Special Topics on Algorithms
Modular Arithmetic, Primality Testing

Vangelis Markakis Ioannis Milis and George Zois

Modular Arithmetic

- Deals with restricted ranges of integers, e.g., $Z_N = \{0, 1, ..., N\text{-}1\}$ for some large N
- Reset a counter to <u>zero</u> when an integer reaches a max value $N > 0$

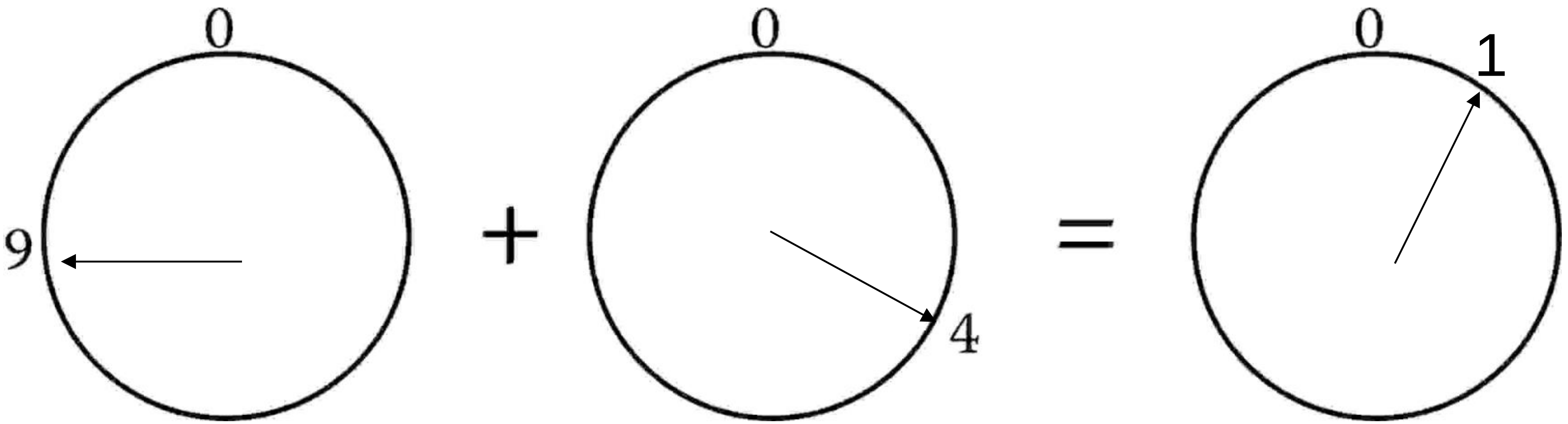
$$\text{If } x = qN + r,\ \ 0 \le r \le N\text{-}1,\ \ N>0$$
$$x \bmod N = r$$

$x \equiv y \pmod N \Leftrightarrow x \bmod N = y \bmod N$
x and y are congruent modulo N

Modular Arithmetic

Examples:

- $1 \equiv (9+4) \bmod 12$



- $253 \equiv 13 (\bmod\ 60)$, since $253 = 4*60+13$

  (253 minutes is 4 hours + 13 min)

Modular Arithmetic

Claim 1: $x \equiv y \pmod N$ iff $N \mid x-y$

Proof :

$\Rightarrow$: $x=pN+r,\ y=qN+r \Rightarrow x-y=(p-q)N \Rightarrow N \mid x-y$

$\Leftarrow$:
$$\left.\begin{array}{r} N \mid x-y \Rightarrow x-y = kN \Rightarrow x=y+kN \\ \text{Let } r= y \bmod N, \\ \text{that is, } y=qN+r \end{array}\right\} \Rightarrow$$

$\Rightarrow x=qN+r+kN \Rightarrow x=(q+k)N+r \Rightarrow r= x \bmod N$

Modular Arithmetic

mod N is an equivalence relation

- $a \equiv a \pmod{N}$ Reflexivity
- $a \equiv b \pmod{N} \Rightarrow b \equiv a \pmod{N}$ Symmetry
- $a \equiv b \pmod{N},\ b \equiv c \pmod{N} \Rightarrow a \equiv c \pmod{N}$ Transitivity

