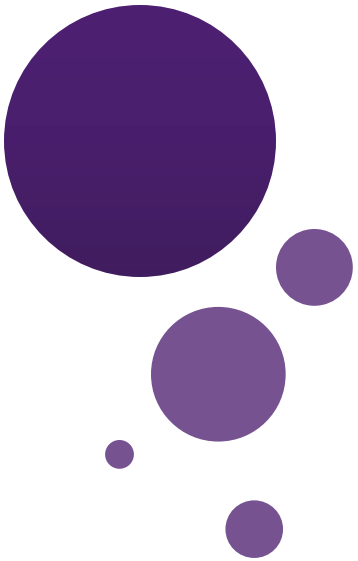
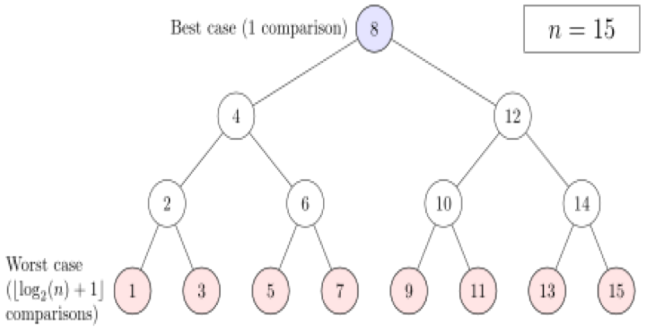


Lecture 5: Number Theory

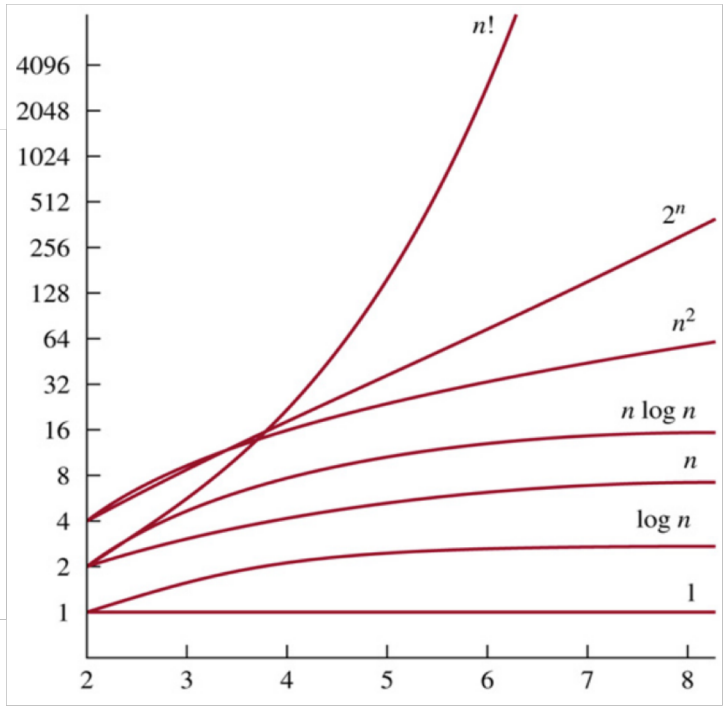
Dr. Chengjiang Long
Computer Vision Researcher at Kitware Inc.
Adjunct Professor at SUNY at Albany.
Email: **clong2@albany.edu**

Recap Previous Lecture

- Algorithm (definition, properties, search problem, sorting problem, and optimization problem)
- Growth functions and complexity (big-O, big-Omega, big-Theta)



$$O(1) \subseteq O(\log n) \subseteq O(n) \subseteq O(n \log n) \subseteq O(n^2) \subseteq O(c^n) \subseteq O(n!)$$



Recap Previous Lecture

- Integer division (divisibility, properties of divisibility, integer division of negative number)
- Modular arithmetic (congruency, congruency of sum and product, properties of arithmetic modulo *m*)

$(a + b) \pmod m = ((a \bmod m) + (b \bmod m)) \bmod m$
$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m.$

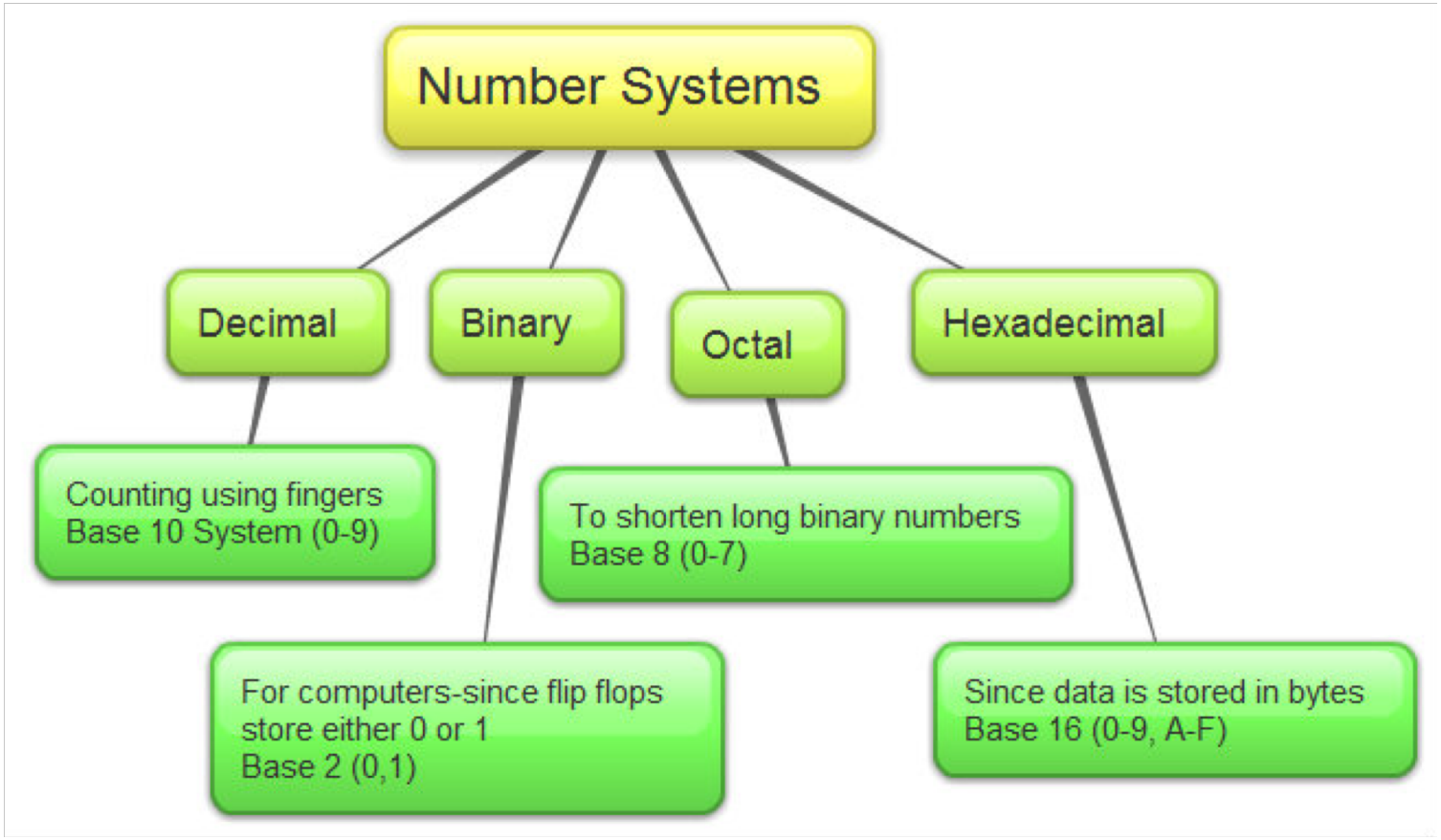
Closure: If a and b belong to $\mathbf{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to $\mathbf{Z}_m$.
Associativity: If a, b, and c belong to $\mathbf{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.
Commutativity: If a and b belong to $\mathbf{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.
Identity elements: The elements 0 and 1 are identity elements for addition and multiplication modulo m, respectively.
If a belongs to $\mathbf{Z}_m$, then $a +_m 0 = a$ and $a \cdot_m 1 = a$.

