Number Theory, Lecture 2

Linear Diophantine equations, congruenses

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Summary

Summary

Summary

1. **Linear Diophantine equations**
   - One eqn, two unknowns
   - One eqn, many unknowns
2. **Congruences**
   - Definition
   - Examples
   - Equivalence relation
   - $\mathbb{Z}_n$
   - Linear equations in $\mathbb{Z}_n$
3. **Chinese Remainder Thm**
   - Proof
   - Example

Diophantine eqn: want only integer solns

Theorem

Let $a, b, c \in \mathbb{Z}$. Put $d = \gcd(a, b)$. The equation

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

is solvable iff $d|c$.

Proof.

Necessity: if soln x, y exists, then $d|LHS$, so $d|c$.
Sufficiency: if $d|c$, then (DE) equivalent to

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

with $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$. So, can assume $d = 1$. $\square$

Theorem

Let $a, b, c \in \mathbb{Z}$, with $\gcd(a, b) = 1$. The equation

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

is solvable.

Proof.

Bezout: $1 = ax' + by'$, so $c = ax'c + by'c$. Put $x = x_p = x'c$, $y = y_p = y'c$. $\square$

All solutions

- If (x_1, y_2) and (x_2, y_2) both solutions to (DE1) then $(x_1 - x_2, y_1 - y_2)$ soln to

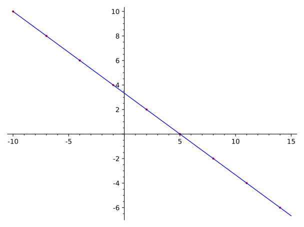
$$ax + by = 0 \tag{DEH}$$

- $(x, y) = (bn, -an)$, $n \in \mathbb{Z}$, are solns to (DEH)
- In fact all solutions: $ax = -by$ so $b|x$, thus $x = bn$. Hence $abn = -by$, so $-an = y$.
- So all solutions to (DE1) given by

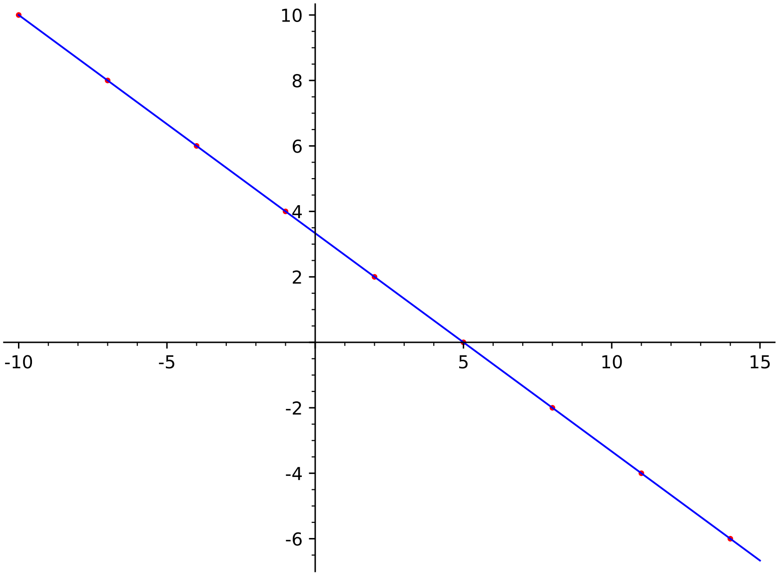
$$(x, y) = (x_p, y_p) + (x_h, y_h) = (x_p, y_p) + n(b, -a)$$

Example

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



- All solutions to $2x + 3y = 0$ are $(x_h, y_h) = n(3, -2)$, $n \in \mathbb{Z}$
- All solutions to original Diophantine is $(x, y) = (x_h, y_h) + (x_p, y_p) = (-10 + 3n, 10 - 2n)$


10
8
6
4
2
-2
-4
-6
-10
-5
5
10
15

Generalization

Theorem

The linear Diophantine eqn

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = c$$

is solvable when $\gcd(a_i, a_j) = 1$ *for* $i \neq j$*.*
(Stronger thm possible)

Proof.

Necessity: obvious. Sufficiency: study

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

Solvable with x, y integers. Now study

$$a_2 x_2 + \cdots + a_n x_n = y,$$

solvable by induction. $\square$

Example

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

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

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

Congruent modulo n

$\mathbb{P} \ni n > 1$.

Definition

For $a, b \in \mathbb{Z}$, we say that a is congruent to b modulo n,

$$a \equiv b \mod n$$

iff $n|(a-b)$.

Lemma

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

Example

- Odd numbers ar congruent to each other modulo 2
- $134632 \equiv 5645234532 \mod 100$
- $4 \equiv -1 \mod 5$,
- $4 \not\equiv 1 \mod 5$.

Definition

A relation $\sim$ on X is an equivalence relation if for all $x, y, z \in X$,

- Reflexive: $x \sim x$,
- Symmetric: $x \sim y \iff y \sim x$,
- Transitive: $x \sim y \quad \wedge \quad y \sim z \implies x \sim z$.

- For $x \in X$, $[x] = [x]_\sim = \{ y \in X | x \sim y \}$ is the equivalence class containing x, and x is a representative of the class
- The classes partition X:

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

  In other words, every element belongs to a unique eq. class.
- $x \sim y \iff x \in [y] \iff [x] = [y]$

- We collect the classes in a bag:

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

- Picture!
- Canonical surjection:

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

- Section:

$$s : X/\sim \to X$$

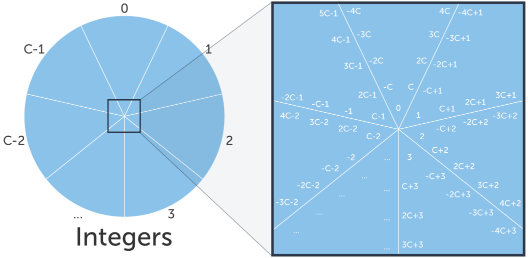
such that $\pi(s(A)) = A$.

