Lecture Notes

Advanced Discrete Structures

COT 4115.001 S15

2015-01-13

Recap

- Divisibility
- Prime Number Theorem
- Euclid’s Lemma
- Fundamental Theorem of Arithmetic
- Euclidean Algorithm

Basic Notions - Section 3.2

SOLVING $ax + by = d$

Definition

A **Diophantine equation** is a polynomial equation (in two or more unknowns) such that only the integer solutions are searched or studied.

<u>Examples</u>:

$3\,x + 3y = 2$ No integer solutions

$2\,x^2 + 5y^2 = -1$ No integer solutions

$3x + 5y = 2$ $\begin{cases} x = 4 + 5k \\ y = -2 - 3k \end{cases}, \ k \in \mathbb{Z}$

Definition

A set of integers is **computably enumerable** if there is an algorithm such that:

For each integer input n, if $n \in S$, then the algorithm eventually halts; otherwise it runs forever.

<u>Example</u>:

S: there is a run of exactly n 6's in the decimal expansion of

$$\tau = 2\pi = \mathbf{6}.2831853071795864769252867\mathbf{66}559\ldots$$

$$S = \{1,2,?,\ldots\}$$

Hilbert's 10^{th} Problem (1900)

Is there a general algorithm for solving all types of Diophantine equations?

Answer (Matiyasevich-Robinson-Davis-Putnam, 1977):
No, every *computably enumerable set* is Diophantine.

"Corresponding to any given consistent axiomatization of number theory, one can explicitly construct a Diophantine equation which has no solutions, but this fact cannot be proved within the given axiomatization."

Linear Diophantine Equations

Theorem:

Let $a, b \in \mathbb{Z}$ with $d = \gcd(a, b)$.

- The equation
$$aX + bY = c$$
has **no integral solutions** if $d \nmid c$.

- If $d \mid c$, then there are **infinitely many integral solutions**. Moreover, if $X = x$ and $Y = y$ is a particular solution of the equation, then all solutions are given by:
$$X = x + \left(\frac{b}{d}\right)k, \qquad Y = y + \left(\frac{a}{d}\right)k$$
where $k \in \mathbb{Z}$.

Linear Diophantine Equations

Consider:

$$aX + bY = c \quad \text{and} \quad d = \gcd(a, b)$$

If $d \mid c$ but $c \neq d$, solve instead:

$$\left(\frac{a}{d}\right) X + \left(\frac{b}{d}\right) Y = \left(\frac{c}{d}\right)$$

Now, $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{c}{d}$.

Solving $aX + bY = \gcd(a, b)$

1. **Extended Euclidean Algorithm**
   Form the following sequence:

$$x_0 = 0, \quad x_1 = 1, \quad x_j = -q_{j-1}x_{j-1} + x_{j-2},$$

$$y_0 = 1, \quad y_1 = 0, \quad y_j = -q_{j-1}y_{j-1} + y_{j-2},$$

Then

$$a\,x_n + b\,y_n = \gcd(a, b)$$

Recall from last Lecture

Use the Euclidean algorithm to find $\gcd(600, 252)$:

$$600 = \mathbf{2} \cdot 252 + 96 \qquad q_1 = 2$$

$$252 = \mathbf{2} \cdot 96 + 60 \qquad q_2 = 2$$

$$96 = \mathbf{1} \cdot 60 + 36 \qquad q_3 = 1$$

$$60 = \mathbf{1} \cdot 36 + 24 \qquad q_4 = 1$$

$$36 = \mathbf{1} \cdot 24 + 12 \qquad q_5 = 2$$

$$24 = \mathbf{2} \cdot 12 + 0 \qquad q_6 = 2$$

$$\gcd(600, 252) = 12$$

Solving Linear Diophantine Equations

Example:

$$252\,x + 600\,y = \gcd(252{,}600) = 12$$

$$q_1 = 2, \quad q_2 = 2, \quad q_3 = 1, \quad q_4 = 1, \quad q_5 = 1, \quad q_6 = 2$$

$x_0 = 0, \quad x_1 = 1,$
$x_j = -q_{j-1}x_{j-1} + x_{j-2}$

$y_0 = 1, \quad y_1 = 0,$
$y_j = -q_{j-1}y_{j-1} + y_{j-2}$

$x_2 = (-2)\,x_1 + x_0 = -2,$
$x_3 = (-2)\,x_2 + x_1 = 5,$
$x_4 = (-1)\,x_3 + x_2 = -7,$
$x_5 = (-1)\,x_4 + x_3 = 12,$
$x_6 = (-1)\,x_5 + x_4 = -\mathbf{19},$

