Math Background

Z. Jerry Shi
Department of Computer Science and Engineering
University of Connecticut

Quiz

There are two containers.

Their capacities are 11 gallons and 7 gallons.

How can you use the two containers to measure 5 gallons water?

Is it hard?

Prime numbers

- An integer that is greater than 1 and whose only positive divisors are 1 and itself
- Numbers that are not prime are composites
- 1 is neither a prime nor a composite

Every number > 1 can be written as a product of prime numbers, and there is only one way.

Example: $12 = 2^2 \times 3$ $15 = 3 \times 5$

Unique factorization of integers (fundamental theorem of number theory)

Question

- How many positive divisors does 72 have?
  - Including 1 and 72

Factorization

Given *n*, find all its prime factors.

For example:

1350664108659952233496032162788059699388814756056670275244851438515265106048595338339402871505719094417982072821644715513736804197039641917430464965892742562393410208643832021103729587257623585096431105640735015081875106765946292055636855294752135008528794163773285339061097505443349998111500569772368909275632

Is it hard?

Factorization - 2

- Factorization is a hard problem!
  - More formally, intractable problem

- Best algorithm for b bits numbers: $\exp((c + o(1))b^{1/3}\log^{2/3}b)$

- The largest number factored was RSA-768 (768-bit long) in 2009
  - Hundreds of computers over 2 years
- Factoring 1024-bit numbers is about 1,000 harder

Onewayness:

Given (large) prime numbers, it is easy to find their product.

Given a (large) product, it is hard to find its factors.

How many prime numbers?

- There are infinite number of prime numbers.
  - The largest is $2^{74,207,281}$-1 (as of Jan 2016)
- The number of prime numbers $\leq x$ is about x / ln(x).
  - So the probability of randomly chosen number is prime is 1 / ln(x).
- The prime numbers become sparse.

- Twin prime: both p and p+2 are prime.
  - The difference is 2 (and the gap is 1).

- Yitang Zhang proved in 2013 that there are infinitely many gaps that do not exceed by 7×10^7. The gap was reduced to 246 in 2015.

Find prime numbers

Given *n*, find all prime numbers ≤ *n*.

The sieve of Eratosthenes

- List all the numbers from 1 to *n*
- Start from 2, delete all multiples of prime numbers
  - 2, 3, 5, …,$\sqrt{n}$
- All remaining numbers are prime

When *n* is large, the process takes loooooong time

Primality test

Given a positive number *n*, is *n* prime?

Note that the problem is different from factorization.

Primality test in practice

Fermat primality test (we are going to learn in a moment)

Miller–Rabin and Solovay–Strassen primality test

AKS test runs in polynomial time (still slow in practice)

Greatest common divisor (GCD)

- The GCD of two or more non-zero integers is the largest positive integer that divide all the integers

Example:

$$\gcd(3, 9) = 3$$

$$\gcd(2^{20} \cdot 3^{50}, 2^{10} \cdot 3^{5} \cdot 7) = 2^{10} \cdot 3^{5}$$

$$\gcd(5, 7) = 1$$

$$\gcd(221, 403) =$$

Is it hard?

Find gcd: Euclidean Algorithm

Suppose $N > D \geq 0$

Let $i = 0$, $N_0 = N$, $D_0 = D$.

1. Find $N_i = D_i \cdot q_i + r_i$ (Quotient-Remainder Theorem)
   $0 \leq r_i < D_i$
2. If $r_i = 0$, return D_i
3. $N_{i+1} = D_i$, $D_{i+1} = r_i$
4. Increment i and goto Step 1

The algorithm works because gcd (N_i, D_i) = gcd (N_{i+1}, D_{i+1})

Coprime

- If two integers do not have any common positive factor other than 1, they are relatively prime, mutually prime, or coprime
  - *x* and *y* are co-prime if and only if gcd (*x*, *y*) = 1
  - 1 is considered to be relatively prime to all numbers

Example

5 and 21

6 and 25

Modular Arithmetic

Quotient-Remainder Theorem

Given any integer n and an integer $m > 0$, there exist unique integers q and r such that

$$n = q \cdot m + r \text{ and } 0 \leq r < m$$

$$r = n \bmod m$$

Properties of modular arithmetic:

$(x+y) \bmod m = ((x \bmod m)+(y \bmod m)) \bmod m.$

$(x - y) \bmod m = ((x \bmod m) - (y \bmod m)) \bmod m.$

$(x\ y) \bmod m = ((x \bmod m)\ (y \bmod m)) \bmod m.$

Notation Properties of modular arithmetic

Instead of writing mod everywhere, we can write like this:

$$a = x^3 + y - z \pmod{m}$$

or formally,

$$a \equiv x^3 + y - z \pmod{m}$$

Example

$$7^{12} + 5^3 \; = 2^{12} + 0^3 \pmod{5}$$

$a \equiv b \pmod{m}$: *a* and *b* are congruent modulo *m*
When divided by *m*, *a* and *b* have the same remainder.
a – *b* is a multiple of *m*.

