Day 11

Primarity Test

Prime numbers that professors love

博士たちの愛する素数

Prime number, its enchantment

- Prime numbers
  - 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37.
- There are infinite number of prime numbers
  - Distribution of prime numbers
    - Prime number theorem
    - Riemann hypothesis
- The arithmetic of mod p → Finite field
- Important computation problems
  - Common divisor
  - Divisor
  - Prime number generation

Magic of powers of numbers

- I noticed a strange rule when I was a child
- If we compute powers of numbers, and list its lowest digit, then….
- 1 2 3 4 5 6 7 8 9
- 1 4 9 6 5 6 9 4 1
- 1 8 7 4 5 6 3 2 9
- 1 6 1 6 5 6 1 6 1
- 1 2 3 4 5 6 7 8 9

Primarity test： idea

- p= 111111111111 is a prime?
  - Fermat test (Fermat's theorem)
    - If p is a prime, for each a < p

      $a^{p-1} - 1$ is divisible by p
  - If Fermat test fails, not a prime
  - If Fermat test pass, either a prime number or a "Carmichael number"
  - How to exclude Carmichael numbers?

Primarity test algorithm

- Do 100 times
  - Randomly select $a<p$
  - compute $z = a^{(p-1)/2} \pmod{p}$
  - If z is not 1 nor p-1, return “non prime”
- If z = 1 for all 100 times, return “non prime”
- Otherwise, return “prime or prime power”

Fermat (little) theorem

- Theorem 1: For $b < p$, $b^{p-1} \bmod p = 1$
  - Proof: expand $(1+x)^p$
- Theorem 2: $b^{(p-1)/2} = 1$ or $-1 \bmod p$. Moreover, it becomes -1 for (p-1)/2 numbers.
  - Proof: Consider solution of euqation.

    $x^{(p-1)/2} = 1$ has at most (p-1)/2 solutions.

Fermat test is not sufficient

- Euler's theorem

For coprime n and b,

$$b^{\varphi(n)} \equiv 1 \pmod{n}$$

$\varphi(n)$ is the number of natural numbers less than n that are coprime to n

Euler number becomes n-1 if and only if n is prime.

If n = pqr, $\varphi(n)$ =(p − 1)(q − 1)(r − 1)

Carmichael number

For　n＝pqr and b coprime to n,

$$b^{\lambda(n)} \equiv 1 \pmod{n}$$

$$\lambda(n) = LCM(p-1, q-1, r-1)$$

If n = 3 x 11 x 17　＝561？(Carmichael number）

Difference：　For a Carmichal number, the power of b by (n-1)/2 is always 1

Old Japanese mathematics

- 105 subtraction: Jinko-ki (M. Yoshida 1627)
- 百五減算：　塵劫記（吉田光由、１６２７）
- We have less than 180 stones. 2 stones remain divided by 7, 1 remains divided by 5, and 1 remains divided by 3. How many?

碁石がいくつかあります。７個づつに分けると2個余ります。５個づつに分けると1個余ります。３個づつに分けると1個余ります。 碁石はいくつありますか？　ただし、碁石は最大で１８０個しかありません。

中国人剰余定理
（Chinese reminder theorem)

$n=n_1,n_2,..n_k$:mutiple of k coprime numbers

m_i : a positive number less than n_i

⇒ There exist a unique nonnegative $m<n$ satisfying $m \equiv m_i \pmod{n_i}$ $i=1,2,..,k$

Very old theorem!

Algorithm for finding m: Just similar to the Euclid's algoirthm

Justify primarity test

- Theorem (Primarity test)

  Assume n = pq where p and q are coprime. Then

  If there is an a such that $a^{(n-1)/2} \equiv -1$

There is a number b such that

  $b^{(n-1)/2}$ is neither 1 nor -1

  Also, there are more than (n-1)/2 such b

Chinese remainder theorem proves it!

Proof

- $a^{(n-1)/2} \equiv -1 \mod n$
- $n = km$
- CRT implies we have the following k
  - $b \equiv a \mod k$
  - $b \equiv 1 \mod m$
- $b^{(n-1)/2} \equiv -1 \mod k$
- $b^{(n-1)/2} \equiv 1 \mod m$
- Thus, $b^{(n-1)/2} \mod n$ is neither 1 nor -1

Correctness of primarity test

$c = a^{(n-1)/2} \mod n$

1. If c is 1 nor -1 ,n is not a prime
   1. Fermat Theorem
2. If always 1, n is not a prime
   1. Fermat Theorem and Primarity test theorem
3. If mix of 1 and —1, n is prime

But we cannot examine all a , thus 2 and 3 only holds with a high probability

The failure probability

- A prime is judged wrongly a composite
  - $a^{(p-1)/2} = 1$ holds for all 100 cadnidates of a
  - Probability $1/2^{100}$
- A composite is judged as a prime
  - There is an a to become -1, and it beomes 1 or -1 for all 100 candidates of a
  - Probability $1/2^{100}$