Outline

- Integer Representation
- Primes and Greatest Common Divisors
- Chinese Remainder Theorem

Integer Representation

Representations of integers



Representations of Integers

- In the modern world, we use *decimal,* or *base* 10, *notation* to represent integers. For example when we write 965, we mean $9 \cdot 10^2 + 6 \cdot 10^1 + 5 \cdot 10^0$.
- We can represent numbers using any base *b*, where *b* is a positive integer greater than 1.
- The bases *b* = 2 (*binary*), *b* = 8 (*octal*) , and *b*= 16 (*hexadecimal*) are important for computing and communications

Binary Expansions

- Most computers represent integers and do arithmetic with binary (base 2) expansions of integers. In these expansions, the only digits used are 0 and 1.

$$2^0 = 1$$
$$2^1 = 2$$
$$2^2 = 2 \times 2 = 4$$
$$2^3 = 2 \times 2 \times 2 = 8$$
$$2^4 = 2 \times 2 \times 2 \times 2 = 16$$

Binary Expansions

- **Example**: What is the decimal expansion of the integer that has $(1\ 0101\ 1111)_2$ as its binary expansion?
- **Solution**:
- $(1\ 0101\ 1111)_2 = 1\cdot 2^8 + 0\cdot 2^7 + 1\cdot 2^6 + 0\cdot 2^5 + 1\cdot 2^4 + 1\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0 = 351.$

Binary Expansions

- **Example**: What is the decimal expansion of the integer that has $(11011)_2$ as its binary expansion?
- **Solution**:
- $(11011)_2 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 27$.

Octal Expansions

- The octal expansion (base 8) uses the digits {0,1,2,3,4,5,6,7}.
- **Example**: What is the decimal expansion of the number with octal expansion $(7016)_8$?
- **Solution**: $7 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8^1 + 6 \cdot 8^0 = 3598$
- **Example**: What is the decimal expansion of the number with octal expansion $(111)_8$?
- **Solution**: $1 \cdot 8^2 + 1 \cdot 8^1 + 1 \cdot 8^0 = 64 + 8 + 1 = 73$

Hexadecimal Expansions

- The hexadecimal expansion needs 16 digits, but our decimal system provides only 10. So letters are used for the additional symbols. The hexadecimal system uses the digits {0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F}. The letters A through F represent the decimal numbers 10 through 15.

Hexadecimal Expansions

- **Example**: What is the decimal expansion of the number with hexadecimal expansion $(2AE0B)_{16}$?
- **Solution**:
- $2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16^1 + 11 \cdot 16^0 = 175627$
- **Example**: What is the decimal expansion of the number with hexadecimal expansion $(E5)_{16}$?
- **Solution**: $14 \cdot 16^1 + 5 \cdot 16^0 = 224 + 5 = 229$

Base Conversion

To construct the base b expansion of an integer n:

- Divide n by b to obtain a **quotient** and **remainder**.
  $n = bq_0 + a_0 \quad 0 \leq a_0 \leq b$
- The remainder, a_0, is the rightmost digit in the base b expansion of n. Next, divide q_0 by b.
  $q_0 = bq_1 + a_1 \quad 0 \leq a_1 \leq b$
- The remainder, a_1, is the second digit from the right in the base b expansion of n.
- Continue by successively dividing the quotients by b, obtaining the additional base b digits as the remainder. The process terminates when the quotient is 0.

- Could we construct expansion of any integer base?

Base Conversion

Example: Find the octal expansion of $(12345)_{10}$

Solution: Successively dividing by 8 gives:

- $12345 = 8 \cdot 1543 + 1$
- $1543 = 8 \cdot 192 + 7$
- $192 = 8 \cdot 24 + 0$
- $24 = 8 \cdot 3 + 0$
- $3 = 8 \cdot 0 + 3$

The remainders are the digits from right to left yielding $(30071)_8$.

Conversion Between Binary, Octal, and Hexadecimal Expansions

Example: Find the octal and hexadecimal expansions of $(11\ 1110\ 1011\ 1100)_2$.

Solution:

- To convert to octal, we group the digits into blocks of three $(011\ 111\ 010\ 111\ 100)_2$, adding initial 0s as needed. The blocks from left to right correspond to the digits 3,7,2,7, and 4. Hence, the solution is $(37274)_8$.
- To convert to hexadecimal, we group the digits into blocks of four $(0011\ 1110\ 1011\ 1100)_2$, adding initial 0s as needed. The blocks from left to right correspond to the digits 3,E,B, and C. Hence, the solution is $(3EBC)_{16}$.

Modular Exponentiation

- Modular exponentiation $c \equiv b^n \pmod{m}$, where b, n and m are positive integers is very important for the cryptography because:
  - if $b < m$ there is unique solution of the congruency,
  - it is relatively easy to to find the solution even for big numbers, but the inverse logarithmic problem is much more complicated.