Fermat’s Little Theorem (FLT)

$a^p \equiv a \pmod{p}$ for every prime p and every integer a.

If this is not true for some a, p is not prime.

We can use FLT for primarily test, but there are better algorithms.

Modular exponentiation

Compute the following:

$$2^{65} \bmod 11$$

$$2^{123456789123456789} \bmod 11$$

Is it hard?

Group

- A group is defined as a set of elements G and an operation $\bigcirc$ such that
  - Closure
    - If a and b are in G, $c = a \bigcirc b$ is also in G.
  - Associativity
    - $(a \bigcirc b) \bigcirc c = a \bigcirc (b \bigcirc c)$.
  - Identity element e
    - $a \bigcirc e = a$.
  - Inverse element
    - Any a, there exists b such that $a \bigcirc b = e$.
- If the operation in a group is also commutative, the group is an abelian group

$$a \bigcirc b = b \bigcirc a.$$

Group Example

- Integers and addition form a group

- Integers and multiplication is not a group

https://www.youtube.com/watch?v=qvx9TnK85bw&list=PLi01XoE8jYoi3SgnnGorR_XOW3IcK-TP6&index=10

Residue classes modulo *m*

- A set of numbers $Z_m = \{0, 1, 2, \ldots, m - 1\}$ is called residue classes modulo *m*
  - All remainders of integers modulo *m*
  - Can also be denoted as $Z(m)$ or Z/mZ

- Z_m and addition (+) form an abelian group
  - $a + b \pmod{m}$ is between 0 and $m - 1$
  - $(a + b) + c = a + (b + c)$
  - $a + 0 = a$
  - Any a, the additive inverse of a is $m - a$
    - $a + (m - a) = 0 \pmod{m}$
  - $a + b = b + a$

Multiplication

Let $Z_m \backslash \{0\}$ denote Z_m excluding 0

Do $Z_m \backslash \{0\}$ and * (multiplication) form a group?

Example of Multiplicative Group

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

Let a and b are the numbers in the set.

$a \cdot b$ is also in the set

$a \cdot (b \cdot c) = (a \cdot b) \cdot c$

$a \cdot 1 = 1 \cdot a$

$1 \cdot 1 = 1, \quad 2 \cdot 3 = 1, \quad 4 \cdot 4 = 1$

Example of Multiplicative Group

$Z_6 \backslash \{0\} = \{1, 2, 3, 4, 5\}$

Let a and b are the numbers in the set.

$a \cdot b$ is also in the set

$a \cdot (b \cdot c) = (a \cdot b) \cdot c$

$a \cdot 1 = 1 \cdot a$

$1 \cdot 1 = 1,$

$2 \cdot ? = 1$ $3 \cdot ? = 1$ $4 \cdot ? = 1$

Group and multiplication

Let $Z_m \backslash \{0\}$ denote Z_m excluding 0

Do $Z_m \backslash \{0\}$ and * form a group?

If m is prime, yes.

If m is not prime, no.

$Z_m{}^*$ is Z_m with elements that are not coprime to m removed

0 is removed

$Z_m{}^*$ and * form a group

Example of Multiplicative Group

$Z_8^* = \{1, 3, 5, 7\}$

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

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

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Multiplication table in groups. Also called Cayley table.

Division

5 / 3 =

$$\frac{5}{3} = 5 \times 3^{-1} = 5 \times 3 = 7$$

$Z_8^* = \{1, 3, 5, 7\}$

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Is it hard?

Find the inverse: Euclidean Algorithm

We use Euclidean algorithm to find gcd.

We can use it to find the inverse (extended Euclidean algorithm)

Given *a* and *n*, use Euclidean algorithm to find gcd(*a*, *n*).

If *a* and *n* are coprime, find *x* and *k* so that

$$a \cdot x + k \cdot n = 1$$

x is the inverse of *a* mod *n* because $a \cdot x \equiv 1 \pmod{n}$.

Note: the first term is $a \cdot x$, not $-a \cdot x$

If *a* and *n* are not coprime, gcd (*a*, *n*). *a* does not have an inverse.

Example: use Euclidean algorithm to find the inverse

Example: *a* = 31, *n* = 72. Find the inverse of *a* mod *n*.

