Number Theory, Lecture 2

Linear Diophantine equations, congruenses

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

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

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Summary

Summary

Summary

Teorem

Låt $a, b, c \in \mathbb{Z}$. Sätt $d = \gcd(a, b)$. Den Diofantiska ekvationen

$$ax + by = c, \qquad x, y \in \mathbb{Z} \tag{DE}$$

är lösbar om och endast om $d|c$.

Bevis.

Nödvändigt: om lösning x, y finns, så $d|LHS$, så $d|c$.
Tillräckligt: om $d|c$, så (DE) ekvivalent med

$$\frac{a}{d}x + \frac{b}{d}x = \frac{c}{d} \tag{DE'}$$

med $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$. Kan alltså anta $d = 1$. □

Fallet $d = 1$ på nästa sida

Teorem

Låt $a, b, c \in \mathbb{Z}$, med $\gcd(a, b) = 1$. Den Diofantiska ekvationen

$$ax + by = c, \qquad x, y \in \mathbb{Z} \tag{DE1}$$

är lösbar.

Bevis.

Bezout: $1 = ax' + by'$, så $c = ax'c + by'c$. Sätt $x = x_p = x'c$, $y = y_p = y'c$. □

Alla lösningar

- Om (x_1, y_2) och (x_2, y_2) båda lösningar till (DE1) så $(x_1 - x_2, y_1 - y_2)$ lösning till

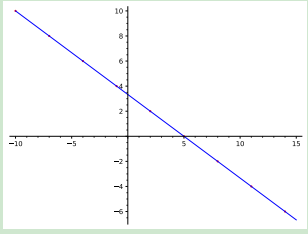
$$ax + by = 0 \qquad \text{(DEH)}$$

- $(x, y) = (bn, -an)$, $n \in \mathbb{Z}$, lösningar till (DEH)
- I själva verket ges alla lösningar av $ax = -by$ så $b|x$, alltså $x = bn$. Därför $abn = -by$, så $-an = y$.
- $(x, y) = (bn, -an)$, $n \in \mathbb{Z}$ är *alla* lösningar till (DEH)
- Så alla lösningar till (DE1) ges av

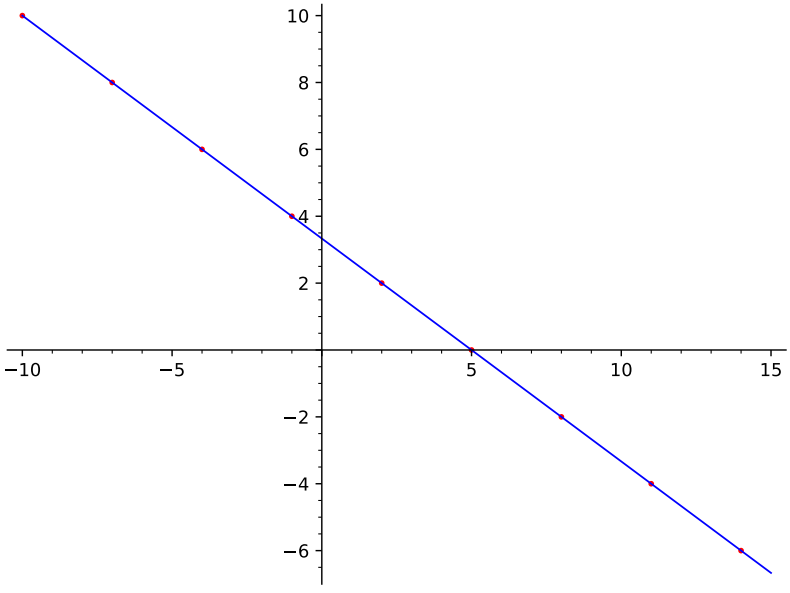
$$(x, y) = (x_p, y_p) + (x_h, y_h) = (x_p, y_p) + n(b, -a)$$

Exempel

- $4x + 6y = 20$
- $\gcd(4, 6) = 2$
- $2x + 3y = 10$
- $\gcd(2, 3) = 1 = 2 * (-1) + 3 * 1$
- $2 * (-10) + 3 * 10 = 10$
- $(x_p, y_p) = (-10, 10)$ partikulärlösning



- Alla lösningar till $2x + 3y = 0$ ges av $(x_h, y_h) = n(3, -2),\ n \in \mathbb{Z}$
- Alla lösningar till ursprungliga Diofantiska ekv. ges av $(x, y) = (x_h, y_h) + (x_p, y_p) = (-10 + 3n, 10 - 2n)$


10
8
6
4
2
−10
−5
5
10
15
−2
−4
−6

Generalisering

Teorem

Den linjära Diofantiska ekvationen

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c$$

är lösbar när $\gcd(a_i, a_j) = 1$ *för* $i \neq j$.
(Lite svagare villkor räcker)

Bevis.