Modulo N arithmetic divides Z into
N equivalence classes each one of the form
$[a] = \{x \mid x \equiv a \pmod{N}\}$, $0 \leq a \leq N-1$
or
$[a] = \{kN+a \mid k \in Z\}$, since $x = kN+a$, $0 \leq a \leq N-1$

Modular Arithmetic

<u>Example:</u>

<u>There are 5 equivalence classes modulo 5</u>

$Z_5 = \{0, 1, 2, 3, 4\}$

$[0] = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$

$[1] = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\}$

$[2] = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\}$

$[3] = \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\}$

$[4] = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\}$

All numbers in [a] are congruent mod N
(any of them is substitutable by any other)

Modular Addition and Multiplication

Substitution Rule

Let $x \equiv x'$ (mod N) and $y \equiv y'$ (mod N),
then, $x+y \equiv x'+y'$ (mod N) and $xy \equiv x'y'$ (mod N)

The following properties also hold:

i) $x+(y+z) \equiv (x+y)+z$ (mod N) Associativity
ii) $xy \equiv yx$ (mod N) Commutativity
iii) $x(y+z) \equiv xy+xz$ (mod N) Distributivity

Hence:

in performing a sequence of additions and multiplications (mod N) we can reduce intermediate results to their remainders mod N in any stage

Example:

$2^{345} \equiv (2^5)^{69} \equiv 32^{69} \equiv 1^{69} \equiv 1 \pmod{31}$

Modular Division

Common arithmetic: inverse of $\alpha \neq 0$: $x = 1/\alpha$, $\alpha x = 1$

Modular arithmetic: multiplicative inverse of α, modulo N:

- $x \in Z$ such that $\alpha x \equiv 1 \pmod N$
- We can also write $x \equiv \alpha^{-1} \pmod N$
- does not always exist!

Claim 2: For $1 \leq a < N$, a has a multiplicative inverse mod N iff $\gcd(a, N) = 1$

i)Assume a has a multiplicative inverse mod N. By contradiction, if $\gcd(a,N) > 1$, it must hold that $\gcd(a,N) \mid ax \bmod N$, for every x. Thus, it does not hold that $\alpha x \equiv 1 \pmod N$

ii)If $\gcd(a,N) = 1$, then by applying ExtEUCLID(a,N) …

Modular Division

Example: $2x \equiv 1 \pmod 6$
$\gcd(2,6) = 2 \Rightarrow 2$ does not have an inverse mod 6

How can we find multiplicative inverses when they exist?
If $\gcd(a,N)=1$ then ExtEUCLID returns integers x,y such that

$$ax + Ny = 1 \Rightarrow ax \equiv 1 \pmod N$$

Example: $11x \equiv 1 \pmod{25}$

ExtEUCLID(11, 25) returns $x = -34$ ($\equiv 16 \bmod 25$), $y = 15$, $\gcd(11, 25) = 1$, and thus $11*(-34) \equiv 1 \pmod{25}$

If $\gcd(a,N)=1$ we say that a, N are relatively primes or coprimes
Hence: α has a multiplicative inverse modulo N iff a, N are coprimes.

Prime Numbers

- A number p is prime iff its only divisors are the trivial divisors 1 and p
- $\nexists$ N: N | p, $2 \leq N \leq p\text{-}1$
- By convention, 1 is not a prime
- P= {2, 3, 5, 7, 11, 13, 17, 19,…….}
- Prime numbers play a special role in number theory and its applications
- A number that is not prime is called composite

<u>Goldbach conjecture:</u>

Any even integer greater than 3 can be written as the sum of two primes

Prime Numbers

- Some big prime numbers:
  - $(333+10^{793})10^{791}+1$ (1585 digits, identified in 1987)
  - $2^{1257787}-1$ (378.632 digits, 1996)
  - $2^{77,232,917}-1$(around 23 million digits, Dec 2017)
  - Mersenne primes: prime numbers in the form 2^m-1
    - Not all numbers of this form are primes
  - Fermat primes: prime numbers in the form $2^{2^n}+1$
    - Again, not all numbers of this form are primes