Modular Exponentiation

- In cryptography it is common that b is 256-bit binary number (77 decimal digits) and n is 3 decimal digits long. Than b^n is a number of several thousands decimal digit.
- Special algorithms are required for such computations.

Example

- Consider small numbers first. Let $b = 13$, $n = 5$, $m = 21$. Calculate $b^n \bmod m$. We may think about exponentiation as a sequence of multiplications:
- $(13^4 \times 13) \bmod 21 = ((13^3 \bmod 21) \times (13 \bmod 21)) \bmod 21$
- In turn, $13^4 \bmod 21 = ((13^2 \bmod 21) \times (13^2 \bmod 21)) \bmod 21$
- The same about $13^2 \bmod 21$. Thus we may reduce power to two and numbers involved to 20 (21-1 because of mod operations).
- To do this, consider n as sum of powers 2: $n = 5_{10} = 101_2$
- a1 mod m = 13 a2 mod m = (13 x 13) mod 21 = 169 mod 21 = 1 a4 mod m = (1 x 1) mod 21 = 1
- **Solution:** ((b1 mod m) x (b4 mod m)) mod m = (13 x 1) mod m = 13.

Binary Modular Exponentiation

- In general, to to compute b^n we may use the binary expansion of n, $n = (a_{k-1},\ldots,a_1,a_0)_2$. Than

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

- Therefore, to compute b^n, we need only compute the values of b, b^2, $(b^2)^2 = b^4$, $(b^4)^2 = b^8$, …, and the multiply the terms b^{2^j} in this list, where $a_j = 1$.

$O((\log m)^2 \log n)$ bit operations are used to find $b^n \bmod m$.

Practice: 175^{235} mod 257

- 235 = 128 + 64 + 32 + 8 + 2 + 1 = $(11101011)_2$.
- ***j*** ***8 7 6 4 2 1*** ***87654321***

- $175^{235} = 175^{128} \times 175^{64} \times 175^{32} \times 175^{8} \times 175^{2} \times 175$
- d: records the temporal result, starting from the rightmost factor.
- t: represents the next term b^{2^j} where b = 175 in this example.

- j = 1, **175 mod 257** = 175

  175^2 mod 257 = 42

  d ← 175, t ← 42.

Practice: $175^{235} \bmod 257$

- $235 = 128 + 64 + 32 + 8 + 2 + 1 = (11101011)_2$.
- ***j 8 7 6 4 2 1 87654321***

- $175^{235} = 175^{128} \times 175^{64} \times 175^{32} \times 175^{8} \times \mathbf{175^2 \times 175}$

- j = 2, $175^2 \times 175 \bmod 257 = (175^2 \bmod 257) \times (175 \bmod 257) \bmod 257 = t \times d \bmod 257 = 42 \times 175 \bmod 257 = 154$
- $175^4 \bmod 257 = (175^2 \bmod 257)^2 \bmod 257$
- $= t \times t \bmod 257$
- $= 42 \times 42 \bmod 257 = 222$
-
- **d ← $175^2 \times 175 \bmod 257 = 154$**
- **t ← $175^4 \bmod 257 = 222$**

Practice: 175^{235} mod 257

- 235 = 128 + 64 + 32 + 8 + 2 + 1 = (11101011)2.
- ***j 8 7 6 4 2 1 87654321***

- $175^{235} = 175^{128} \times 175^{64} \times 175^{32} \times 175^{8} \times \mathbf{175^{2} \times 175}$

- j = 3, **no factor 175^{4}.**
- $175^{8} \bmod 257 = (175^{4} \bmod 257)^{2} \bmod 257$
- $= t \times t \bmod 257$
- $= 222 \times 222 \bmod 257 = 197$
-
- **d ← $175^{2} \times 175 \bmod 257 = 154$**
- **t ← $175^{8} \bmod 257 = 197$**

Practice: 175^{235} mod 257

- 235 = 128 + 64 + 32 + 8 + 2 + 1 = $(11101011)_2$.
- ***j 8 7 6 4 2 1 87654321***

- $175^{235} = 175^{128} \times 175^{64} \times 175^{32} \times \mathbf{175^8 \times 175^2 \times 175}$

- j = 4, $\mathbf{175^8 \times 175^2 \times 175}$ mod 257 = (175^8 mod 257) x ($\mathbf{175^2 \times 175}$ mod 257) mod 257 = t x d mod 257 = 197 x 154 mod 257 = 12
- 175^{16} mod 257 = (175^8 mod 257)^2 mod 257
- = t x t mod 257
- = 197 x 197 mod 257 = 2
- **d ← $175^8 \times 175^2 \times 175$** mod 257 = 12
- **t ← 175^{16} mod 257 = 2**

Practice: 175^{235} mod 257

- 235 = 128 + 64 + 32 + 8 + 2 + 1 = $(11101011)_2$.
- ***j 8 7 6 4 2 1 87654321***

- $175^{235} = 175^{128} \times 175^{64} \times 175^{32} \times \mathbf{175^8 \times 175^2 \times 175}$

- j = 5, no factor $\mathbf{175^{16}}$
- 175^{32} mod 257 = $(175^{16}$ mod 257$)^2$ mod 257
- = t x t mod 257
- = 2 x 2 mod 257 = 4
- **d ← 175^8 x175^2 x175** mod 257 = 12
- **t ← 175^{32} mod 257 = 14**

Practice: 175^{235} mod 257

- 235 = 128 + 64 + 32 + 8 + 2 + 1 = $(11101011)_2$.
- ***j 8 7 6 4 2 1 87654321***

- $175^{235} = 175^{128} \times 175^{64} \times \mathbf{175^{32} \times 175^{8} \times 175^{2} \times 175}$

- j = 6, $\mathbf{175^{32} \times 175^{8} \times 175^{2} \times 175}$ mod 257 = (175^{32} mod 257) x ($\mathbf{175^{8} \times 175^{2} \times 175}$ mod 257) mod 257 = t x d mod 257 = 4 x 12 mod 257 = 48

- 175^{64} mod 257 = (175^{32} mod 257)^2 mod 257
- = t x t mod 257
- = 4 x 4 mod 257 = 16
- **d ← $175^{32} \times 175^{8} \times 175^{2} \times 175$ mod 257 = 48**
- **t ← 175^{64} mod 257 = 16**

Practice: $175^{235} \bmod 257$

- $235 = 128 + 64 + 32 + 8 + 2 + 1 = (11101011)_2$.
- ***j 8 7 6 4 2 1 87654321***

- $175^{235} = 175^{128} \times \mathbf{175^{64} \times 175^{32} \times 175^{8} \times 175^{2} \times 175}$