Nödvändighet: uppenbar.
Tillräcklighet: studera

$$a_1x + 1 * y = c, \qquad \gcd(a_1, y) = 1$$

Lösbar med x, y heltal. Betrakta nu

$$a_2x_2 + \cdots + a_nx_n = y,$$

lösbar per induktion. □

Exempel

$$2x + 3y + 5z = 1$$

- Lös $2x + 1u = 1$
- $(x, u) = (0, 1) + n(1, -2)$.
- Lös $3y + 5z = u = 1 - 2n$.
- $(y, z) = (1 - 2n)(2, -1) + m(5, -3)$.
- Kombinera:

$$(x, y, z) = (0, 2, -1) + n(1, 4, -2) + m(0, 5, -3)$$

Kongruens modulo n

$n \in \mathbb{Z}$, $n > 1$.

Definition

För $a, b \in \mathbb{Z}$ säger vi att a är kongruent med b modulo n,

$$a \equiv b \mod n$$

omm $n|(a-b)$.

Lemma

- $a \equiv a \mod n$,
- $a \equiv b \mod n \iff b \equiv a \mod n$,
- $a \equiv b \mod n \wedge b \equiv c \mod n \implies a \equiv c \mod n$.

Exempel

- Udda tal är kongruenta med varandra modulo 2
- $134632 \equiv 5645234532 \mod 100$
- $4 \equiv -1 \mod 5$,
- $4 \not\equiv 1 \mod 5$.

Definition

En relation $\sim$ på X är en ekvivalensrelation om för alla $x, y, z \in X$ gäller att

- $x \sim x$, (relationen är reflexiv)
- $x \sim y \iff y \sim x$, (symmetrisk)
- $x \sim y \wedge y \sim z \implies x \sim z$ (transitiv).

- För $x \in X$, $[x] = [x]_\sim = \{ y \in X | x \sim y \}$ är ekvivalensklassen innehållande x, och x är en representat för klassen
- Klasserna partitionerar X:

$$X = \cup_{x \in X} [x], \qquad \text{union disjoint}$$

  Med andra ord så tillhör varje element precis en ekvivalensklass.

- $x \sim y \iff x \in [y] \iff [x] = [y]$

- Vi samlar ihop ekvivalensklasserna i en påse:

$$X/\sim = \{\,[x] \mid x \in X\,\}$$

- Bild kommer!
- Kanonisk surjektion:

$$\pi : X \to X/\sim$$
$$\pi(y) = [y]$$

- Sektion:

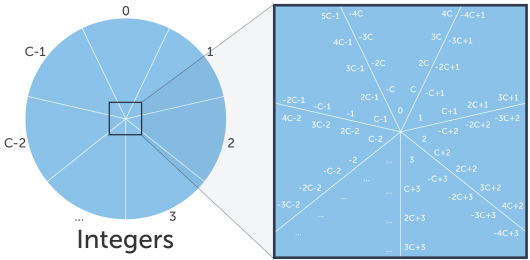
$$s : X/\sim \rightarrowtail X$$

  så att $\pi(s(A)) = A$.
- Transversal T: val av precies en representant från varje klass
- Normalform: $w = s \circ \pi$ uppfyller $n(y) \sim y$, $n(n(y)) = n(y)$
- Dessa begrepp är intimt sammanflätade. Bild!

- Fixera positivt heltal $n > 1$, och låt $\sim$ vara ekvivalensrelationen

$$x \sim y \iff x \equiv y \mod n$$

- Då är $X = \mathbb{Z}$
- X partitioneras i n klasser, eller hur?



- Om

$$x = kn + r, \quad 0 \leq r < n$$
$$x' = k'n + r', \quad 0 \leq r' < n$$

  så $x \equiv x' \mod n$ omm $r = r'$.
- Så $T = \{0, 1, 2, \ldots, n-1\}$ är en transversal
- $\mathbb{Z} = [0] \cup [1] \cup \cdots \cup [n-1]$,
- $[a] = n\mathbb{Z} + a$,
- Sektion: $s([a]) = b$ med $b \equiv a \mod n$ och $0 \leq b < n$, i.e., $b \in T$.
- Normal form: $kn + r \mapsto r$
- $\mathbb{Z}_n = \mathbb{Z}/(n\mathbb{Z}) = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$
- Kan addera och multiplicera kongruensklasser genom att addera och multiplicera representater!

