Number Theory and its Applications

- Modular Exponentiation
- Euclidean Algorithm for GCD
- Solving Linear Congruences
- Chinese Remainder Theorem and Application to Arithmetic with large numbers
- Covered in Sections 3.6 and 3.7

Based on Rosen and slides by K. Busch

Modular Arithmetic Recap

$a, b \in Z$ $\quad m \in Z^+$

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

" a is congruent to b modulo m "

$$a \bmod m = b \bmod m$$

Examples:

$1 \equiv 13 \pmod{12}$ $\quad 0 \equiv m \pmod{m}$

$11 \equiv 5 \pmod{6}$ $\quad k \cdot m \equiv 0 \pmod{m}$

Equivalent statements

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

$$\Updownarrow$$

$$a \bmod m = b \bmod m$$

$$\Updownarrow$$

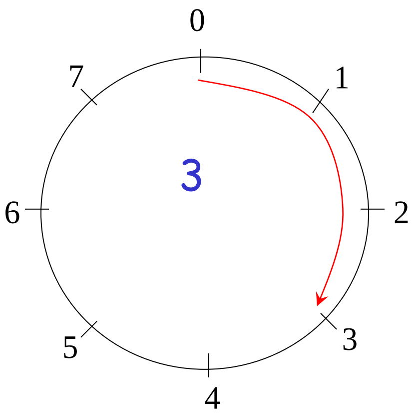
$$m \mid a - b$$

$$\Updownarrow$$

$$\exists k \in Z, \quad a = b + km$$

3

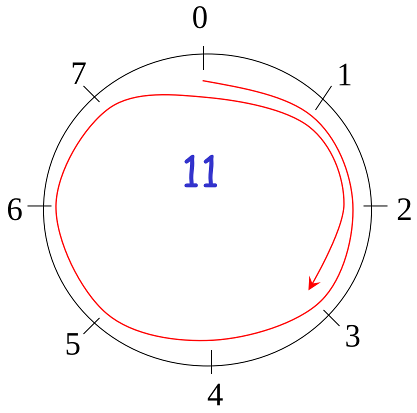
$$3 \bmod 8 = 3$$



Length of line represents number

4

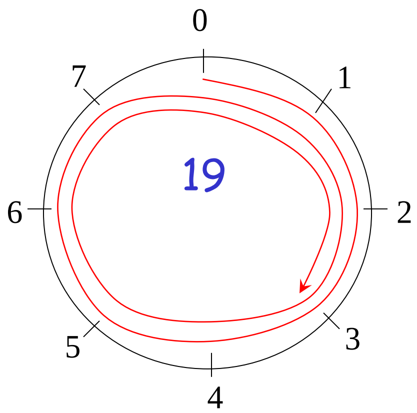
$$11 \bmod 8 = 3$$



Length of line represents number

5

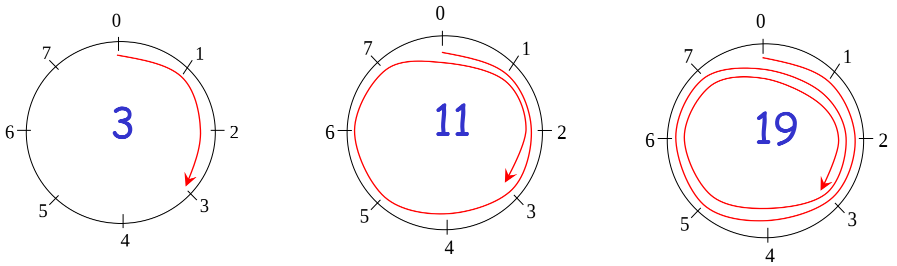
$$19 \bmod 8 = 3$$



Length of line represents number

6

$$3 \equiv 11 \equiv 19 \pmod 8$$



All lines terminate in same number

"Congruence class" of a modulo m :

$$S_a = \{b \mid a \equiv b \pmod m\}$$

There are m congruence classes:

$$S_0, S_1, \ldots, S_{m-1}$$

Closure under addition:

$$\left.\begin{array}{l} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{array}\right\} \Rightarrow a + c \equiv b + d \pmod{m}$$

Proof sketch:

$$\left.\begin{array}{l} a \equiv b \pmod{m} \Rightarrow a = b + sm \\ c \equiv d \pmod{m} \Rightarrow c = d + tm \end{array}\right\} a + c = d + b + (s+t)m$$