$y_2 = (-2)\,y_1 + y_0 = 1,$
$y_3 = (-2)\,y_2 + y_1 = -2,$
$y_4 = (-1)\,y_3 + y_2 = 3,$
$y_5 = (-1)\,y_4 + y_3 = -5,$
$y_6 = (-1)\,y_5 + y_4 = \mathbf{8},$

$$252(-19) + 600(8) = 12 = \gcd(252{,}600)$$

Solving Linear Diophantine Equations

Recursive Form:

$x_0 = 0, \qquad x_1 = 1, \qquad x_j = -q_{j-1}x_{j-1} + x_{j-2},$

$y_0 = 1, \qquad y_1 = 0, \qquad y_j = -q_{j-1}y_{j-1} + y_{j-2},$

Matrix Form:

$$\begin{pmatrix} 0 & 1 \\ 1 & -q_{j-1} \end{pmatrix} \begin{pmatrix} x_{j-2} & y_{j-2} \\ x_{j-1} & y_{j-1} \end{pmatrix}$$

$$= \begin{pmatrix} x_{j-1} & y_{j-1} \\ x_{j-2} - q_{j-1}\, x_{j-1} & y_{j-2} - q_{j-1}\, y_{j-1} \end{pmatrix} = \begin{pmatrix} x_{j-1} & y_{j-1} \\ x_j & y_j \end{pmatrix}$$

Solving Linear Diophantine Equations

$$\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} -5 & 8 \\ \mathbf{12} & -\mathbf{19} \end{pmatrix}$$

Two was to solve $ax + by = \gcd(a, b)$

"Reverse Euclidean Algorithm" (Substitution)

$600 = 2 \cdot 252 + 96$	$12 = 8(600 - 2 \cdot 252) - 3 \cdot 252 = 8 \cdot 600 - 19 \cdot 252$
$252 = 2 \cdot 96 + 60$	$12 = 2 \cdot 96 - 3 \cdot (252 - 2 \cdot 96) = 8 \cdot 96 - 3 \cdot 252$
$96 = 1 \cdot 60 + 36$	$12 = 2 \cdot (96 - 1 \cdot 60) - 1 \cdot 60 = 2 \cdot 96 - 3 \cdot 60$
$60 = 1 \cdot 36 + 24$	$12 = 36 - 1 \cdot (60 - 1 \cdot 36) = 2 \cdot 36 - 1 \cdot 60$
$36 = 1 \cdot 24 + 12$	$12 = 36 - 1 \cdot 24$
$24 = 2 \cdot 12 + 0$	

Basic Notions - Section 3.3

CONGRUENCES

Definition

Let $a, b, n \in \mathbb{Z}$ with $n \neq 0$. We say that

$$a \equiv b \pmod{n}$$

(read: a is **congruent** to b mod n) if $n \mid a - b$, i.e., there exists a $k \in \mathbb{Z}$ such that

$$a - b = k\,n \qquad \text{or} \qquad a = b + k\,n.$$

Examples

$-2 \equiv 9 \pmod{11}$ $\quad -2 - 9 = -11 = -1 \cdot 11$

$123 \equiv 3 \pmod{10}$ $\quad 123 - 3 = 120 = 12 \cdot 10$

$21 \equiv 21 \pmod{10}$ $\quad 21 - 21 = 0 = 0 \cdot 10$

$21 \equiv 0 \pmod{21}$ $\quad 21 - 0 = 21 = 1 \cdot 21$

Proposition

Let $a, n \in \mathbb{Z}$ with $n \neq 0$.

- $a \equiv 0 \pmod{n}$ if and only if $n \mid a$.

Proof. ($\Rightarrow$) Suppose $a \equiv 0 \pmod{n}$, i.e., there exists a $k \in \mathbb{Z}$ such that $a - 0 = k\,n$. By definition, $n \mid a$.

($\Leftarrow$) Likewise, if $n \mid a$ there exists a $k \in \mathbb{Z}$ such that $a - 0 = k\,n$ which means $a \equiv 0 \pmod{n}$. $\blacksquare$

- $a \equiv a \pmod{n}$.

Proof. Note that $a - a = 0 = 0 \cdot n$, thus $a \equiv a \pmod{n}$. $\blacksquare$

Proposition

Let $a, b, n \in \mathbb{Z}$ with $n \neq 0$.

- $a \equiv b \pmod{n}$ if and only if $b \equiv a \pmod{n}$.