Lemma

Antag att

$$a_1 \equiv a_2 \mod n$$
$$b_1 \equiv b_2 \mod n$$

Då gäller att

$$a_1 + b_1 \equiv a_2 + b_2 \mod n$$
$$a_1 b_1 \equiv a_2 b_2 \mod n$$

Bevis.

$n|(a_1 - a_2)$, $n|(b_1 - b_2)$. Eftersom $(a_1 - a_2) + (b_1 - b_2) = (a_1 + b_1) - (a_2 + b_2)$, $n|((a_1 + b_1) - (a_2 + b_2))$.
Vidare,

$$\begin{aligned} a_1 b_1 - a_2 b_2 &= a_1 b_1 + a_2 b_1 - a_2 b_1 - a_2 b_2 \\ &= (a_1 - a_2) b_1 - a_2 (b_1 - b_2) \end{aligned}$$

□

Definition

Vi adderar och multiplicerar kongruensklasser i $\mathbb{Z}_n$ genom

$$[a]_n + [b]_n = [a+b]_n$$
$$[a]_n[b]_n = [ab]_n$$

Teorem

$$[a] + [0] = [a]$$
$$[a] + [-a] = [0]$$
$$[a] + [b] = [b+a]$$
$$([a] + [b]) + [c] = [a] + ([b] + [c])$$
$$[a] * [1] = [a]$$
$$[a] * [b] = [b] * [a]$$
$$([a] * [b]) * [c] = [a] * ([b] * [c])$$
$$[a] * ([b] + [c]) = ([a] * [b]) + ([a] * [c])$$

Exempel

Addition och multiplikation modulo 4:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Addition and multiplikation modulo 5:

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

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

Lemma

Om $ac \equiv bc \mod n$ *och* $\gcd(c, n) = 1$, *så* $a \equiv b \mod n$.

Bevis.

$n|(ac - bc)$, så $n|c(a - b)$, så $n|(a - b)$ (föregående lemma). □

Exempel

$$0 * 2 \equiv 2 * 2 \mod 4,$$

men

$$0 \not\equiv 2 \mod 4$$

Lemma

Om $T = \{t_1, \ldots, t_n\}$ *transversal (mod n) och* $\gcd(a, n) = 1$, *så* $aT = \{at_1, \ldots, at_n\}$ *också transversal.*

Bevis.

Behöver bara visa att $at_i \equiv at_j \mod n$ medför $i = j$. Men $n|(at_i - at_j)$ ger $n|(t_i - t_j)$, som ger $i = j$, ty T transversal. □

Teorem

Om $\gcd(a, n) = 1$ *så är*

$$ax \equiv b \mod n$$

lösbar, och lösningen är unik modulo n*.*

Bevis.

Unikhet: om $ax \equiv ax' \equiv b \mod n$ så $ax - ax' \equiv 0 \mod n$, varför $x \equiv x' \mod n$. Existens: $T = \{t_1, \ldots, t_n\}$ transversal. $aT = \{at_1, \ldots, at_n\}$ också transversal, så någon $at_j \equiv 1 \mod n$. □

Exempel

Lös $3x \equiv 2 \mod 5$. $T = \{0, 1, 2, 3, 4\}$, $3T = \{0, 3, 6, 9, 12\} \equiv \{0, 3, 1, 4, 2\} \mod 5$. So $3 * 4 \equiv 2 \mod 5$.

Teorem

Låt $d = \gcd(a, n)$. *Ekvationen*

$$ax \equiv b \mod n$$

är lösbar omm $d|b$; *lösningen då unik modulo* n/d.

Bevis.