Step 1:

Dividend	Divisor	Remainder	
72	31	10	$72 = 31 * 2 + 10$
31	10	1	$31 = 10 * 3 + 1$

gcd(31, 72) = 1 (they are coprime)

Step 2:

$72 - 32 * 2 = 10$
$31 - 10 * 3 = 1$
$31 - (72 - 31 * 2) * 3 = 1$
$31 - 72 * 3 + 31 * 2 * 3 = 1$
$31 * 7 + 72 * (-3) = 1$

Therefore, 7 is the inverse of 31.

Fermat’s Little Theorem (FLT) and the inverse

$a^p \equiv a \pmod{p}$ for every prime p and every integer a

- If $a \neq 0$, $a^{p-1} \equiv 1 \pmod{p}$
  - Divide both sides by a

- a^{p-2} is the inverse of a in Z_p

$$a^{p-1} = a \cdot a^{p-2} = 1 \pmod{p}$$
$$\therefore a^{-1} = a^{p-2}$$

Finite group

- A group is called finite if it has a finite number of elements

- The number of elements is the order of the group
  - Denoted as |G|

- In group (G, ·), the order of an element *a* is *t* if

$$\underbrace{a \cdot a \cdot \cdots \cdot a}_{t} = 1$$

assuming 1 is the identity element

Cyclic group

- A cyclic group is a group all of whose elements can be generated from a single element
  - The element is called a primitive element, or a generator

- If the operation is addition, each element is a multiple of the generator
- If the operation is multiplication, each element is a power of the generator

- A cyclic group is abelian (commutative)

One line proof:

$$x + y = ag + bg = (a + b)g = (b + a)g = y + x$$

Example: Cyclic group

$Z_6 = \{0, 1, 2, 3, 4, 5\}$ and +

0 = 6 * 5, 1 = 5 * 5, 2 = 4 * 5, 3 = 3 * 5, 4 = 2 * 5, 5 = 1 * 5

5 is a generator. 2, 3, and 4 are not.

Multiplicative group of Z_5, excluding 0, is cyclic

$2^0 = 1$ $2^1 = 2$ $2^2 = 4$ $2^3 = 3$

Multiplicative group of Z_8* is not cyclic (see the multiplication table)

Example: Cyclic group

$Z_9^* = \{1, 2, 4, 5, 7, 8\}$

6 elements. 2 is a generator.

*	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Not every element in a cyclic group is a generator.

For example, 4 is not a generator $4^0 = 1$, $4^1 = 4$, $4^2 = 7$, $4^3 = 1$.

Powers of 2:

exponents:	**0**	**1**	**2**	**3**	**4**	**5**	**6**
results:	**1**	**2**	**4**	**8**	**7**	**5**	**1**

$Z_9^* = \langle 2 \rangle$

Discreet Logarithm Problem (DLP)

Suppose G is a multiplicative cyclic group and a generator g of G. Given an element h of G, find x such that

$$g^x = h$$

DLP is a hard problem if the group is chosen carefully.

Commonly used groups: Z_p* where p is a large safe prime.
Example: p is 1024 bits, and $(p – 1)/2$ is also prime

Onewayness: easy from x to h, hard from h to x.

n-th root

- Find the n^{th} root of c mod n
- It is hard if the factors of n is unknown

For example: $\sqrt{c} \pmod{n}$

Is $\sqrt{c}$ $(\mathrm{mod}\ 2^{64}\ )$hard?

Number of elements in a group

- How many elements are in the following group?

Z_p^* where p is prime.

Z_m^*

Euler’s totient function (1)

- If $0 < x \leq n$, and x is relatively prime to n, x is a totative of n
  - x and n do not a common divisor that is larger than 1

- Euler's totient function $\varphi(n)$ is the number of totatives of n

$\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, …

$\varphi(24) = 8$ The set of totatives is $\{1, 5, 7, 11, 13, 17, 19, 23\}$.

$\varphi(p) = p - 1$ if p is prime

Euler’s totient function (2)

Suppose *n* > 1, and the standard factored form of *n* is

$$n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \ldots p_r^{k_r}$$

$$\begin{aligned}\varphi(n) &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_r}\right)\\ &= n\sum_{i=1}^{r}\left(1-\frac{1}{p_i}\right)\end{aligned}$$

Totient function example

$$\varphi(9) = \varphi(3^2) = 9\left(1 - \frac{1}{3}\right) = 6$$

$$\varphi(10) = \varphi(2 \times 5) = 10\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 4$$

$$\varphi(100) = \varphi(2^2 \times 5^2) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$$

Example: product of two prime numbers

If p and q are prime, and $n = pq$,

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

Check:

Among pq – 1 numbers, these are not totatives:

$p, 2p, 3p, \ldots, (q-1)p$

$q, 2q, 3q, \ldots, (p-1)q$

Therefore, $\varphi(n) = (pq - 1) - (p - 1 + q - 1) = (p - 1)(q - 1)$

Computing Euler’s totient function

- If *n*’s factors are known, it is easy to compute φ(*n*)
  - Otherwise, it is hard

- The two problems are equivalent

Carmichael’s totient function conjecture:

For every positive integer *n*, there exists a positive integer *m* such that $\varphi(m) = \varphi(n)$ and $m \neq n$.