Prime Numbers

Fundamental theorem of arithmetic (or unique factorization theorem):

Every natural number ≥ 2, can be written in a unique way as a product of prime powers:

$$n = p_1^{e_1} p_2^{e_2} \ldots p_r^{e_r}$$

- where each p_i is prime, $p_1 < p_2 < \cdots < p_r$ and each e_i is a positive integer
- 6000 is uniquely decomposed as $2^4 \cdot 3 \cdot 5^3$
- Proof by (strong) induction
- Corollary: If p is prime and p|ab ➔ p|a or p|b (not true when p is not prime)

Prime Numbers

<u>CLAIM 1 (Euclid's theorem):</u> There are infinitely many primes

<u>Proof:</u> Suppose that $P = \{p_1, p_2, \ldots, p_n\}$ for some n

Let $p = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n + 1$

- If <u>p is prime</u>, contradiction, since we assumed no other primes
- If <u>p is not prime</u>

  By the fundamental theorem, there exists a prime that divides p

  But p mod $p_i = 1$, $\forall i, 1 \le i \le n$

  again a contradiction.

Prime Numbers

- Relatively prime numbers
  - Two integers a, b are relatively prime (or co-primes) if gcd(a, b) = 1.
    - E.g., 8 and 15 are relatively prime,
    - By Euclid’s algorithm we can decide in polynomial time if 2 numbers are relatively prime with each other

Prime Numbers

Euler's phi function

Definition: For every $n \geq 2$, $\varphi(n)$ = number of integers between 1 and n that are relatively prime with n

Properties:

- For any prime number p: $\varphi(p) = p-1$
- $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha (1-1/p)$
- $\varphi(mn) = \varphi(m)\varphi(n)$, iff $\gcd(m,n) = 1$

Corollary: For every $n \geq 2$

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

(where p refers to all prime numbers that divide n)

Prime Numbers

Euler's phi function

– The properties help in simplifying the calculations

- $\varphi(45) = 24$, since the prime factors of 45 are 3 and 5
  - $\varphi(45)=45*(1-1/3)(1-1/5)=45*(2/3)(4/5)=24$
- $\varphi(1512) = \varphi(2^3*3^3*7) = \varphi(2^3)*\ \varphi(3^3) * \varphi(7) =$

  $(2^3-2^2) * (3^3-3^2)*(7-1) = 4 * 18 * 6 = 432$
- Hence there are 432 numbers between 1 and 1512 that are relatively prime with 1512

Prime Numbers

2 useful properties for simplifying calculations

Fermat's Little theorem [around 1640]

If p is prime then for every α such that $1 \leq \alpha \leq p\text{-}1$

$\alpha^{p-1} \equiv 1 \pmod{p}$

A generalization: Euler's theorem

For every integer n>1, $\alpha^{\varphi(n)} \equiv 1 \pmod{n}$ for every α such that $\gcd(\alpha, n) = 1$ [if n is prime, $\varphi(n) = n\text{-}1$]

For example: Find 2^{26} mod 7

$2^{26} = 2^2 \cdot 2^{24} = 2^2 \cdot (2^6)^4 \equiv 2^2 \cdot 1 \bmod 7 \equiv 4 \bmod 7$

Prime Numbers

<u>Fermat's Little theorem</u> [around 1640]

