Primes

Dr. Odelu Vanga

Computer Science and Engineering
Indian Institute of Information Technology
Sri City, India

Prime Numbers

Prime numbers: divisors of 1 and itself

- They cannot be written as a product of other numbers

Prime: 2,3,5,7

Not primes: 4,6,8,9,10

List of prime number less than 200 is:

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59
61 67 71 73 79 83 89 97 101 103 107 109 113
127 131 137 139 149 151 157 163 167 173 179
181 191 193 197 199

Prime Factorisation

Factorization: $n = a \times b \times c$

Note that factoring a number is relatively hard compared to multiplying the factors together to generate the number

The **prime factorisation** of a number **n** is **unique**

(a product of primes)

$$91 = 7 \times 13$$

$$3600 = 2^4 \times 3^2 \times 5^2$$

Relatively Prime Numbers & GCD

Two numbers a, b are **relatively prime** if the **common divisor is** 1

- **Eg.** 8 and 15 are relatively prime

  since factors of 8 are 1,2,4,8 and

  15 are 1,3,5,15 and

  1 is the only common factor

- **eg.** $300=2^1\times3^1\times5^2$ and $18=2^1\times3^2$

  GCD $\mathbf{(18,300)=2^1\times3^1\times5^0=6}$

Fermat's Little Theorem

Let p is prime and a is a positive integer not divisible by p, then

$$a^{p-1} \bmod p = 1$$

Eg. p=7, a=4, $4^{7-1} \bmod 7 = 1$

- **In the above case, p divides exactly into $a^p - a$.**

Fermat's primality test is a necessary, but not sufficient test for primality.

- For example, let a = 2 and n = 341, then a and n are relatively prime and 341 divides exactly into $2^{341} - 2$.
- However, $341 = 11 \times 31$, so it is a composite number.
- Thus, 341 is a Fermat **pseudoprime** to the base 2

Euler Totient Function ø (n)

Number of relatively primes to **n** from 0 to (n-1).

- when doing arithmetic modulo n
- **Complete set of residues**: {0..n-1}

- **E.g.** for n=10,
- Complete set of residues: {0,1,2,3,4,5,6,7,8,9}
- Reduced set of residues: {1,3,7,9}

Euler Totient Function ø(n):

- number of elements in reduced set of residues of n
- **ø(10) = 4**

Euler Totient Function $\varnothing(n)$

To compute ø(n), we need to count number of elements to be excluded

In general, it needs prime factorization.

We know

- for p (p prime) $\varnothing(p) = p-1$
- for p.q (p,q prime) $\varnothing(p.q) = p-1)(q-1)$

E.g.

- $\varnothing(37) = 36$
- $\varnothing(21) = (3-1)\times(7-1) = 2\times 6 = 12$

Euler's Theorem

A generalisation of Fermat's Theorem

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

where gcd(a,n)=1

E.g.

- $a=3; n=10; \varnothing(10)=4;$

  Hence $3^4 = 81 = 1 \bmod 10$
- $a=2; n=11; \varnothing(11)=10;$

  Hence, $2^{10} = 1024 = 1 \bmod 11$

Primality Testing

Many cryptographic algorithms needs large prime numbers

Traditionally, **sieve** using **trial division**

- divide by all numbers (primes) in turn less than the square root of the number
- only works for small numbers

Statistical primality tests

- all prime numbers satisfy property
- But, some composite numbers, called **pseudo-primes**, also satisfy the property, with a low probability.

Prime is in P: Deterministic polynomial algorithm - 2002.

Miller Rabin Algorithm

A test based on Fermat's Theorem

TEST (n) is:

1. Find biggest k, $k > 0$, so that $(n-1)=2^k q$
2. Select a random integer a, $1<a<n-1$
3. **if** $a^q \bmod n = 1$ **then** return ("maybe prime");
4. **for** $j = 0$ **to** $k - 1$ **do**
   5. **if** $(a^{2^j q} \bmod n = n-1)$
      then return(" maybe prime ")
6. return ("composite")

TEST (n) is:

1. Find biggest k, $k > 0$, so that $(n-1)=2^k q$
2. Select a random integer a, $1<a<n-1$
3. **if** $a^q \bmod n = 1$ **then** return ("maybe prime");
4. **for** $j = 0$ **to** $k - 1$ **do**
    5. **if** ($a^{2^j q} \bmod n = n-1$)
        then return(" maybe prime ")
6. return ("composite")

Probabilistic Considerations

- **If Miller-Rabin returns "composite" the number is definitely not prime**
- **Otherwise is a prime or a pseudo-prime**
- Chance it detects a pseudo-prime is < ¼
- Hence if repeat test with different random a then chance n is prime after t tests is:
  - Pr(n prime after t tests) = $1-4^{-t}$
  - eg. for t=10 this probability is > 0.99999

Prime Distribution

- There are infinite prime numbers
  - Euclid's proof
- Prime number theorem states that
  - primes near n occur roughly every ($\ln n$) integers
- Since can immediately ignore evens and multiples of 5, in practice only need test $0.4 \ln(n)$ numbers before locate a prime around n
  - Note this is only the "average" sometimes primes are close together, at other times are quite far apart

THANK YOU