- j = 7, $\mathbf{175^{64} \times 175^{32} \times 175^{8} \times 175^{2} \times 175} \bmod 257 = (175^{64} \bmod 257) \times (\mathbf{175^{32} \times 175^{8} \times 175^{2} \times 175} \bmod 257) \bmod 257 = t \times d \bmod 257 = 16 \times 48 \bmod 257 = 254$

- $175^{128} \bmod 257 = (175^{64} \bmod 257)^2 \bmod 257$
- $= t \times t \bmod 257$
- $= 16 \times 16 \bmod 257 = 256$
- $\mathbf{d \leftarrow 175^{64} \times 175^{32} \times 175^{8} \times 175^{2} \times 175 \bmod 257 = 48}$
- $\mathbf{t \leftarrow 175^{128} \bmod 257 = 256}$

Practice: 175^{235} mod 257

- 235 = 128 + 64 + 32 + 8 + 2 + 1 = $(11101011)_2$.
- ***j 8 7 6 4 2 1 87654321***

- $175^{235} = \mathbf{175^{128}\ x175^{64}\ x175^{32}\ x175^{8}\ x175^{2}\ x175}$

- j = 8, $\mathbf{175^{128}\ x\ 175^{64}\ x175^{32}x175^{8}\ x175^{2}\ x175}$ mod 257 = (175^{128} mod 257) x ($\mathbf{175^{64}\ x\ 175^{32}x\ 175^{8}\ x\ 175^{2}\ x175}$ mod 257) mod 257 = t x d mod 257 = 256 x 254 mod 257 =3

- 175^{128} mod 257 = $(175^{64}$ mod $257)^2$ mod 257
- = t x t mod 257
- = 16 x 16 mod 257 = 256
- **d ← 175^{128} x 175^{64} x 175^{32}x175^{8} x175^{2} x175 mod 257 = 3**
- **return d.**

Analysis on d and t (1)

- d = $175 \bmod 257$
- d = $175^2 \times 175 \bmod 257$
- d = $175^8 \times 175^2 \times 175 \bmod 257$
- d = $175^{32} \times 175^8 \times 175^2 \times 175 \bmod 257$
- d = $175^{64} \times 175^{32} \times 175^8 \times 175^2 \times 175 \bmod 257$
- d = $175^{128} \times 175^{64} \times 175^{32} \times 175^8 \times 175^2 \times 175 \bmod 257$

$d = t \times d \bmod 257$ when $t = \mathbf{175^k}$ **and** $\mathbf{k = 2^{j-1}}$

Analysis on d and t (2)

- $t = 175^2 \bmod 257 = 42$
- $t = 175^4 \bmod 257 = (175^2 \bmod 257)^2 \bmod 257 = 222$
- $t = 175^8 \bmod 257 = (175^4 \bmod 257)^2 \bmod 257 = 197$
- $t = 175^{16} \bmod 257 = (175^8 \bmod 257)^2 \bmod 257 = 2$
- $t = 175^{32} \bmod 257 = (175^{16} \bmod 257)^2 \bmod 257 = 4$
- $t = 175^{64} \bmod 257 = (175^{32} \bmod 257)^2 \bmod 257 = 16$
- $t = 175^{128} \bmod 257 = (175^{64} \bmod 257)^2 \bmod 257 = 256$

$$t = t^2 \bmod 257$$

Practice: $175^{235} \bmod 257$

- $235_{10} = 11101011_2$.
- *1*. d := 1 × 175 mod 257 = 175, t := 175^2 mod 257 = 42;
- *2*. d := 175 × 42 mod 257 = 154, t := 42^2 mod 257 = 222;
- *3*. t := 222^2 mod 257 = 197;
- *4*. d := 154 × 197 mod 257 = 12, t := 197^2 mod 257 = 2;
- *5*. t := 2^2 mod 257 = 4;
- *6*. d := 12 × 4 mod 257 = 48, t := 4^2 mod 257 = 16;
- *7*. d := 48 × 16 mod 257 = 254, t := 16^2 mod 257 = 256;
- *8*. d := 254 × 256 mod 257 = 3
- ***Return* d = 3**

Primes and Greatest Common Divisors

Prime, Composite and Theorem 1

- **Prime**: a positive integer p greater than 1 if the only positive factors of p are 1 and p
- A positive integer greater than 1 that is not prime is called **composite**

THE FUNDAMENTAL THEOREM OF ARITHMETIC Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

Example

- Prime factorizations of integers
  - $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
  - $641 = 641$
  - $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$
  - $1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

Theorem 2

If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

- As n is composite, n has a factor 1<a<n, and thus n=ab
- We show that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ (by contraposition)
- Thus n has a divisor not exceeding $\sqrt{n}$
- This divisor is either prime or by the fundamental theorem of arithmetic, has a prime divisor less than itself, and thus a prime divisor less than less than $\sqrt{n}$
- In either case, n has a prime divisor $b \leq \sqrt{n}$

Example

- Show that 101 is prime
- The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, 7.
- As 101 is not divisible by 2, 3, 5, 7, it follows that 101 is prime.

Procedure for prime factorization

- Begin by diving n by successive primes, starting with 2
- If n has a prime factor, we would find a prime factor not exceeding $\sqrt{n}$.
- If no prime factor is found, then n is prime
- Otherwise, if a prime factor p is found, continue by factoring n/p

Procedure for prime factorization

- Note that n/p has no prime factors less than p
- If n/p has no prime factor greater than or equal to p and not exceeding its square root, then it is prime
- Otherwise, if it has a prime factor q, continue by factoring n/(pq)
- Continue until factorization has been reduced to a prime

Example

- Find the prime factorization of 7007
- Start with 2, 3, 5, and then 7, 7007/7=1001
- Then, divide 1001 by successive primes, beginning with 7, and find 1001/7=143
- Continue by dividing 143 by successive primes, starting with 7, and find 143/11=13
- As 13 is prime, the procedure stops
- $7007=7\cdot 7\cdot 11\cdot 13=7^2\cdot 11\cdot 13$

Theorem 3

There are infinitely many primes.

- Proof by contradiction
- Assume that there are only finitely many primes, p_1, p_2, …, p_n. Let $Q=p_1p_2\ldots p_n+1$
- By Fundamental Theorem of Arithmetic: Q is prime or else it can be written as the product of two or more primes

Mersenne primes

- Primes with the special form 2^p-1 where p is also a prime, called **Mersenne prime**.
- $2^2-1=3$, $2^3-1=7$, $2^5-1=31$ are Mersenne primes while $2^{11}-1=2047$ is not a Mersenne prime ($2047=23 \cdot 89$)
- The largest Mersenne prime known (as of early 2011) is $2^{43,112,609}-1$, a number with over 13 million digits

Theorem 4

THE PRIME NUMBER THEOREM The ratio of the number of primes not exceeding x and $x/\ln x$ approaches 1 as x grows without bound. (Here $\ln x$ is the natural logarithm of x.)