If p is prime then for every α such that $1 \leq \alpha \leq p-1$

$\alpha^{p-1} \equiv 1 \pmod{p}$

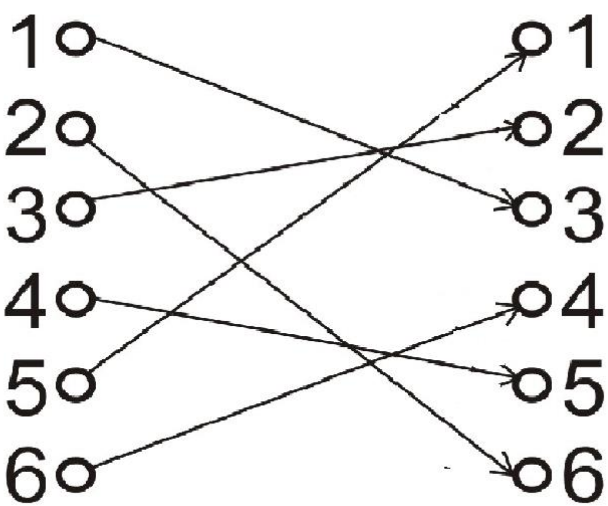
<u>Proof:</u>

- Let S = {1, 2, 3, …, p-1} all possible non-zero mod p integers
- Main observation: By multiplying integers in S by a (mod p) we simply re-permute them!
  - It is an implication of the fact that α has a multiplicative inverse mod p, since gcd(α, p)=1

Prime Numbers

Example:

$\alpha = 3$, $p = 7$, $\alpha^6 \equiv 1 \pmod 7$



$1\cdot 3 \pmod 7 = 3$

$2\cdot 3 \pmod 7 = 6$

$3\cdot 3 \pmod 7 = 2$

$4\cdot 3 \pmod 7 = 5$

$5\cdot 3 \pmod 7 = 1$

$6\cdot 3 \pmod 7 = 4$

$$\{\underbrace{1,2,3,4,5,6}_{x}\} = \{\underbrace{1\cdot 3,\ 2\cdot 3,\ 3\cdot 3,\ 4\cdot 3,\ 5\cdot 3,\ 6\cdot 3}_{x}\ (\overset{\text{all}}{\text{mod}}\ 7)\}$$

Taking products: $6! \equiv 3^6 \cdot 6! \pmod 7$

$6!$ is relatively prime to $7 \Rightarrow 3^6 \equiv 1 \pmod 7$

Prime Numbers

Proof continued (for general α and prime p)

Consider 2 distinct numbers

$i, j \in S \Rightarrow i \neq j,\ i, j \leq p\text{-}1,\ i,j \neq 0$

The numbers resulting by multiplying the elements of S by α (mod p) are:

- **Distinct**

  if not: $\alpha \cdot i \equiv \alpha \cdot j \pmod{p} \Rightarrow i \equiv j \pmod{p} \Rightarrow i \equiv j$, contradiction
- **Non zero mod p**

  if $\alpha \cdot i \equiv 0 \pmod{p} \Rightarrow i=0$, contradiction
- **In the range [1, p-1]**

Hence, they are a permutation of S

$\Rightarrow (p\text{-}1)! \equiv \alpha^{p-1} \cdot (p\text{-}1)! \pmod{p} \Rightarrow \alpha^{p-1} \equiv 1 \pmod{p}$

Primality Testing

Problem Primes:

I: An integer $N > 1$

Q: Answer whether or not N is prime

One of the most fundamental problems in Computer Science

A naive approach: Trial division

- Try to see if any of the numbers 2, 3, 4,…,N-1 divides N
- Actually it suffices to try only with the numbers 2, 3, ..., $\lfloor\sqrt{N}\rfloor$
  - If N is composite it has a factor, which is at most $\sqrt{N}$
- In fact, since N is odd, we can also remove the even numbers
- Worst case complexity: $\sqrt{N}/2$, hence $O(\sqrt{N})$, exponential since $\sqrt{N} = 2^{\log N/2}$
- Effective only for small values of N (for RSA, N has 512 bits or even more)

Primality Testing

A different approach

- Faster but with a small probability of error

Fermat Test

Algorithm PRIME (N)

Pick a positive integer α<N at random

if $\alpha^{N-1} \equiv 1 \pmod{N}$ then return YES // we hope yes

else return NO // definite no

Complexity: only need to use the algorithm for exponentiation mod N (repeated squaring), hence O(logN) multiplications

Primality Testing

The algorithm can make errors but only of one kind:

- If it says that N is composite, then it is correct
- If it says that N is prime then it may be wrong

- gcd(α,N) > 1: N is not prime, and N fails the test
- gcd(α,N) = 1

  - if N is prime: passes the test

  - if N is composite: can pass the test for some α' s!

    e.g. $341 = 11*31$ and $2^{340} \equiv 1 (\mathrm{mod} 341)$

    - if N is a Carmichael number: passes the test for all α' s!!

    e.g. $561 = 3*11*17$ and $\alpha^{560} \equiv 1 \ (\mathrm{mod}\ 561)$

    for every α for which: gcd(α,n)=1!