- Transversal T: choice of exactly one representative from each class
- Normal form: $w = s \circ \pi$ satisfies $n(y) \sim y$, $n(n(y)) = n(y)$
- Concepts above related. Picture!

- Now fix positive integer $n > 1$, and let $\sim$ be the equivalence relation

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

- So $X = \mathbb{Z}$
- It is partitioned into n classes, why?



-

- If

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

  then $x \equiv x' \mod n$ if and only if $r = r'$.
- So a transversal is $T = \{0, 1, 2, \ldots, n-1\}$
- $\mathbb{Z} = [0] \cup [1] \cup \cdots \cup [n-1]$,
- $[a] = n\mathbb{Z} + a$,
- One section: $s([a]) = b$ with $b \equiv a \mod n$ and $0 \le b < n$, i.e., $b \in T$.
- Normal form: $kn + r \mapsto r$
- $\mathbb{Z}_n = \mathbb{Z}/(n\mathbb{Z}) = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$
- Can add congruence classes by adding representatives!

Lemma

Suppose that

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

Then

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

Proof.

$n|(a_1 - a_2)$, $n|(b_1 - b_2)$. Since $(a_1 - a_2) + (b_1 - b_2) = (a_1 + b_1) - (a_2 + b_2)$, $n|((a_1 + b_1) - (a_2 + b_2))$.
Furthermore,

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

□

Definition

We add and multiply congruence classes in $\mathbb{Z}_n$ by

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

$(\mathbb{Z}_n, +, [0], *, [1])$ is unitary, commutative ring:

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

Example

Addition and multiplication 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 multiplication modulo 5:

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

*	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

If $ac \equiv bc \mod n$ *and* $\gcd(c, n) = 1$, *then* $a \equiv b \mod n$.

Proof.

$n|(ac - bc)$, so $n|c(a - b)$, so $n|(a - b)$ (previous lemma). □

Example

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

yet

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

Lemma

If $T = \{t_1, \ldots, t_n\}$ transversal (mod n) and $\gcd(a, n) = 1$, then $aT = \{at_1, \ldots, at_n\}$ also transversal.

Proof.

Need only show $at_i \equiv at_j \mod n$ implies $i = j$. But $n | (at_i - at_j)$ gives $n | (t_i - t_j)$, which gives $i = j$, since T transversal. $\square$

Theorem

If $\gcd(a, n) = 1$ *then*

$$ax \equiv b \mod n$$

solvable; soln unique modulo n*.*

Proof.

Uniqueness: if $ax \equiv ax' \equiv b \mod n$ then $ax - ax' \equiv 0 \mod n$, so $x \equiv x' \mod n$.
Existence: $T = \{t_1, \ldots, t_n\}$ transversal. $aT = \{at_1, \ldots, at_n\}$ also transversal, so some $at_j \equiv 1 \mod n$. $\square$

Example

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

Theorem

Let $d = \gcd(a, n)$. The eqn

$$ax \equiv b \mod n$$

is solvable iff $d|b$; the soln then unique modulo n/d.

Proof.

Since $d = \gcd(a, n)$ then $d|n$ and $d|a$.
Necessity: if soln exists then $n|(ax - b)$, hence $d|b$.
Sufficiency: Suppose $d|b$.

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

Since $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$, we apply previous lemma: soln exists, unique modulo $\frac{n}{d}$. $\square$

Example

$$
\begin{aligned}
4x &\equiv 2 \mod 6 \\
2x &\equiv 1 \mod 3 \\
2x - 1 &\equiv 0 \mod 3
\end{aligned}
$$

- Diophantine eqn, $2x - 1 = 3y$
- soln for instance $x = -1, y = -1$
- Hence $x \equiv -1 \equiv 2 \mod 3$ is the soln, unique mod 3

Units in $\mathbb{Z}_n$

Definition

R commutative ring with one. An element $r \in R$ is a *unit* if exists $s \in R$ with $rs = 1$. R is a field if every element in $R \setminus \{0\}$ is a unit.

Theorem

- *$[a]_n \in \mathbb{Z}_n$ is a unit iff $\gcd(a, n) = 1$.*
- *$\mathbb{Z}_n$ is a field iff n is prime.*

Proof.

First part already proved. If n prime, then $\gcd(a, n) = 1$ for $n \not| a$. If $n = uv$ is composite, then $\gcd(u, n) = u > 1$. $\square$

Theorem

CRT If $\gcd(m,n)=1$, *then the system of eqns*

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

is solvable; the soln unique modulo mn.

Proof

Uniqueness: if

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

then

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

Thus $m|(x-x')$, $n|(x-x')$, so since $\gcd(m,n)=1$, $mn|(x-x')$.

Proof.

Existence: we have that $x \equiv a \mod m$, so $x = a + rm$, $r \in \mathbb{Z}$. Thus

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

This is a linear Diophantine eqn, solvable since $\gcd(m, n) = 1$.
Alternatively, $rm \equiv b - a \mod n$ is solvable (for r) since $\gcd(m, n) = 1$. $\square$

Example

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

Solve first two eqns:

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

Example

Now to solve

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

As before:

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

Find mult inverse of 5 modulo 7:

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

Example

Now to solve

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

As before:

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

Find mult inverse of 5 modulo 7:

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

Example

Now to solve

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

As before:

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

Find mult inverse of 5 modulo 7:

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