Closure under multiplication:

$$\left.\begin{array}{l} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{array}\right\} \Rightarrow a \cdot c \equiv b \cdot d \pmod{m}$$

Proof sketch:

$$\left.\begin{array}{l} a \equiv b \pmod{m} \Rightarrow a = b + sm \\ c \equiv d \pmod{m} \Rightarrow c = d + tm \end{array}\right\} \begin{array}{l} a \cdot c = (b + sm)(d + tm) \\ \quad = \mathrm{bd} + m(bt + ds + stm) \end{array}$$

Closure under mod:

$$a \bmod m = (a \bmod m) \bmod m$$

(Follows from definition of mod)

$$(7 \bmod 5) = 2$$
$$(7 \bmod 5) \bmod 5 = 2 \bmod 5 = 2$$

11

Useful results for arithmetic with large numbers:

$$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

$$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$$

(Follows from previous slides)

Example:

$$\begin{aligned} 57 \cdot 55 \bmod 50 &= ((57 \bmod 50)(55 \bmod 50)) \bmod 50 \\ &= 7 \cdot 5 \bmod 50 \\ &= 35 \end{aligned}$$

12

Modular exponentiation

Compute $b^n \bmod m$ efficiently using small numbers

Binary expansion of n

$$b^n = b^{\overbrace{a_{k-1}2^{k-1}+\cdots+a_1 2+a_0}} = b^{a_{k-1}2^{k-1}} \cdots b^{a_1 2} b^{a_0}$$

$b^n \bmod m$

$= b^{a_{k-1}2^{k-1}} \cdots b^{a_1 2} b^{a_0} \bmod m$

$= ((b^{a_{k-1}2^{k-1}} \bmod m) \cdot \cdots \cdot (b^{a_1 2} \bmod m) \cdot (b^{a_0} \bmod m)) \bmod m$

13

Example: $3^{644} \bmod 645 = 36$

$$644 = 1010000100 = 2^9 + 2^7 + 2^2$$

$$3^{644} = 3^{2^9+2^7+2^2} = 3^{2^9} 3^{2^7} 3^{2^2}$$

$3^{644} \bmod 645$

$= (3^{2^9} 3^{2^7} 3^{2^2}) \bmod 645$

$= ((3^{2^9} \bmod 645)(3^{2^7} \bmod 645)(3^{2^2} \bmod 645) \bmod 645)$

14

Compute the powers of 3 efficiently

$$3^2 \bmod 645 = 9 \bmod 645 = 9$$

$$3^{2^2} \bmod 645 = \left(3^2\right)^2 \bmod 645 = ((3^2 \bmod 645)(3^2 \bmod 645)) \bmod 645 = (9 \cdot 9 \bmod 645) = 81$$

$$3^{2^3} \bmod 645 = \left(3^{2^2}\right)^2 \bmod 645 = ((3^{2^2} \bmod 645)(3^{2^2} \bmod 645)) \bmod 645 = 81 \cdot 81 \bmod 645 = 111$$

$$\vdots$$

Use the powers of 3 to get result efficiently

$$\begin{aligned}
&3^{644} \\
&= (3^{2^9} 3^{2^7} 3^{2^2} \bmod 645) \\
&= (3^{2^9} 3^{2^7} (3^{2^2} \bmod 645) \bmod 645) = (3^{2^9} 3^{2^7} 81 \bmod 645) \\
&= (3^{2^9} (((3^{2^7} \bmod 645) 81) \bmod 645) \bmod 645) = (3^{2^9} ((396 \cdot 81) \bmod 645) \bmod 645) = (3^{2^9} \cdot 471 \bmod 645) \\
&= (((3^{2^9} \bmod 645) \cdot 471) \bmod 645) = 111 \cdot 471 \bmod 645 = 36
\end{aligned}$$

Modular_Exponentiation(b, n, m) {

$\quad n = (a_{n-1} a_{n-2} \cdots a_1 a_0)_2$

$\quad x \leftarrow 1$

$\quad power \leftarrow b \bmod m$

$\quad$ for $i = 0$ to $k-1$ {

$\quad\quad$ if ($a_i = 1$) $x \leftarrow (x \cdot power) \bmod m$

$\quad\quad power \leftarrow (power \cdot power) \bmod m$

$\quad$ }

$\quad$ return x $\quad (b^n \bmod m)$

}

Recall: Greatest Common Divisor

$\gcd(a,b) =$ largest integer d
such that $d \mid a$ and $d \mid b$

$a, b \in Z$

$|a| + |b| \neq 0$

Examples: $\gcd(24,36) = 12$

Common divisors of 24, 36: 1, 2, 3, 4, 6, 12

$\gcd(17,22) = 1$

Common divisors of 17, 22: 1

17

Trivial cases:

$\gcd(m,1) = 1$

$\gcd(m,0) = m \qquad m \neq 0$

If $\gcd(a,b) = 1$ then a, b are relatively prime

a and b have no common factors

Example: 21, 22 are relatively prime

$\gcd(21,22) = 1$

18

How do we compute GCD efficiently?