Primality Testing

Carmichael numbers

- Actually due to Korselt
- They are the composite numbers that pass the Fermat test *for all* a's that are relatively prime to them
- Alternative definition: A number n is a Carmichael number if it is not divisible by the square of a prime and, for all prime divisors p of n, it is true that $p-1 \mid n-1$
- They are extremely rare (561, 1105, 1729, 2465,…)
- $561 = 3 \cdot 11 \cdot 17$
- There are only 255 of them less than 10^8
- There are 20,138,200 Carmichael numbers between 1 and 10^{21} (approximately one in 50 billion numbers)
- Ignore them for now (see Miller-Rabin test for a better algorithm to test primality)

Primality Testing

N

Prime: passes the Fermat test

Composite: passes or fails the test depending on α, but there is an α for which it fails if it is not a Carmichael number

If N is composite and not a Carmichael number, for how many values of α does it fail the test?

CLAIM 3: If a number N fails the Fermat test for some value of α, then N **also fails the test for at least half of the choices of α < N**

Primality Testing

N — Prime, $\alpha^{N-1} \equiv 1 \pmod{N}$, for all $\alpha<N$

N — not Prime, $\alpha^{N-1} \equiv 1 \pmod{N}$, <u>for at most half of the values $\alpha<N$</u>

Pr[Fermat test returns YES, when N is Prime]=1

Pr[Fermat test returns YES, when N is not Prime] $\leq 1/2$

Repeat the algorithm k times for different $\alpha_1, \alpha_2, \ldots, \alpha_k$

Pr[Fermat test returns YES, when N is not Prime] $\leq 1/2^k$

Generating Random Primes

Density of prime numbers

- Very important to be able to find prime numbers quickly
- How should we search for prime numbers?

- Theorem: For every n≥1, there is always a prime between n and 2n
- Initial proof: Chebyshev (1850)
- Simpler proof: Erdos (1932), at the age of 19!!
- Thus primes are relatively dense within the natural numbers

Generating Random Primes

<u>Prime number Theorem (Conjectured by Legendre et al. ~1797-1798, proved in 1896)</u>

Lex $\pi(x)$ be the number of primes $\leq$ x. Then

$$p(x) \sim \frac{x}{\ln x} \quad \text{or} \quad \lim_{x \text{®} \text{¥}} \frac{p(x)}{x / \ln x} = 1$$

If N is a random integer of n bits (hence $\leq 2^n$), it has roughly a one-in-n chance of being prime:

$$p = \Pr\, [N\ is\ prime] = \frac{2^n / \ln 2^n}{2^n} = \frac{1}{\ln 2^n} = \frac{\log e}{\log 2^n} = \frac{\log e}{n} = \frac{1.44}{n}$$

Generating Random Primes

Algorithm

Repeat

    Pick a random n-bit integer N

    Run the Fermat test on N

Until N passes

How many iterations? (Waiting for the first success)

Generating Random Primes

Analysis on the number of iterations

- Let k= #trials until first success
- Let p = success probability of each trial = Pr[randomly chosen N is prime]
- Pr[k=j] = probability that we succeed in the j-th trial (and hence fail in previous ones)
- Pr [k=j]= $(1\text{-p})^{j\text{-}1} \cdot p$