- This theorem was proved in 1896 and proof is complicated.
- Can use this theorem to estimate the odds that a randomly chosen number is prime
- The odds that a randomly selected positive integer less than n is prime are approximately

  $(n/\ln n)/n = 1/\ln n$
- The odds that an integer less than 10^{1000} is prime are approximately $1/\ln 10^{1000}$, approximately 1/2300

Open Problems about Primes

- **Goldbach's conjecture**: every even integer n, n>2, is the sum of two primes

  4=2+2, 6=3+3, 8=5+3, 10=7+3, 12=7+5, …
- As of 2011, the conjecture has been checked for all positive even integers up to $1.6 \cdot 10^{18}$
- **Twin prime conjecture**: Twin primes are primes that differ by 2. There are infinitely many twin primes

Greatest common divisor

- Let a and b be integers, not both zero. The largest integer d such that d | a and d | b is called the **greatest common divisor** (GCD) of a and b, often denoted as gcd(a,b)
- The integers a and b are **relative prime** if their GCD is 1

  gcd(10, 17)=1, gcd(10, 21)=1, gcd(10,24)=2
- The integers a_1, a_2, …, a_n are **pairwise relatively prime** if $\gcd(a_i, a_j)=1$ whenever $1 \leq i < j \leq n$

Prime factorization and GCD

- Finding GCD

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$
$$\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$$
$$120 = 2^3 \cdot 3 \cdot 5, \quad 500 = 2^2 \cdot 5^3$$
$$\gcd(120,500) = 2^2 \cdot 3^0 \cdot 5^1 = 20$$

- **Least common multiples** of the positive integers a and b is the smallest positive integer that is divisible by both a and b, denoted as lcm(a,b)

Least common multiple

- Finding LCM

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$
$$\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$
$$120 = 2^3 \cdot 3 \cdot 5, 500 = 2^2 \cdot 5^3$$
$$\text{lcm}(120,500) = 2^3 \cdot 3^1 \cdot 5^3 = 8 \cdot 3 \cdot 125 = 3000$$

- Let a and b be positive integers, then ab=gcd(a,b)·lcm(a,b)

Euclidean algorithm

- Need more efficient prime factorization algorithm
- Example: Find gcd(91,287)
- $287 = 91 \cdot 3 + 14$
- Any divisor of 287 and 91 must be a divisor of $287 - 91 \cdot 3 = 14$
- Any divisor of 91 and 14 must also be a divisor of $287 = 91 \cdot 3$
- Hence, the gcd(91,287)=gcd(91,14)

Euclidean algorithm

- Need more efficient prime factorization algorithm
- Example: Find gcd(91,287)
- gcd(91,287)=gcd(91,14)
- Next, $91 = 14 \cdot 6 + 7$
- Any divisor of 91 and 14 also divides $91 - 14 \cdot 6 = 7$ and any divisor of 14 and 7 divides 91, i.e., gcd(91,14)=gcd(14,7)
- $14 = 7 \cdot 2$, gcd(14,7)=7,
- Thus gcd(287,91)=gcd(91,14)=gcd(14,7)=7

Euclidean algorithm

Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

- Proof: Suppose that d divides both a and b. Then it follows that d also divides a − bq = r. Hence, any common divisor of a and b is also a common divisor of b and r.
- Likewise, suppose that d divides both b and r. Then d also divides bq + r = a. Hence, any common divisor of b and r is also a common divisor of a and b.
- Consequently, gcd(a, b)=gcd(b,r)

Euclidean algorithm

- Suppose a and b are positive integers, a≥b. Let r_0=a and r_1=b, we successively apply the division algorithm

$$
\begin{aligned}
r_0 &= r_1 q_1 + r_2, 0 \le r_2 < r_1 \\
r_1 &= r_2 q_2 + r_3, 0 \le r_3 < r_2 \\
&\dots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, 0 \le r_n < r_{n-1} \\
r_{n-1} &= r_n q_n \\
\gcd(a,b) &= \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1}) \\
&= \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n
\end{aligned}
$$

- Hence, the gcd is the last nonzero remainder in the sequence of divisions

Example

- Find the GCD of 414 and 662

  $662 = 414 \cdot 1 + 248$

  $414 = 248 \cdot 1 + 166$

  $248 = 166 \cdot 1 + 82$

  $166 = 82 \cdot 2 + 2$

  $82 = 2 \cdot 41$

  $a = bq + r$

  $\gcd(a,b) = \gcd(b,r)$

  $\gcd(414,662) = 2$ (the last nonzero remainder)

The Euclidean algorithm

procedure $gcd(a, b$: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ **mod** y
    $x := y$
    $y := r$
return $x\{\gcd(a, b)$ is $x\}$

- The time complexity is O(log b) (where a ≥ b)

Chinese Remainder Theorem

About Chinese Reminder Theorem

- Chinese Reminder Theorem is a method to solve equations about remainders.
  - One equation
  - Ancient application
  - Two equations and three equations
  - Chinese Remainder theorem

Case Study

How to solve the following equation?

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

For example, consider the equation $2x \equiv 3 \pmod{7}$

Suppose there is a solution x to the equation,
then there is a solution x in the range from 0 to 6,
because we can replace x by $x \bmod 7$.

Then we can see that $x=5$ is a solution.

Also, $5+7$, $5+2\cdot7$, $5+3\cdot7$, …, $5-7$, $5-2\cdot7$…, are solutions.
Therefore the solutions are of the form $5+7k$ for some integer k.

One Equation

How to solve the following equation?

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

$2x \equiv 3 \pmod{7}$	$x = 5 + 7k$ for any integer k
$5x \equiv 6 \pmod{9}$	$x = 3 + 9k$ for any integer k
$4x \equiv -1 \pmod{5}$	$x = 1 + 5k$ for any integer k
$4x \equiv 2 \pmod{6}$	$x = 2 + 3k$ for any integer k
$10x \equiv 2 \pmod{7}$	$x = 3 + 7k$ for any integer k
$3x \equiv 1 \pmod{6}$	no solutions

One Equation: Relatively Prime

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

Case 1: a and n are relatively prime

Without loss of generality, we can assume that $0 < a < n$.

