $f(c + tp^r) \equiv 0 \mod p^{r+1}$ för något t
- "Kombinera":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  medför $f(c) \equiv 0 \mod mn$ (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 $f(x) \equiv 0 \mod m$, ej omvänt
- $f(c) \equiv 0 \mod mn$ medför $f(x) \equiv 0 \mod m$, ej omvänt
- "Lyft":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ men inte mod p^{r+1} för $1 \leq t \leq p-1$, olika
  - Kanske $f(c + tp^r) \equiv 0 \mod p^{r+1}$ för något t
- "Kombinera":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

  medför $f(c) \equiv 0 \mod mn$ (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 $f(x) \equiv 0 \mod m$, ej omvänt
- $f(c) \equiv 0 \mod mn$ medför $f(x) \equiv 0 \mod m$, ej omvänt
- "Lyft":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ men inte mod p^{r+1} för $1 \le t \le p-1$, olika
  - Kanske $f(c + tp^r) \equiv 0 \mod p^{r+1}$ för något t
- "Kombinera":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

medför $f(c) \equiv 0 \mod mn$ (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 $f(x) \equiv 0 \mod m$, ej omvänt
- $f(c) \equiv 0 \mod mn$ medför $f(x) \equiv 0 \mod m$, ej omvänt
- "Lyft":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ men inte mod p^{r+1} för $1 \leq t \leq p-1$, olika
  - Kanske $f(c + tp^r) \equiv 0 \mod p^{r+1}$ för något t
- "Kombinera":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

medför $f(c) \equiv 0 \mod mn$ (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 $f(x) \equiv 0 \mod m$, ej omvänt
- $f(c) \equiv 0 \mod mn$ medför $f(x) \equiv 0 \mod m$, ej omvänt
- "Lyft":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ men inte mod p^{r+1} för $1 \leq t \leq p-1$, olika
  - Kanske $f(c + tp^r) \equiv 0 \mod p^{r+1}$ för något t
- "Kombinera":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

medför $f(c) \equiv 0 \mod mn$ (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 $f(x) \equiv 0 \mod m$, ej omvänt
- $f(c) \equiv 0 \mod mn$ medför $f(x) \equiv 0 \mod m$, ej omvänt
- "Lyft":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ men inte mod p^{r+1} för $1 \leq t \leq p-1$, olika
  - Kanske $f(c + tp^r) \equiv 0 \mod p^{r+1}$ för något t
- "Kombinera":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

medför $f(c) \equiv 0 \mod mn$ (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 $f(x) \equiv 0 \mod m$, ej omvänt
- $f(c) \equiv 0 \mod mn$ medför $f(x) \equiv 0 \mod m$, ej omvänt
- "Lyft":
  - $f(c) \equiv 0 \mod p^r$
  - $c \equiv c + tp^r \mod p^r$ men inte mod p^{r+1} för $1 \leq t \leq p-1$, olika
  - Kanske $f(c + tp^r) \equiv 0 \mod p^{r+1}$ för något t
- "Kombinera":
  - $\gcd(m, n) = 1$
  - $f(c) \equiv 0 \mod m$
  - $f(c) \equiv 0 \mod n$

medför $f(c) \equiv 0 \mod mn$ (Kinesiska Restsatsen)

primtal

$ax \equiv b \mod p$

$p \nmid a$

$[a]_p \neq [0]_p$

$x \equiv a^{-1} b \mod p$

$aa^{-1} \equiv 1 \mod p$

Exempel

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

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:

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

Kombinera med Restsatsen:

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

Tre lösningar till, hitta dem!

Exempel

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

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

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

Tre lösningar till, hitta dem!