(Finding prime factorization is slow)

Theorem: If $a = b \cdot q + r$ $\qquad 0 \le r < b$
then $\gcd(a,b) = \gcd(b,r)$

Proof:

$d \mid a$, $d \mid b$ ⇒ $a = ds$, $b = dt$ ⇒ $r = d(s - tq)$, $b = dt$ ⇒ $d \mid r$, $d \mid b$

Thus, (a,b) and (b,r) have the same set of common divisors

End of proof

divisions $a = r_0$ $b = r_1$ remainder

$$
\begin{array}{llcll}
r_0 / r_1 & r_0 & = & r_1 q_1 + r_2 & 0 < r_2 < r_1 \\
r_1 / r_2 & r_1 & = & r_2 q_2 + r_3 & 0 < r_3 < r_2 \\
\vdots & & \vdots & & \vdots \\
r_{n-2} / r_{n-1} & r_{n-2} & = & r_{n-1} q_{n-1} + r_n & 0 < r_n < r_{n-1} \\
r_{n-1} / r_n & r_{n-1} & = & r_n q_n + 0 &
\end{array}
$$

first zero result

$$
\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3) \cdots
$$
$$
\cdots = \gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n
$$

21

$a = 662$ $b = 414$

$$
\begin{array}{rcll}
662 & = & 414 \cdot 1 + 248 & r_2 = 248 < 414 = r_1 \\
414 & = & 248 \cdot 1 + 166 & r_3 = 166 < 248 = r_2 \\
248 & = & 166 \cdot 1 + 82 & r_4 = 82 < 166 = r_3 \\
166 & = & 82 \cdot 2 + 2 & r_5 = 2 < r_4 = 82 \\
82 & = & 2 \cdot 41 + 0 &
\end{array}
$$

result

$$
\gcd(662, 414) = \gcd(414, 248) = \gcd(248, 166)
$$
$$
= \gcd(166, 82) = \gcd(82, 2) = \gcd(2, 0) = 2
$$

22

Euclidean Algorithm for GCD

gcd(a, b) {
  $x \leftarrow a$
  $y \leftarrow b$
  while ($y \neq 0$) {
    $r \leftarrow x \bmod y$
    $x \leftarrow y$
    $y \leftarrow r$
  }
  return x
}

23

Useful Result regarding GCDs

if $a, b \in Z^+$ then there are $s, t \in Z$ such that

$$\gcd(a, b) = sa + tb$$

(i.e., gcd is a linear combination of a and b)

Example: $\gcd(6,14) = 2 = (-2) \cdot 6 + 1 \cdot 14$

24

The linear combination can be found by reversing the Euclidian algorithm steps

$$\gcd(252,198) = 18 = 4 \cdot 252 - 5 \cdot 198$$

$$\begin{aligned} 252 &= 1 \cdot 198 + 54 \\ 198 &= 3 \cdot 54 + 36 \\ 54 &= 1 \cdot 36 + 18 \\ 36 &= 2 \cdot 18 + 0 \end{aligned}$$

$$\begin{aligned} &\gcd(252,198) = 18 \\ &= 54 - 1 \cdot 36 = 54 - 1 \cdot (198 - 3 \cdot 54) \\ &= 4 \cdot 54 - 1 \cdot 198 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 \\ &= 4 \cdot 252 - 5 \cdot 198 \end{aligned}$$

Linear congruences

We want to solve this equation for x

$$a \cdot x \equiv b \pmod{m}$$

$$\Downarrow$$

$$x \equiv \,?\, \pmod{m}$$

Inverse of a: $\bar{a}a \equiv 1 \pmod{m}$

$$\left.\begin{array}{r} a \cdot x \equiv b \pmod{m} \\ \bar{a} \equiv \bar{a} \bmod m \end{array}\right\} \Rightarrow \bar{a}a \cdot x \equiv \bar{a}b \pmod{m}$$

$$\left.\begin{array}{r} \bar{a}a \equiv 1 \pmod{m} \\ x \equiv x \pmod{m} \end{array}\right\} \Rightarrow \bar{a}a \cdot x \equiv 1 \cdot x \pmod{m}$$

$$\Downarrow$$

$$x \equiv \bar{a}b \pmod{m}$$

27

Theorem: If a and m are relatively prime then the inverse $\bar{a}$ modulo m exists