Euler’s theorem

- If n is a positive integer and a is coprime to n, then

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

- A generalization of Fermat’s little theorem
  - $a^p \equiv a \pmod{p}$ for every prime p and every integer a
  - If $a \neq 0$, $a^{p-1} \equiv 1 \pmod{p}$

- Further generalized by Carmichael’s theorem
  - The exponent is smaller (than $\varphi(n)$)

A formal proof: http://www.mizar.org/JFM/Vol10/euler_2.html

Find the inverse - 3

Given Z_n*, how to find the mupltiplicative inverse of an element *a*.

If you know φ (*n*),

$$a^{\varphi(n)} = 1 \quad \bmod n \qquad \text{(Euler's theorem)}$$

$$a \cdot a^{\varphi(n)-1} = 1 \bmod n$$

$$a^{-1} = a^{\varphi(n)-1} \bmod n$$

Special case: *n* is prime, $\varphi(n) = n - 1$.

$$a^{-1} = a^{n-2} \bmod n$$

Summary of problems

Can you identify the hard problems?

- Primality test
- Multiplication
- Exponentiation
- Factorization
- Find GCD
- Find modular inverse
- Discreet logarithm problem (DLP)
- Euler's totient function
- n-th root

Field

- A field has addition, subtraction, multiplication and division
  - Allow division, but not division by zero

- A field has the following elements:
  - F, +, -, *, /, 0, 1
  - There are two groups in a field
    - F, +, -, 0
    - F*=F\{0}, *, /, 1 The multiplicative group of the field.

Finite field (Galois field)

- A filed with finitely many elements
  - The number of elements in a field is the order of the field
- If p is prime, $Z_p = \{0, 1, \ldots p - 1\}$ is a finite field
  - Also denoted as F_p or GF(p)
- For every prime number p and positive integer n, there exists a finite field with p^n elements
- The order of a field can be represented as p^n, where p is prime
  - p is called the characteristic of the field
  - Called a prime field if $n = 1$
  - Called a binary field if $p = 2$
- Any two finite fields with the same number of elements are isomorphic

Multiplicative group in a finite field is cyclic

- The multiplicative group of a finite field is a cyclic group

- There are φ(q – 1) generators for a group of size q
  - φ (x) is the Euler’s totient function

Links

- V. Shoup. A Computational Introduction to Number Theory and Algebra. https://shoup.net/ntb/ntb-v2.pdf

Évariste Galois

- Many myths surround Galois and his work
  - Trying to solve equations
    - General solution to quadratic equation was found many years ago
    - Solution also found for cubic and quartic equations
    - But how about quintic equations?
  - Submitted the paper to Grand Prize of the Paris Academy (1830)
  - Paper was rejected
    - Niels Henrik Abel proved quintic equations have no general solution (1826)
  - Extended the paper and …
    - Submitted to Fourier. Unfortunately, Fourier died and the paper was lost
    - Submitted to Cauchy, but Cauchy lost it
    - That year’s Prize was awarded to Abel and Carl Jacobi
    - Tried a year later
      - Nobody understood it
  - Three papers were published in 1830
    - Galois theory
  - Died on May 31, 1832 at the age of 20

Ring

Add multiplication operation (•) on an abelian group with addition

- The **abelian** group is a ring if
  - Multiplication is closed
    - $a \bullet b$ is also an element in the set
  - Multiplication is commutative
    - $a \bullet b = b \bullet a$
  - Multiplication associative
    - $a \bullet (b \bullet c) = (a \bullet b) \bullet c$
  - There is a multiplication identity 1
    - $a \bullet 1 = 1 \bullet a = a$
  - The distributive property is satisfied
    - $(a + b) \bullet c = (a \bullet c) + (b \bullet c)$
    - $a \bullet (b+c) = (a \bullet b) + (a \bullet c)$

Examples of ring

- Integers Z
- Real number R
- Complex numbers C
- Z_m is a ring
  - Z_m is a finite ring