$ax \equiv b \mod n$ lösbart omm $\gcd(a,n) \mid b$

Exempel

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

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

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

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

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

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

För nollställe, lös

Exemple (fortsättning)

$\gcd = 7$

$$21s \equiv -7 \mod 49$$

$3 \cdot 5 = 15 \equiv 1 \mod 7$

$$3s \equiv -1 \mod 7$$

$$s \equiv 2 \mod 7$$

$-1 \cdot 5 = -5 \equiv 2 \mod 7$

varför

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

Datorn kontrollerar:

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

hittar

$$f(15) = 0$$

Exempel (cont)

Är det enda nollstället?

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

hittar

$$\mathtt{myroots} = [33, 15]$$

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

Formell derivata

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

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

$K(x) = \left\{ \frac{p(x)}{q(x)} : p, q \in K[x] \right\}$

för något $g(x,y) \in K[x,y]$.

rationell fnk

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

$2x+5 \qquad \frac{1}{2x+5}$

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

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:

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

Därför:

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

□

Hensels lemma

- p primtal
- $f(x) \in \mathbb{Z}[x]$
- $c \in \mathbb{Z}$, $f(c) \equiv 0 \mod p^r$
- 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

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

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

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

unikt. Dela med p^r för att erhålla

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

Hensels lemma

- p primtal
- $f(x) \in \mathbb{Z}[x]$
- $c \in \mathbb{Z}$, $f(c) \equiv 0 \mod p^r$
- 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
$$f(c + sp^r) \equiv f(c) + f'(c)p^r s \mod p^{r+1}$$
- Om $f'(c) \not\equiv 0 \mod p$ så $f'(c) \not\equiv 0 \mod p^{r+1}$ och vi kan lösa
$$(f'(c)p^r)s \equiv -f(c) \mod p^{r+1}$$
unikt. Dela med p^r för att erhålla
$$f'(c)s \equiv \frac{-f(c)}{p^r} \mod p$$

Hensels lemma

- p primtal
- $f(x) \in \mathbb{Z}[x]$
- $c \in \mathbb{Z}$, $f(c) \equiv 0 \mod p^r$
- 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

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

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

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

unikt. Dela med p^r för att erhålla

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

Hensels lemma

$x + y$

$f(c+tp^r) \equiv 0 \mod p$

- p primtal
- $f(x) \in \mathbb{Z}[x]$
- $c \in \mathbb{Z}$, $f(c) \equiv 0 \mod p^r$
- 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

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

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

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

unikt. Dela med p^r för att erhålla

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

Hensels lemma

- p primtal
- $f(x) \in \mathbb{Z}[x]$
- $c \in \mathbb{Z}$, $f(c) \equiv 0 \mod p^r$
- 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

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

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

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

unikt. Dela med p^r för att erhålla

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

- p primtal
- $f(x) \in \mathbb{Z}[x]$
- $c \in \mathbb{Z}$, $\boxed{f(c) \equiv 0 \mod p^r}$
- 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

$$0 \equiv f(c + sp^r) \equiv f(c) + \underline{f'(c)}p^r s \mod p^{r+1}$$

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

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

unikt. Dela med p^r för att erhålla

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

Lemma (Hensels lemma)

$p^j \nearrow p^{j+1}$

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

Då finns unikt t (mod p) så att

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

Detta t är den unika lösningen till ekvationen

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

Lemma (Hensels lemma)

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

Då finns $c_2, c_3, c_4, \ldots$ så att

1. $c_j \equiv c \mod p$ *(det är ett lyft av c)*
2. $c_j \equiv c_{j-1} \mod p^{j-1}$ *(lyft av c_{j-1})*
3. $f(c_j) \equiv 0 \mod p^j$ *(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 mod p^{j+1}
- Om $f'(c) \equiv 0 \mod p$ så första lyftet icke-existerande eller ej unikt