Proof.
($\Rightarrow$) Suppose $a \equiv b \pmod{n}$, i.e., there exists a $k \in \mathbb{Z}$ such that $a - b = k\,n$. Multiply both sides by -1 to get:

$$b - a = -(a - b) = -(k\,n) = (-k)\,n$$

which means $b \equiv a \pmod{n}$.

($\Leftarrow$) Proof is similar; interchange a and b. $\blacksquare$

Proposition

Let $a, b, c, n \in \mathbb{Z}$ with $n \neq 0$. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Proof. By definition, $a = b + k_1 n$ and $b = c + k_2 n$ for some integers $k_1, k_2 \in \mathbb{Z}$. Thus,

$$a = b + k_1 n = (c + k_2 n) + k_1 n = c + (k_2 + k_1)\, n$$

which means $a \equiv c \pmod{n}$. ■

Proposition

Let $a, b, c, d, n \in \mathbb{Z}$ with $n \neq 0$, and suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then

$$a + c \equiv b + d \pmod{n}.$$

Proof.

We have that $a = b + n\,k_1$ and $c = d + n\,k_2$ for some $k_1, k_2 \in \mathbb{Z}$. Thus,

$$\begin{aligned} a + c &= (b + n\,k_1) + (d + n\,k_2) \\ &= (b + d) + n\,(k_1 + k_2), \end{aligned}$$

i.e., $a + c \equiv b + d \pmod{n}$. ∎

Proposition

Let $a, b, c, d, n \in \mathbb{Z}$ with $n \neq 0$, and suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then

$$a\,c \equiv b\,d \pmod{n}\,.$$

Proof.

We have that $a = b + n\,k_1$ and $c = d + n\,k_2$ for some $k_1, k_2 \in \mathbb{Z}$. Thus,

$$\begin{aligned} a\,c &= (b + n\,k_1)(d + n\,k_2) \\ &= b\,d + n\,(d\,k_1 + b\,k_2 + n\,k_1\,k_2), \end{aligned}$$

i.e., $a\,c \equiv b\,d \pmod{n}$. ■

Examples

We can do algebra modulo n:

$$x + 7 \equiv 3 \pmod{11}$$

$$x + 7 + (-7) \equiv 3 + (-7) \pmod{11}$$

$$x \equiv -4 \pmod{11}$$

Remember, this means that

$$\ldots, \quad x = -15, \quad x = -4, \quad x = 7, \quad x = 18, \quad \ldots$$

are all solutions.

Basic Notions - Section 3.3.1

DIVISION

Subtraction and Division

<u>Subtraction</u>: Addition of negative numbers

$$7 - 4 = 7 + (-4)$$

<u>Division</u>: Multiplication of fractions

$$\frac{3}{4} = 3\left(\frac{1}{4}\right) = 3 \cdot 4^{-1}$$

<u>Negative numbers</u>:

-4 is the number k which solves $4 + k = 0$

<u>Negative powers</u>:

4^{-1} is the number k which solves $4 \cdot k = 1$

Proposition

Let $a, b, c, n \in \mathbb{Z}$ with $n \neq 0$ and $\gcd(a, n) = 1$.

If $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{n}$.

Proof. Recall that $\gcd(a, n) = 1$ implies that there exist $x, y \in \mathbb{Z}$ such that

$$a\,x + n\,y = 1 \implies (b - c)(a\,x + n\,y) = (b - c)$$

or $$(a\,b - a\,c)\,x + (b\,y - c\,y)\,n = b - c.$$

Since $n \mid ab - ac$ and $n \mid (by - cy)\,n$, $n \mid b - c$ also. Thus, $b \equiv c \pmod{n}$. $\blacksquare$

Example

Solve: $2x + 5 \equiv 9 \pmod{11}$

$$2x + 5 + (-5) \equiv 9 + (-5) \pmod{11}$$

$$2x \equiv 4 \pmod{11}$$

$$x \equiv 2 \pmod{11}$$

since $\gcd(2,11) = 1.$

Example

Solve: $2x + 5 \equiv 8 \pmod{11}$

$$2x + 5 + (-5) \equiv 8 + (-5) \pmod{11}$$

$$2x \equiv 3 \pmod{11}$$

$$2^{-1}(2x) \equiv 2^{-1}3 \pmod{11}$$

since $\gcd(2,11) = 1$.

But what does $2^{-1} \pmod{11}$ mean?