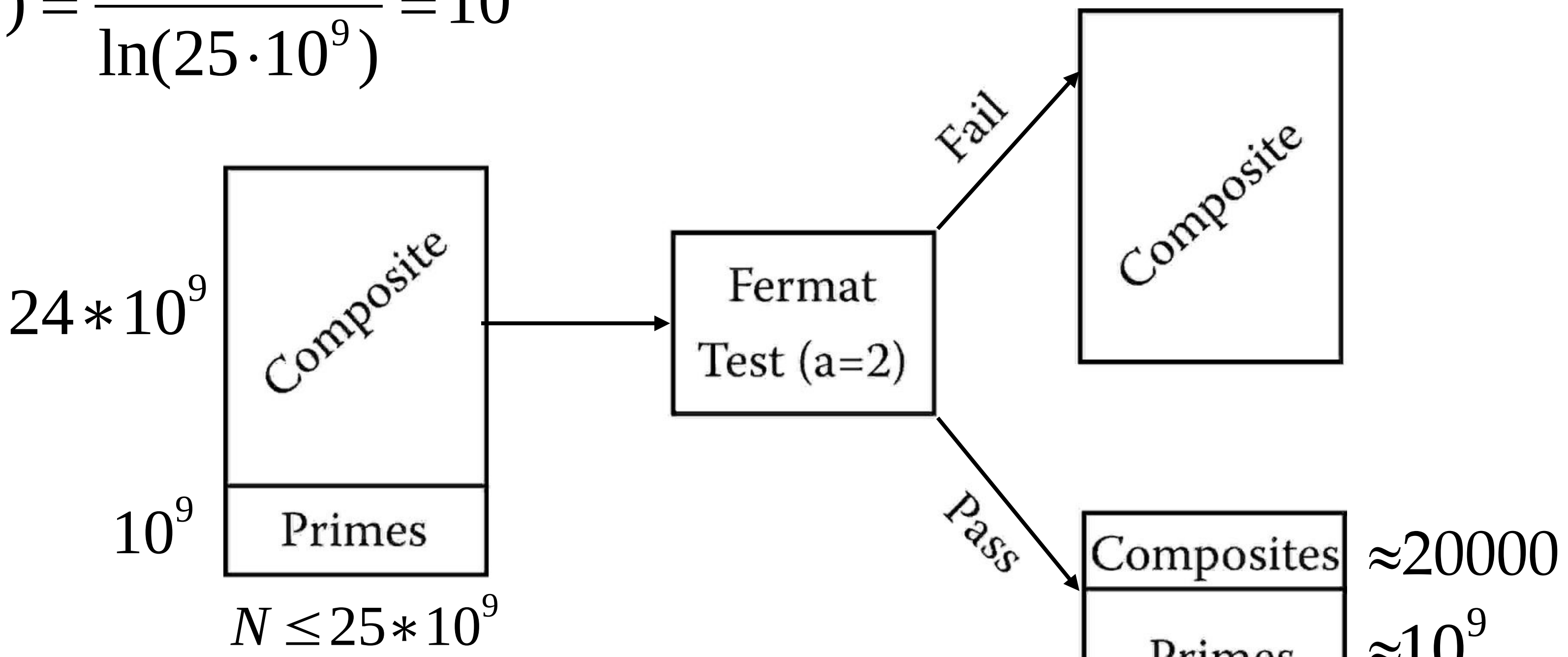
$$E[k] = \sum_{j=1}^{\infty} j \Pr[k=j] = \sum_{j=1}^{\infty} j(1-p)^{j-1} p = \frac{p}{p-1} \sum_{j=1}^{\infty} j(1-p)^{j}$$

$$= \frac{p}{p-1} \frac{1-p}{p^2} = \frac{1}{p} = \frac{n}{1.44}$$

Generating Random Primes

$$N = 25 * 10^9$$

$$\pi(N) = \frac{25 \cdot 10^9}{\ln(25 \cdot 10^9)} = 10^9$$



$$\Pr[a\ composite\ \leq 25 \cdot 10^9\ passes\ the\ test] \approx \frac{20.000}{10^9} = 2 \cdot 10^{-5}$$

