8.1 More Number Theory

Number theory: branch of pure mathematics concerned with properties of numbers in general, and integers in particular

Concepts from number theory are essential to public-key cryptographic algorithms

- Fermat's theorem
- Euler's theorem
- Discrete logarithms

Prime Factorization

To factor a number n is to write it as a product of other numbers

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

- Note: factoring a number is relatively hard compared to multiplying the factor together to generate the number

The **prime factorization** of a number n is when it's written s a product of primes

Any integer a > 1 can be factored uniquely as:

$$a = \prod_{p \in \mathrm{p}} p^{a_p} = p_1^{a_1} \times p_2^{a_2} \times ... \times p_t^{a_t}$$

- $p_1 < p_2 < \ldots < p_t$ are prime numbers
- a_i is a positive integer

Integer multiplication:

- Given:
  - $a = \prod_{p \in \mathrm{p}} p^{a_p}$
  - $b = \prod_{p \in \mathrm{p}} p^{b_p}$
- $k = ab$
- k can be expressed as the product of powers of primes:
  - $k = \prod_{p \in \mathrm{p}} p^{k_p}$
  - $k_p = a_p + b_p$ for all $p \in P$

Relatively Prime Numbers & GCD

Relatively Prime: two numbers a, b are **relatively prime** if they have no common divisors apart from 1.

If a divides b then:

- Given: $a = \prod_{p \in \mathrm{p}} p^{a_p}$, $b = \prod_{p \in \mathrm{p}} p^{b_p}$
- Then: $a_p \leq b_p$ for all p

Determining the GCD of two numbers

- If k = GCD(a,b), then $k_p = \min(a_p, b_p)$ for all p
- Not practical for large numbers due to difficulty of factoring
- Example:
  - $300 = 2^1 \times 3^1 \times 5^2$
  - $18 = 2^1 \times 3^2$
  - $\mathrm{GCD}(18,300) = 2^1 \times 3^1 \times 5^0 = 6$

Fermat's Theorem

Fermat's theorem: If p is prime and a is a positive integer not divisible by p, then

- $\mathbf{a^{p-1} \equiv 1 \ (mod\ p)}$
- Requires that a be relatively prime to p

Alternative form

- $\mathbf{a^{p} \equiv a \ (mod\ p)}$
- a doesn't have to be relatively prime to p (a can be divisible by p)

Fermat's Theorem Proof (Assume Basic True, Formulate Alternative)

1. Assume $a^{p-1} \equiv 1$ (mod p)
2. From (1) can write: $a^{p} \cdot a^{-1} \equiv 1$ (mod p)
3. Multiple a^{1} on both sides

   $\mathbf{a^1} \cdot a^p \cdot a^{-1} \equiv 1$ (mod p) $\mathbf{a^1}$

   $\mathbf{a^p \equiv a^1}$ **(mod p)** Proof Complete

Fermat's Theorem Proof (Basic Form)

1. Construct set X
   - X = {1,2,...,p-1}
2. Construct set X' by multiplying X with (a mod p)
   - X' = {a mod p, 2a mod p, ..., (p-1)a mod p}
3. Show p does divide a.
   a. Show no element in X' is equal to zero
      - Assume $(a*i) \equiv (a*p)(\text{mod } p) \rightarrow i \equiv p(\text{mod } p) \equiv 0(\text{mod } p)$
      - But $0 < i < p$
   b. Show elements in X' are unique
      - Assume $(a*i) \equiv (a*j)(\text{mod } p) \rightarrow i \equiv j(\text{mod } p)$
      - But $0 < i, j < p$, and $i \neq j$
   c. Show X' is equivalent to X thus...
      - $(a * 2a * \ldots * (p-1)a) \equiv (1 * 2 * \ldots * p-1)(\text{mod} p)$
      - $(p-1)!a^{p-1} \equiv (p-1)!(\text{mod } p)$, thus
      - $\mathbf{a^{p-1} \equiv 1(mod\ p)}$

Euler Totient Function ϕ(n)

Totient Function - ϕ(n): The number of positive integers less than n and relative prime to n

- Professors definition: computing ϕ(n) counts the number of residues to be excluded

For prime numbers p and q:

- $\phi(p) = p-1$
- $\phi(p \cdot q) = (p - 1) \cdot (q - 1)$

Proof for ϕ(p $\cdot$ q) = (p - 1) $\cdot$ (q - 1)

1. The integers in the complete set {1, ... , (pq -1)} that aren't relative prime to n can be taken out. They are:
   - {p, 2p, ..., (q - 1)p}
   - {q, 2q, ..., (p - 1)q}
2. From that you can rewrite the equation to:

$$\begin{aligned}\phi(\mathrm{n}) &= (\mathrm{pq} - 1) - [(\mathrm{q} - 1) + (\mathrm{p} - 1)] \\ &= \mathrm{pq} - (\mathrm{p} + \mathrm{q}) + 1 \\ &= (\mathrm{p} - 1) \times (\mathrm{q} - 1) \\ &= \phi(\mathrm{p}) \times \phi(\mathrm{q})\end{aligned}$$

Euler's Theorem

Euler's Theorem: A generalization of Fermat's theorem:

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

- If a and n are relatively prime

Proof:

1. n being prime is true due to Fermat's theorem
2. For any n:
   - Consider the reduced set of residues R = $\{x_1, x_2, \ldots, x_{\phi(n)}\}$
   - Consider R' = $\{(ax_1 \bmod n), (ax_2 \bmod n), \ldots, (ax_{\phi(n)} \bmod n)\}$
   - R' is equivalent to R, ..., similar to proof of Fermat's theory

Alternate Euler's Theorem: aˆϕ(n) + 1ˆ ≡ a (mod n)