$\to x^3 + 2 \equiv 0 \quad \text{mod } 125$

Exempel

- $p = 5$ $\qquad [2]_5 \in \mathbb{Z}_5 \qquad 2^3 + 2 = 10 \equiv 0 \text{ mod } 5$
- $f(x) = x^3 + 2$
- f saknar nollställen i $\mathbb{Z}$ eller $\mathbb{Q}$, men ett nollställe i $\mathbb{R}$, och 3 nollställen i $\mathbb{C}$
- $f(2) \equiv 0 \mod 5$ $\qquad 10 \not\equiv 0 \text{ mod } 25$
- $f'(x) = 3x^2$, $f'(2) = 12 \not\equiv 0 \mod 5$
- Hensel: lyfter unikt till alla potenser av 5 $\qquad 2 \quad 7 \quad 12 \quad 17 \quad 22 \quad \text{mod } 25$
-

p	p^2	p^3	p^4	p^5
2	22	72	322	947

$2 \qquad \text{mod } 5$

Exempel

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

1 4 7 mod 9

0 1 2 mod 3

Exempel

- $p = 3$
- $f(x) = x^4 - 7x^3 + 2x^2 + 2x + 1$
- $f(2) = -27 \equiv 0 \mod 3$
- $f'(x) = 4x^3 - 21x^2 + 4x + 2$
- $f'(2) = -42 \equiv 0 \mod 3$
- Hensel: om lyfter, så ej unikt
- Lyfter på varjehanda sätt:

moduli	roots
3	$[2]$
3^2	$[2, 5, 8]$
3^3	$[2, 5, 11, 14, 20, 23]$
3^4	$[11, 23, 38, 50, 65, 77]$

- Motsäger verkligen inte Lagranges fina resultat

2 5 8 mod 9

0 1 2 mod 3

Exempel

- Vi lyfter "manuellt"
- $0 \equiv f(2+3t) \equiv f(2) + \overbrace{f'(2)3}^{0 \bmod 9}t \mod 9$
- $f(2)$ råkar bli 0 mod 9
- $f'(2) \equiv 3 \mod 9$
- $3 * 3 * t \equiv 0 \mod 9$, t är vadsomhelst
- $2 + 0 * 3$, $2 + 1 * 3$, $2 + 2 * 3$ alla giltiga lyft

Tillämpning: faktorisera heltal

Givet

Hitta q_1, q_2

- Antag q_1, q_2 primtal, $N = q_1 q_2$
- $N \equiv q_1 q_2 \mod p^j$
- Om $x_j y_j \equiv N \mod p^j$, sätt $x_{j+1} = x_j + sp^j$, $y_{j+1} = y_j + tp^j$,
- Vill ha $x_{j+1} y_{j+1} \equiv N \mod p^{j+1}$
- $N \equiv (x_j + sp^j)(y_j + tp^j) \equiv x_j y_j + tp^j x_j + sp^j y_j + sp^j tp^j \mod p^{j+1}$
- $0 \equiv \cancel{x_j y_j} + sp^j y_j + tp^j x_j \mod p^{j+1}$
- Dela med p^j, får $\cancel{x_j y_j} + sy_j + tx_j \equiv 0 \mod p$
- Antag $x_j y_j \not\equiv 0 \mod p$, då lösbar

Exempel

- $q_1 q_2 = 653 * 467 = 304951 = N$
- $N \equiv 7 \mod 2^3$
- Icke-trivial factorisering $5 * 3 \equiv 7 \mod 2^3$
- För att lyfta, lös $15 + 3s + 5t \equiv 0 \mod 2$
- $(s, t) \equiv (1, 0)$ eller $(0, 1)$.
- Första varianten ger $13 * 3 \equiv 7 \mod 2^4$
- Andra varianten ger $5 * 11 \equiv 7 \mod 2^4$
- Försöker lyfta den senare: skall lösa $55 + 5s + 11t \equiv 0 \mod 2$ Återigen $(s, t) \equiv (1, 0)$ eller $(0, 1)$. Första ger $21 * 11 \equiv 7 \mod 32$, men $N \equiv 23 \mod 32$, dödfött lyft. Andra ger $5 * 27 \equiv 7 \mod 32$ inte bra.
- Lyfter vi $13 * 3 \equiv 7 \mod 16$ istället får vi $29 * 3 \equiv 23 \mod 32$ eller $13 * 19 \equiv 23 \mod 32$, båda duger hittils
- I själva verket så är $q_1 \equiv 13 \mod 32$, $q_2 \equiv 19 \mod 32$, så det är det rätta lyftet