Proof: $\gcd(a, m) = 1 = sa + tm$ (linear combo theorem)

$$\Downarrow$$

$sa \equiv 1 \pmod{m}$ (Def. of mod)

$$\Downarrow$$

$\bar{a} = s$ (Def. of inverse mod m)

End of proof

28

Example: solve equation $3x \equiv 4 \pmod 7$

$a = 3, b = 4, m = 7$

Inverse of 3:

$\gcd(3,7) = 1 = -2 \cdot 3 + 1 \cdot 7 \Rightarrow -2 \cdot 3 \equiv 1 \pmod m$

$\Rightarrow \bar{a} = -2$

$$x \equiv \bar{a} b \pmod m$$

$$x \equiv -2 \cdot 4 \pmod 7 \equiv -8 \pmod 7 \equiv 6 \bmod 7$$

29

A Chinese Puzzle

(by Sun-Tzu, 300-500 AD)

I have some things whose number you don't know.

If divided by 3, the remainder is 2

If divided by 5, the remainder is 3

If divided by 7, the remainder is 2

How many things do I have?

30

Sun-Tzu's Puzzle

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

What is x?

Chinese remainder theorem (CRT)

$m_1, m_2, \ldots, m_n$:pairwise relatively prime

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

Has unique solution for x modulo $m = m_1 \cdot m_2 \cdots m_n$

Unique solution modulo $m = m_1 \cdot m_2 \cdots m_n$:

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$$

where $M_k = \frac{m}{m_k}$

y_k :inverse of M_k modulo m_k

33

Explanation: y_k :inverse of M_k modulo m_k

$$M_k = \frac{m}{m_k}$$

$$M_k y_k \equiv 1 \bmod m_k$$

k = 1: $M_1 y_1 \equiv 1 \bmod m_1$

$$x = a_1 M_1 y_1 + \underbrace{a_2 M_2 y_2}_{0 \pmod{m_1}} + \cdots + \underbrace{a_n M_n y_n}_{0 \pmod{m_1}}$$

$M_{k \neq 1} \equiv 0 \pmod{m_1}$

$x \equiv a_1 M_1 y_1 \pmod{m_1}$

$x \equiv a_1 \pmod{m_1}$ i.e., x satisfies 1st equation

Similar for any m_j

34

Example: $x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

$m = 3 \cdot 5 \cdot 7 = 105$

$M_1 = m/3 = 105/3 = 35$ $\quad y_1 = 2$

$M_2 = m/5 = 105/5 = 21$ $\quad y_2 = 1$

$M_3 = m/7 = 105/7 = 15$ $\quad y_3 = 1$

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$$
$$= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1$$
$$= 233 \equiv 23 \pmod{3 \cdot 5 \cdot 7} \equiv 23 \pmod{105}$$

35

An Application of CRT

Perform arithmetic with large numbers using arithmetic modulo small numbers

Example: Suppose your CPU can only perform fast arithmetic for positive integers < 100, but your input numbers are huge.

36

An Application of CRT

Idea: Convert your large numbers to small numbers < 100 using mod, perform modular arithmetic, convert back using CRT.

Choose relatively prime numbers < 100

$$m_1 = 99, \quad m_2 = 98, \quad m_3 = 97, \quad m_4 = 95$$

$$m = 99 \cdot 98 \cdot 97 \cdot 95 = 89{,}403{,}930$$

Any number smaller than m has unique Representation (CRT)

$$123{,}684 = (33, 8, 9, 89)$$

$$123{,}684 \bmod 99 = 33$$
$$123{,}684 \bmod 98 = 8$$
$$123{,}684 \bmod 97 = 9$$
$$123{,}684 \bmod 95 = 89$$

Decimal — Mod representation

$$123{,}684 = (33, 8, 9, 89)$$

$$+ \quad 413{,}456 = (32, 92, 42, 16)$$

$$(65 \bmod 99, 100 \bmod 98, 51 \bmod 97, 105 \bmod 95)$$

$$537{,}140 = (65, 2, 51, 10)$$

Obtain answer x from 65, 2, 51, 10 using the Chinese remainder theorem