- Like Fermat's, this form doesn't require a and n to be relatively prime

Primality Testing

Primality testing is needed because finding large prime numbers is useful (There's no simple way to do this though)

- Traditionally used **trial division**
  - Divide by all numbers(primes) in turn less than the square root of the number)
  - Only works for small numbers
- Alternatively can use **statistical primality testing** based on the necessary properties of primes for which all prime numbers satisfy property
  - Some composite numbers called pseudo-primes, can also satisfy the properties
- Can use a slower deterministic primality test

Two properties of Prime Numbers

First property

- If p is prime and a is a positive integer less than p, then

  a^2 mod p = 1 iff either [a mod p = 1] or [a mod p = p - 1]

Second property

- Let p be a prime number greater than 2. We can write p - 1 = $2^k q$ with k > 0, q odd. Let a be any integer in the range 1 < a < p - 1. Then one of the following conditions is true:
  1. a^q mod p = 1
  2. One of the numbers a^q, a^{2q}, a^{4q}, ..., $a^{2^{k-1}q}$mod p = p - 1

Miller Rabin Algorithm

A test based on prime properties that result from Fermat's Theorem

Algorithm:

- TEST(n) is:
  1. Find integers k , q, k > 0, q odd, so that (n - 1) = $2^k q$
  2. Select a random integer a, 1 < a < n - 1
  3. if a^q mod n = 1 then return ("inconclusive")
  4. For j = 0 to k - 1 do → if ($a^{2^j q}$ mod n = n - 1) then return("inconclusive")
  5. return("composite")

Probabilistic considerations:

- If Miller-Rabin returns "composite", the number is definitely not prime
- Otherwise, is a prime or a pseudo-prime
- Probability it returns "inconclusive" is < $\frac{1}{4}$
- Hence, if ran repeated test with different random a, then chance n is prime after t test is:
  - Pr(n prime after t tests) = 1 - 4^{-t}

Prime Distribution

Prime number theorem states that primes near n occur roughly one every (ln n) integers

- Can immediately ignore even numbers
- Therefore, in practice we only need to test 0.5ln(n) numbers of size n to locate a prime
  - This is only the average
  - Sometimes primes are close together
  - Other times are quite far apart

Primitive Roots

From Euler's theorem ($a^{\phi(n)}$mod n = 1), consider the general case:

> a^m mod n = 1

- if GCD(a,n) = 1, there must exist a m = ϕ(n)
- Smaller m may exist
- Once powers reach m, mod results will repeat

If smallest m = ϕ(n) then **a** is called a **primitive root of n**

- Successive powers of a "generate" ϕ(n) distinct integers relatively prime to n (a, a^2, a^3, ..., $a^{\phi(n)}$)
- For a prime number p, successive powers of a "generate" p-1 distinct integers relatively prime to p: (a, a^2, a^3, ..., a^{p-1})
- The only integers with primitive roots are those of the form 2, 4, p^a, and $2p^a$
  - p is any odd prime
  - a is a positive integer

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

Figure 1: Example of Powers mod 19 (n = 19), all a less than 19

Logarithms

Ordinary Logarithms

$y = x^{\log_x(y)}$

Properties:

- $\log_x(1) = 0$
- $\log_x(x) = 1$
- $\log_x(yz) = \log_x(y) + \log_x(z)$
- $\log_x(y^r) = r \times \log_x(y)$

Discrete Logarithms

The inverse problem to exponentiation modulo p is to find the **discrete logarithm** of a number modulo p.

- Similar to saying find i such that $b = a^i \pmod p$
  - i is the **discrete logarithm** of the number b for the base a (mod p)
  - written as $\mathbf{i = dlog_{a,p} b}$
- If a is a primitive root of p then i **always exist**, otherwise it may not exist or be unique
  - Example:
    - $i = \mathrm{dlog}_{5,19}\ 3$ has no answer, $i = \mathrm{dlog}_{5,19} 11$ has no unique answers
    - $i = \mathrm{dlog}_{10,19}\ 3 = 5$ by trying sucessive powers
- Whilst exponentiation is relatively easy, finding discrete logarithms is generally a hard problem

(a) Discrete logarithms to the base 2, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{2,19}(a)$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

(b) Discrete logarithms to the base 3, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{3,19}(a)$	18	7	1	14	4	8	6	3	2	11	12	15	17	13	5	10	16	9

(c) Discrete logarithms to the base 10, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{10,19}(a)$	18	17	5	16	2	4	12	15	10	1	6	3	13	11	7	14	8	9

(d) Discrete logarithms to the base 13, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{13,19}(a)$	18	11	17	4	14	10	12	15	16	7	6	3	1	5	13	8	2	9

(e) Discrete logarithms to the base 14, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{14,19}(a)$	18	13	7	8	10	2	6	3	14	5	12	15	11	1	17	16	4	9

(f) Discrete logarithms to the base 15, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{15,19}(a)$	18	5	11	10	8	16	12	15	4	13	6	3	7	17	1	2	14	9

Figure 2: Example of discrete logarithms with mod 19

Properties of discrete logarithms

- $\mathrm{dlog}_{a,p}(1) = 0$, because $a^0 \bmod p = 1 \bmod p = 1$
- $\mathrm{dlog}_{a,p}(a) = 1$, because $a^1 \bmod p = a \bmod p = a$
- $\mathrm{dlog}_{a,p}(xy) = [\mathrm{dlog}_{a,p}(x) + \mathrm{dlog}_{a,p}(y)] (\mathrm{mod}\ \phi(p))$
- $\mathrm{dlog}_{a,p}(y^r) = [r \cdot \mathrm{dlog}_{a,p}(y)] (\mathrm{mod}\ \phi(p))$