Hackmans

a givet   sökt b

så $ab \equiv 1 \mod p^{n+1}$

Exempel (Hackman)

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

Exempel (fortsättning)

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

125

7.1.4 Lös

$\varphi(mn) = \varphi(m)\varphi(n)$
då $\gcd(m,n) = 1$

$\varphi(p^r) = p^r - p^{r-1}$

$\varphi(2) = 2^1 - 2^0 = 1$

$\varphi(2m) = \varphi(m)$
om $2 \nmid m$

a) $\varphi(n) = 1$ $\quad n = 2$

b) $\varphi(n) = 2$,

$\varphi(5) = 4 > 2$

$\varphi(3^a) = 3^a - 3^{a-1}$, $\quad \varphi(3) = 2$. $\quad \varphi(2^a) = 2^a - 2^{a-1}$

$\varphi(4) = 4 - 2 = 2$

så 3 duger, och $2 \cdot 3 = 6$
och 4 duger

c) $\varphi(n) = 3$

$\varphi(2) = 1$, $\varphi(4) = 2$, $\cancel{\varphi(8) = 4}$

$\varphi(3) = 2$, $\varphi(9) = \cancel{9 - 3 = 6}$ $\qquad$ ingen

$\cancel{\varphi(5) = 4}$

d) $\varphi(n) = 4$ $\quad \varphi(2) = 1$, $\varphi(4) = 2$, $\boxed{\varphi(8) = 4}$

$\varphi(5) = 4$

så 8 och 5 och $2 \cdot 5$

$\varphi(3 \cdot 4)$
$= \varphi(3) \cdot \varphi(4)$
$= 2 \cdot 2 = 4$

7.1.11. Lös $\varphi(3n) = 3\varphi(n)$ (*)

1) $3 \nmid n$. $\varphi(3n) = \varphi(3)\varphi(n)$

så ~~(*) ger $\varphi(n)=0$ el $\varphi(3)=3$~~, går ej.

2) $n = 3^a m$, $3 \nmid m$.

$$VL = \varphi(3n) = \varphi(3^{a+1} m) = \varphi(3^{a+1})\,\varphi(m)$$
$$= 3^a(3-1)\,\varphi(m) = \underline{2 \cdot 3^a \varphi(m)}$$

$$HL = 3\varphi(n) = 3\varphi(3^a m) = 3 \cdot 3^{a-1}(3-1)\,\varphi(m)$$
$$= 3^a \cdot 2 \cdot \varphi(m)$$

alla sådana.

p^h

$1, p, p^2, \ldots, p^h$

7.2.12 Visa att $\sigma(n) = k$ har ändligt många lösningar för $k > 0$

Bl $n = \prod_{j=1}^{r} p_j^{a_j}$, $\sigma(n) = \prod_{j=1}^{r} \frac{p_j^{a_j+1}-1}{p_j-1}$

Om $\sigma(n) = k$ så $\frac{p_j^{a_j+1}-1}{p_j-1} \le k$

Men

$$\frac{p^{a_j+1}-1}{p_j} = 1 + p_j + p_j^2 + \dots p_j^{a_j} \ge p_j^{a_j}$$

så $p_j^{a_j} \le k$, ger $p_j \le k$ och $a_j \le \log_{p_j}(k) \le \log_2(k)$.

Hur är det med $\tau(n) = k$?

$$\tau\left(\prod_j p_j^{a_j}\right) = \prod_j (a_j + 1)$$

Så $\tau(n) = 6$ har lösningar

$$n = p_j^1 p_k^2 \quad , j \neq k$$

∞ många.

$\tau(9) = 3$

1, 3, 9

$\sigma(9) = 13$

4

1, 2, 4