Because we can replace a by $a \bmod n$ without changing the equation.

e.g. $103x \equiv 6 \pmod{9}$ is equivalent to $4x \equiv 6 \pmod{9}$.

Since a and n are relatively prime, there exists a multiplicative inverse a' for a.

Hence we can multiply a' on both sides of the equation to obtain

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

Therefore, a solution always exists when a and n are relatively prime.

One Equation: Common Factor

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

Case 2: a and n have a common factor c>=2.

Case 2a: c divides b.

$ax \equiv b \pmod{n}$

$\Leftrightarrow ax = b + nk$ for some integer k

$\Leftrightarrow a_1cx = b_1c + n_1ck$

$\Leftrightarrow a_1x = b_1 + n_1k$

$\Leftrightarrow a_1x \equiv b_1 \pmod{n_1}$

we assume c|a and c|n and also c|b.

In Case (2a) we can simplify the equation, and solve the new equation instead.

One Equation: Common Factor

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

Case 2: a and n have a common factor $c>=2$.

Case 2b: c does not divides b.

$ax \equiv b \pmod{n}$

$\Leftrightarrow ax = b + nk$ for some integer k

$\Leftrightarrow a_1cx = b + n_1ck$

$\Leftrightarrow a_1x = b/c + n_1k$

This is a contradiction, since a_1x and n_1k are integers, but b/c is not an integer since c does not divide b.

Therefore, in Case 2b, there is no solution.

One Equation

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

Theorem. Let a, b, n be given integers.
The above equation has a solution if and only if gcd(a,n) | b.
Furthermore, if the condition gcd(a,n) | b is satisfied,
then the solutions are of the form y mod (n/gcd(a,n)) for some integer y.

Proof. First, divide b by gcd(a,n).
If not divisible, then there is no solution by Case (2b).
If divisible, then we simplify the solution as in Case (2a).
Then we proceed as in Case (1) to compute the solution.

One Equation: Exercise

$87x \equiv 3 \pmod{15}$	Replace 87 by 87 mod 15
$12x \equiv 3 \pmod{15}$	Divide both sides by gcd(12,15) = 3
$4x \equiv 1 \pmod{5}$	Compute the multiplicative inverse of 4 modulo 5
$x \equiv 4 + 5k$	

$114x \equiv 5 \pmod{22}$	Replace 114 by 114 mod 22
$4x \equiv 5 \pmod{22}$	Divide both sides by gcd(4,22) = 2
no solutions	Because 2 does not divide 5.

Important: to be familiar with the extended Euclidean algorithm to compute gcd and to compute multiplicative inverse.

Computing Multiplicative Inverse

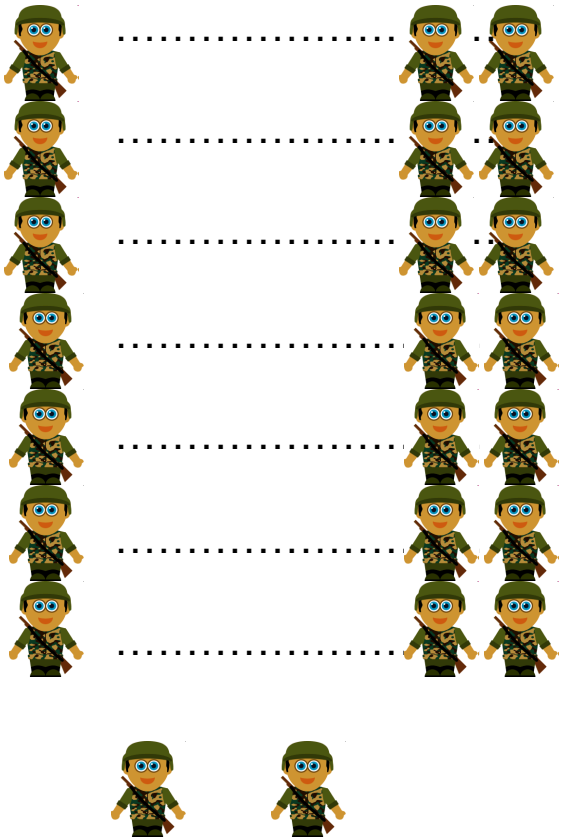
Example: n = 123, k=37

$123 = 3 \cdot 37 + 12$	so $12 = n - 3k$
$37 = 3 \cdot 12 + 1$	so $1 = 37 - 3 \cdot 12$
	$= k - 3(n-3k) = 10k - 3n$
$12 = 12 \cdot 1 + 0$	done, gcd=1

So 1 = 10k-3n.

Then we know that 10 is the multiplicative inverse of 37 under modulo 123.

Ancient Application of Number Theory

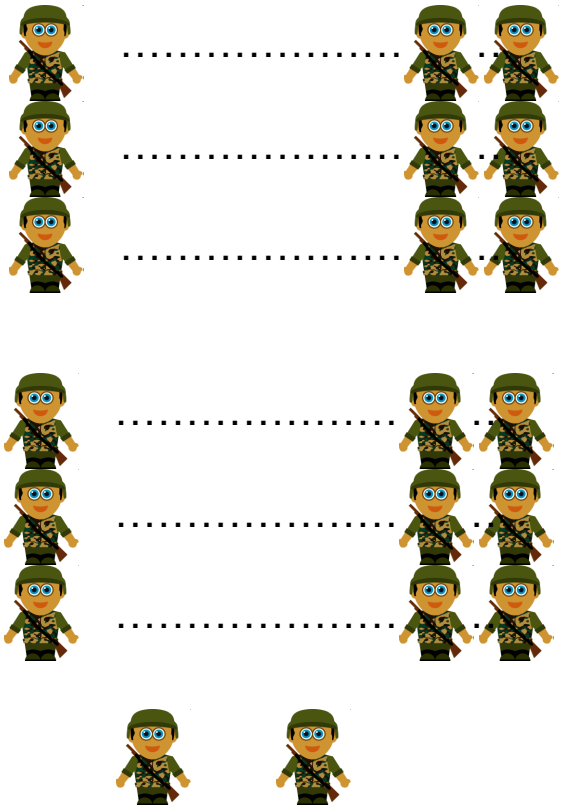


There are 2 soliders left.