Eftersom $d = \gcd(a, n)$ så $d|n$ och $d|a$.
Nödvändigt: om lösning finns så $n|(ax - b)$, alltså $d|b$.
Tillräckligt: antag $d|b$.

$$n|(ax - b) \iff \frac{n}{d}|(\frac{a}{d}x - \frac{b}{d}) \iff \frac{a}{d}x \equiv \frac{b}{d} \mod \frac{n}{d}$$

Eftersom $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$ kan vi tillämpa tidigare lemmat: lösning finns, unik modulo $\frac{n}{d}$. □

Exempel

$$4x \equiv 2 \mod 6$$
$$2x \equiv 1 \mod 3$$
$$2x - 1 \equiv 0 \mod 3$$

- Diofantisk ekvation $2x - 1 = 3y$
- En lösning är $x = -1, y = -1$
- Så $x \equiv -1 \equiv 2 \mod 3$ unik lösning mod 3

Teorem (Kinesiska restsatsen)

Om $\gcd(m, n) = 1$ *så har ekvationssystemet*

$$\begin{aligned} x &\equiv a \mod m \\ x &\equiv b \mod n \end{aligned} \tag{CRT}$$

en lösning, som är unik modulo mn.

Proof

Unikhet: om

$$\begin{aligned} x \equiv x' &\equiv a \mod m \\ x \equiv x' &\equiv b \mod n \end{aligned}$$

så

$$\begin{aligned} x - x' &\equiv 0 \mod m \\ x - x' &\equiv 0 \mod n \end{aligned}$$

Alltså $m|(x - x')$, $n|(x - x')$, så eftersom $\gcd(m, n) = 1$ får vi att $mn|(x - x')$.

Bevis.

Existens: vi har att $x \equiv a \mod m$, så $x = a + rm$, $r \in \mathbb{Z}$. Alltså

$$\begin{aligned} x &\equiv b \mod n \\ a + rm &\equiv b \mod n \\ a + rm &= b + sn \\ rm - sn &= b - a \end{aligned}$$

Detta är en linjär Diofantisk ekv, lösbar ty $\gcd(m, n) = 1$.
Alternativt, $rm \equiv b - a \mod n$ lösbar (för r) eftersom $\gcd(m, n) = 1$. □

Exempel

$$
\begin{aligned}
x &\equiv 1 \mod 2 \\
x &\equiv 3 \mod 5 \\
x &\equiv 5 \mod 7
\end{aligned}
$$

Lös två första ekv:

$$
\begin{aligned}
x = 1 + 2r &\equiv 3 \mod 2 \\
2r &\equiv 2 \mod 5 \\
r &\equiv 1 \mod 5 \\
r &= 1 + 5s \\
x = 1 + 2(1 + 5s) &= 3 + 10s \\
x &\equiv 3 \mod 10
\end{aligned}
$$

Exempel

Sen löser vi

$$\begin{aligned} x &\equiv 3 \mod 10 \\ x &\equiv 5 \mod 7 \end{aligned}$$

Som tidigare:

$$\begin{aligned} x = 3 + 10s &\equiv 5 \mod 7 \\ 10s &\equiv 2 \mod 7 \\ 5s &\equiv 1 \mod 7 \end{aligned}$$

Hitta mult invers av 5 modulo 7:

$$\begin{aligned} s &\equiv 3 \mod 7 \\ s &= 3 + 7t \\ x = 3 + 10s &= 3 + 10(3 + 7t) \\ &= 33 + 70t \\ x &\equiv 33 \mod 70 \end{aligned}$$

Exempel

Sen löser vi

$$\begin{aligned} x &\equiv 3 \mod 10 \\ x &\equiv 5 \mod 7 \end{aligned}$$

Som tidigare:

$$\begin{aligned} x = 3 + 10s &\equiv 5 \mod 7 \\ 10s &\equiv 2 \mod 7 \\ 5s &\equiv 1 \mod 7 \end{aligned}$$

Hitta mult invers av 5 modulo 7:

$$\begin{aligned} s &\equiv 3 \mod 7 \\ s &= 3 + 7t \\ x = 3 + 10s &= 3 + 10(3 + 7t) \\ &= 33 + 70t \\ x &\equiv 33 \mod 70 \end{aligned}$$

Exempel

Sen löser vi

$$\begin{aligned} x &\equiv 3 \mod 10 \\ x &\equiv 5 \mod 7 \end{aligned}$$

Som tidigare:

$$\begin{aligned} x = 3 + 10s &\equiv 5 \mod 7 \\ 10s &\equiv 2 \mod 7 \\ 5s &\equiv 1 \mod 7 \end{aligned}$$

Hitta mult invers av 5 modulo 7:

$$\begin{aligned} s &\equiv 3 \mod 7 \\ s &= 3 + 7t \\ x = 3 + 10s &= 3 + 10(3 + 7t) \\ &= 33 + 70t \\ x &\equiv 33 \mod 70 \end{aligned}$$