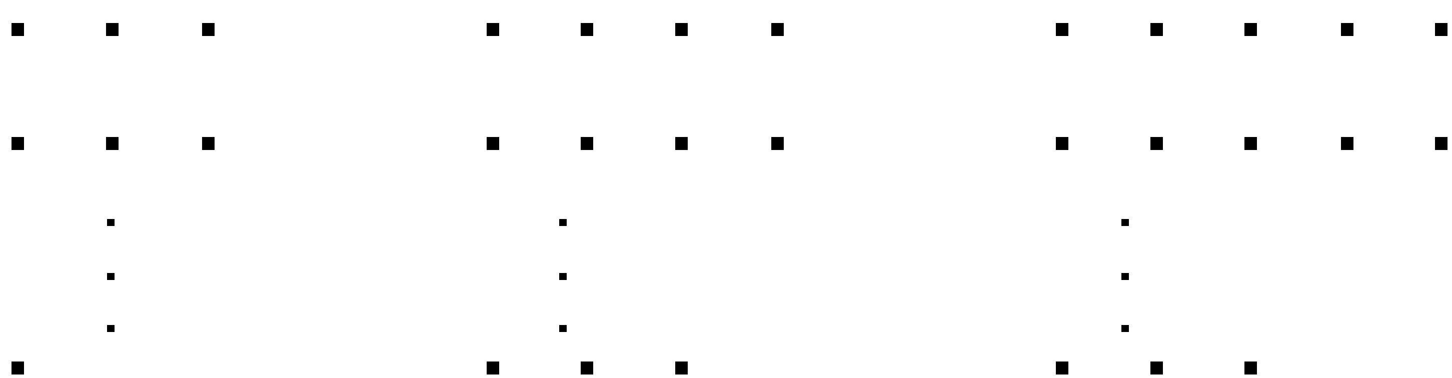
Chinese Remainder Theorem

Linear equations in modular arithmetic

– Around 100 A.D.

– Question: Is there an integer x such that in a parade of x soldiers, when they align themselves in

1. Groups of 3, there is only 1 remaining soldier in the last row
2. Groups of 4, there are 3 remaining soldiers
3. Groups of 5, there are 3 remaining soldiers



Chinese Remainder Theorem

Theorem:

– Let $n_1, n_2, ..., n_k$ be positive integers that are relatively prime with each other, hence $\gcd(n_i, n_j) = 1, \forall\ i \neq j$.

– Then for any integers $a_1, a_2, ..., a_k$, the system

$$x \equiv a_1 \bmod n_1,\ x \equiv a_2 \bmod n_2,\ \ldots,\ x \equiv a_k \bmod n_k,$$

has a unique solution within Z_n, where $n = n_1 \cdot n_2 \cdot \ldots \cdot n_k$

Corollary: If $n_1, n_2, ..., n_k$, are positive integers that are relatively prime with each other, then for any x and a:

$x \equiv a \bmod n_i$ for $i = 1, 2, ..., k$ iff $x \equiv a \bmod n$

where $n = n_1 \cdot n_2 \cdot \ldots \cdot n_k$

Chinese Remainder Theorem

Proof:

- Let $n_1, n_2, ..., n_k$ be relatively prime with each other
- Let $a_1, a_2, ..., a_k$ be arbitrary integers
- $\forall i$ define $c_i = n/n_i$.
- $\gcd(c_i, n_i) = 1 \Rightarrow c_i$ has an inverse mod n_i.
- Let d_i be the inverse, hence $c_i d_i \bmod n_i = 1$
- The number $x^* = a_1c_1d_1 + a_2c_2d_2 + \dots + a_kc_kd_k$ satisfies all the equations

- Complexity: polynomial since we are just using the extended Euclidean algorithm

Chinese Remainder Theorem

Example

- Which x satisfies the following equations?

  $x \equiv 2 \pmod{5}$

  $x \equiv 3 \pmod{13}$
- $a_1=2$, $n_1=5$, $a_2=3$, $n_2=13$
- We have $n=n_1 * n_2=5*13=65$, $c_1 = 65/5 = 13$, $c_2 = 5$
- Since $13^{-1} \equiv 2 \pmod{5}$ and $5^{-1} \equiv 8 \pmod{13}$, $d_1=2$, $d_2=8$
- Then, $x = a_1c_1d_1+a_2c_2d_2$

$$x \equiv 2 \cdot 2 \cdot 13 \cdot + 3 \cdot 5 \cdot 8 \pmod{65}$$

$$\equiv 52 + 120 = 42 \pmod{65}$$

All the solutions are in the form $x(t)=42+65t$, $t \in Z$