Form groups of 3 soldiers

Han, Xin (韓信)

Ancient Application of Number Theory

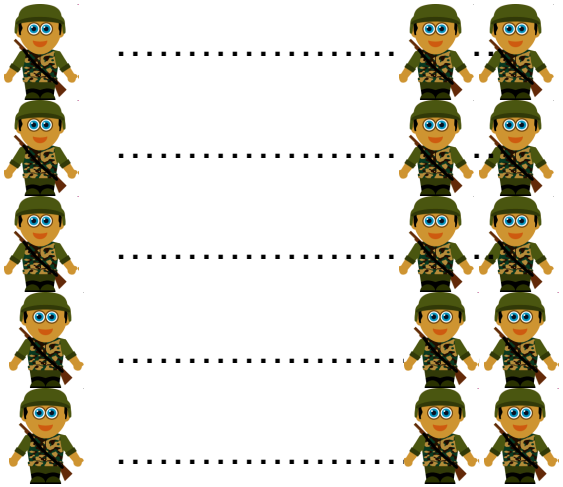


There are 3 soliders left.

Form groups of 5 soldiers

Han, Xin (韓信)

Ancient Application of Number Theory



There are 2 soliders left.

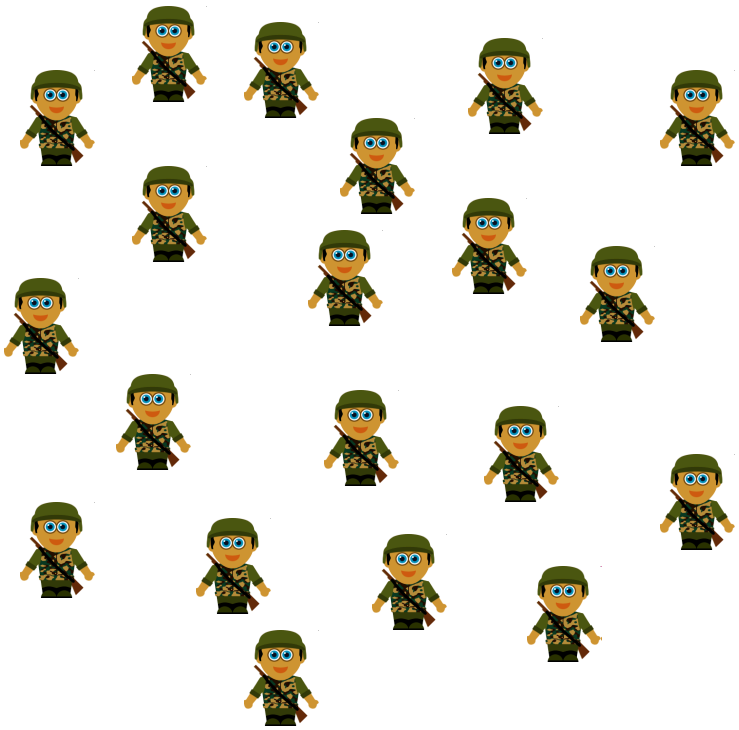
Form groups of 7 soldiers

Han, Xin (韓信)

Ancient Application of Number Theory

Starting from 1500 soldiers, after a war, about 400-500 soldiers died.

Now we want to know how many soldiers are left.



We have 1073 soliders.

How could he figure it out?!

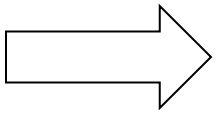
The Mathematical Question

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

+



$x = 1073$

$1000 <= x <= 1100$

How to solve this system of modular equations?

Two Equations

Find a solution to satisfy both equations simultaneously.

$$c_1 x \equiv d_1 \pmod{m_1}$$
$$c_2 x \equiv d_2 \pmod{m_2}$$

First we can solve each equation to reduce to the following form.
(Of course, if one equation has no solution, then there is no solution.)

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$

There may be no solutions simultaneously satisfying both equations.

For example, consider $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 3$.

$x \equiv 1 \pmod 6$, $x \equiv 2 \pmod 4$.

Two Equations

Case 1: n_1 and n_2 are relatively prime.

$$x \equiv 2 \pmod 3$$
$$x \equiv 4 \pmod 7$$

$x = 2+3u$ and $x = 4+7v$ for some integers u and v.

$2+3u = 4+7v \quad \Rightarrow \quad 3u = 2+7v$

$$\Rightarrow \quad 3u \equiv 2 \pmod 7$$

5 is the multiplicative inverse for 3 under modulo 7

Multiply 5 on both sides gives:

$$5 \cdot 3u \equiv 5 \cdot 2 \pmod 7$$

$$\Rightarrow \quad u \equiv 3 \pmod 7 \quad \Rightarrow \quad u = 3 + 7w$$

Therefore, $x = 2+3u = 2+3(3+7w) = 11+21w$

So any $x \equiv 11 \pmod{21}$ is the solution.

Where did we use the assumption that n_1 and n_2 are relatively prime?

Two Equations

Assume n_1 and n_2 are relatively prime.

$$x \equiv 2 \pmod 3$$
$$x \equiv 4 \pmod 7$$

The original idea is to construct such an x directly.

Let $x = 3 \cdot a + 7 \cdot b$

Note that when x is divided by 3, the remainder is decided by the second term.
And when x is divided by 7, the remainder is decided by the first term.

More precisely, $x \bmod 7 = (3 \cdot a + 7 \cdot b) \bmod 7 = 3a \bmod 7$

Similarly, $x \bmod 3 = (3 \cdot a + 7 \cdot b) \bmod 3 = 7b \bmod 3$

Therefore, to satisfy the equations, we just need to find
a such that $3a \bmod 7 = 4$ and b such that $7b \bmod 3 = 2$.

Two Equations

Assume n_1 and n_2 are relatively prime.

$$x \equiv 2 \pmod 3$$
$$x \equiv 4 \pmod 7$$

The original idea is to construct such an x directly.

Let $x = 3 \cdot a + 7 \cdot b$

Therefore, to satisfy the equations, we just need to find a such that $3a \bmod 7 = 4$ and b such that $7b \bmod 3 = 2$.

Since 3 and 7 are relatively prime, both the equations can be solved.

The first equation is $3a \equiv 4 \pmod 7$, and the answer is $a=6$.

Similarly, the second equation is $7b \equiv 2 \pmod 3$, and the answer is $b=2$.

So one answer is $x = 3a+7b = 3(6)+7(2) = 32$.

Two Equations

Assume n_1 and n_2 are relatively prime.

$$x \equiv 2 \pmod 3$$
$$x \equiv 4 \pmod 7$$

The original idea is to construct such an x directly.

Let $x = 3 \cdot a + 7 \cdot b$

So one answer is $x = 3a+7b = 3(6)+7(2) = 32$.

Are there other solutions?

Note that $32 + 3 \cdot 7 \cdot k$ is also a solution to satisfy both equations.

Are there other solutions?

The only solutions are of the form $32 + 21k$ for some integer k.