$2^{-1} \pmod{11}$

Want to find a $k \in \mathbb{Z}$ with the following property:

$$k \cdot 2 \equiv 1 \pmod{11},$$

this would mean

$$2k - 1 = 11j$$

for some $j \in \mathbb{Z}$. Rewritten, we are looking for $j, k \in \mathbb{Z}$ such that

$$2k - 11j = 1.$$

Using the extended Euclidean algorithm: $k = 6,\ j = 1$

Check: $6 \cdot 2 = 12 \equiv 1 \pmod{11}$ ✓

Example

Solve: $2x + 5 \equiv 8 \pmod{11}$

$$2x + 5 + (-5) \equiv 8 + (-5) \pmod{11}$$

$$2x \equiv 3 \pmod{11}$$

$$2^{-1}(2x) \equiv 2^{-1}3 \pmod{11}$$

$$x \equiv 6 \cdot 3 = 18 \equiv 7 \pmod{11}$$

Proposition

Suppose $\gcd(a, n) = 1$. Let $s, t \in \mathbb{Z}$ s.t. $as + nt = 1$. Then

$$a\,s \equiv 1 \pmod{n}.$$

[The integer s is said to be the **multiplicative inverse** of a modulo n and written a^{-1}.]

Proof.

Since $a\,s - 1 = n\,t$, $a\,s \equiv 1 \pmod{n}$. ■

What can happen when $\gcd(a, n) \neq 1$? $3k \not\equiv 1 \pmod{6}$

Example

However,

$$15\,x \equiv 21 \pmod{39}$$

$$3 \cdot 5 \cdot x \equiv 3 \cdot 7 \pmod{39}$$

$$5\,x \equiv 7 \pmod{39}$$

Here we're looking for $5^{-1} \pmod{39}$. Find j, k such that

$$39j + 5k = 1$$

by the extended Euclidean algorithm: $j = -1, k = 8$ works, so

$$x \equiv 8 \cdot 7 = 56 \equiv 17 \pmod{39}$$

Other solutions: $x \equiv 4 \pmod{39}$ and $x \equiv 30 \pmod{39}$.

Solving $ax \equiv c \pmod{n}$

- <u>If $\gcd(a, n) = 1$</u>:
  1. Use the extended Euclidean algorithm to find $s, t \in \mathbb{Z}$ such that $a\,s + n\,t = 1$.
  2. The solution is $x \equiv s\,c \pmod{n}$.

- <u>If $\gcd(a, n) > 1$</u>:
  1. If d does not divide b, there is no solution.
  2. Assume $d \mid b$. Consider the new congruence
     $$(a/d)\,x \equiv b/d \pmod{n}$$
     and obtain the new solution $x = x_0$.
  3. Solutions to original congruence are:

$$x_0,\ x_0 + \left(\frac{n}{d}\right),\ x_0 + 2\left(\frac{n}{d}\right),\ \ldots,\ x_0 + (d-1)\left(\frac{n}{d}\right) \pmod{n}$$

Non-linear Equations

An important congruence:

$$x^2 \equiv a \pmod{n}.$$

Example

$$x^2 \equiv 1 \pmod{5}$$

Check:

$$0^2 = 0 \equiv 0 \pmod{5}$$
$$1^2 = 1 \equiv 1 \pmod{5}$$
$$2^2 = 4 \equiv 4 \pmod{5}$$
$$3^2 = 9 \equiv 4 \pmod{5}$$
$$4^2 = 16 \equiv 1 \pmod{5}$$

Solutions: $x \equiv \pm 1 \pmod{5}$

Non-linear Equations

Example

$$x^2 \equiv 1 \pmod{15}$$

Check:

$$1^2 = 1 \equiv 1 \pmod{15}$$
$$2^2 = 4 \equiv 4 \pmod{15}$$
$$3^2 = 9 \equiv 9 \pmod{15}$$
$$4^2 = 16 \equiv 1 \pmod{15}$$
$$5^2 = 25 \equiv 10 \pmod{15}$$
$$6^2 = 36 \equiv 6 \pmod{15}$$
$$7^2 = 49 \equiv 4 \pmod{15}$$
$$8^2 = 64 \equiv 4 \pmod{15}$$
$$9^2 = 81 \equiv 6 \pmod{15}$$
$$10^2 = 100 \equiv 10 \pmod{15}$$
$$11^2 = 121 \equiv 1 \pmod{15}$$
$$12^2 = 144 \equiv 9 \pmod{15}$$
$$13^2 = 169 \equiv 4 \pmod{15}$$
$$14^2 = 196 \equiv 1 \pmod{15}$$

Solutions: $x \equiv \pm 1, \pm 4 \pmod{5}$

Basic Notions - Section 3.3.2

WORKING WITH FRACTIONS

Don’t

- Use multiplicative inverse notation: a^{-1}

- Always check that the integer a^{-1} actually exists, i.e., $\gcd(a, n) = 1$.