Three Equations

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

Let $x = 5 \cdot 7 \cdot a + 3 \cdot 7 \cdot b + 3 \cdot 5 \cdot c$

So the first (second, third) term is responsible for the first (second, third) equation.

More precisely, $x \bmod 3 = (5 \cdot 7 \cdot a + 3 \cdot 7 \cdot b + 3 \cdot 5 \cdot c) \bmod 3 = 5 \cdot 7 \cdot a \bmod 3$

$x \bmod 5 = (5 \cdot 7 \cdot a + 3 \cdot 7 \cdot b + 3 \cdot 5 \cdot c) \bmod 5 = 3 \cdot 7 \cdot b \bmod 5$

$x \bmod 7 = (5 \cdot 7 \cdot a + 3 \cdot 7 \cdot b + 3 \cdot 5 \cdot c) \bmod 7 = 3 \cdot 5 \cdot c \bmod 7$

Therefore, to satisfy the equations, we want to find a,b,c to satisfy the following:

$x \bmod 3 = 35a \bmod 3 = 2$

$x \bmod 5 = 21b \bmod 5 = 3$

$x \bmod 7 = 15c \bmod 7 = 2$

Three Equations

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

Let $x = 5 \cdot 7 \cdot a + 3 \cdot 7 \cdot b + 3 \cdot 5 \cdot c$

So the first (second, third) term is responsible for the first (second, third) equation.

Now we just need to solve the following three equations separately.

$35a \equiv 2 \pmod 3$, $21b \equiv 3 \pmod 5$, $15c \equiv 2 \pmod 7$.

This is equal to

$2a \equiv 2 \pmod 3$, $b \equiv 3 \pmod 5$, $c \equiv 2 \pmod 7$

Therefore, we can set $a = 1, b = 3, c = 2$.

Then $x = 35a+21b+15c = 35(1)+21(3)+15(2) = 128$.

Note that $128+3 \cdot 5 \cdot 7 \cdot k = 128+105k$ is also a solution.

Since Han, Xin (韓信) knows that $1000 <= x <= 1100$, he concludes that $x = 1073$.

Wait, but how does he know that there is no other solution?

Chinese Reminder Theorem

Theorem: If $n_1, n_2, \ldots, n_k$ are relatively prime and $a_1, a_2, \ldots, a_k$ are integers, then

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$

$$x \equiv a_k \pmod{n_k}$$

have a simultaneous solution x that is **unique** modulo n, where $n = n_1 n_2 \ldots n_k$.

We will give a proof when k=3, but it can be extended easily to any k.

Proof of Chinese Remainder Theorem

Let $\mathbf{N_1} = n_2\, n_3$ $\mathbf{N_2} = n_1\, n_3$ $\mathbf{N_3} = n_1\, n_2$

Since N_i and n_i are relatively prime, this implies that there exist $x_1\ x_2\ x_3$

$N_1x_1 \equiv 1 \pmod{n_1}$ $N_2x_2 \equiv 1 \pmod{n_2}$ $N_3x_3 \equiv 1 \pmod{n_3}$

So, $a_1N_1x_1 \equiv a_1 \pmod{n_1}$, $a_2N_2x_2 \equiv a_2 \pmod{n_2}$, $a_3N_3x_3 \equiv a_3 \pmod{n_3}$

Let $x = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3$

Since $n_1 \mid \mathbf{N}_2$ and $n_1 \mid \mathbf{N}_3$, $x \equiv a_1\, N_1x_1 \pmod{n_1}$

Since $N_1x_1 \equiv 1 \pmod{n_1}$, $x \equiv a_1 \pmod{n_1}$

Similarly, $x \equiv a_2 \pmod{n_2}$ $x \equiv a_3 \pmod{n_3}$

Uniqueness

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$

$$x \equiv a_k \pmod{n_k}$$

Suppose there are two solutions, x and y, to the above system.

Then $x - y \equiv 0 \pmod{n_i}$ for any i.

This means that $n_i \mid x - y$ for any i.

Since $n_1, n_2, \ldots, n_k$ are relatively prime,

this means that $n_1 n_2 \ldots n_k \mid x - y$. (why?)

Therefore, $x = y \pmod{n_1 n_2 \ldots n_k}$.

So there is a unique solution in every $n_1 n_2 \ldots n_k$ numbers.

General Systems

What if n1,n2,…,nk are not relatively prime?

$x \equiv 3 \pmod{10}$

- $x \equiv 3 \pmod 2 \equiv \mathbf{1 \pmod 2}$ (a)
- $x \equiv \mathbf{3 \pmod 5}$ (b)

$x \equiv 8 \pmod{15}$

- $x \equiv 8 \pmod 3 \equiv \mathbf{2 \pmod 3}$ (c)
- $x \equiv 8 \pmod 5 \equiv \mathbf{3 \pmod 5}$ (d)

$x \equiv 5 \pmod{84}$

- $x \equiv 5 \pmod 4 \equiv \mathbf{1 \pmod 4}$ (e)
- $x \equiv 5 \pmod 3 \equiv \mathbf{2 \pmod 3}$ (f)
- $x \equiv \mathbf{5 \pmod 7}$ (g)

So we reduce the problem to the relatively prime case.

The answer is 173 (mod 420).

(b) and (d) are the same.

(c) and (f) are the same.

(e) is stronger than (a).

Quick Summary

First we talk about how to solve one equation $ax \equiv b \pmod{n}$.

The equation has solutions if and only if $\gcd(a,n)$ divides b.

Then we talk about how to find simultaneous solutions to two equations

$a_1x \equiv b_1 \pmod{n_1}$ and $a_2x \equiv b_2 \pmod{n_2}$.

First use the technique in one equation to reduce to the form

$x \equiv \mathbf{c}_1 \pmod{n_1}$ and $x \equiv \mathbf{c}_2 \pmod{n_2}$.

By setting $x = k_1n_1 + k_2n_2$, then we just need to find k_1 and k_2 so that

$\mathbf{c}_2 \equiv \mathbf{k}_1 n_1 \pmod{n_2}$ and $\mathbf{c}_1 \equiv \mathbf{k}_2 n_2 \pmod{n_1}$.

These equations can be solved separately by using techniques for one equation.

The same techniques apply for more than two equations.

And the solution is unique mod $n_1 n_2 \ldots n_k$ if there are k equations.

Finally, when $n_1 n_2 \ldots n_k$ are not relatively prime, we show how to reduce it back to the relatively prime case.

Next class

- Topic: Cryptograph and Basics of Counting
- Pre-class reading: Chap 5-6