Cryptography and Network Security
Chapter 8

by William Stallings

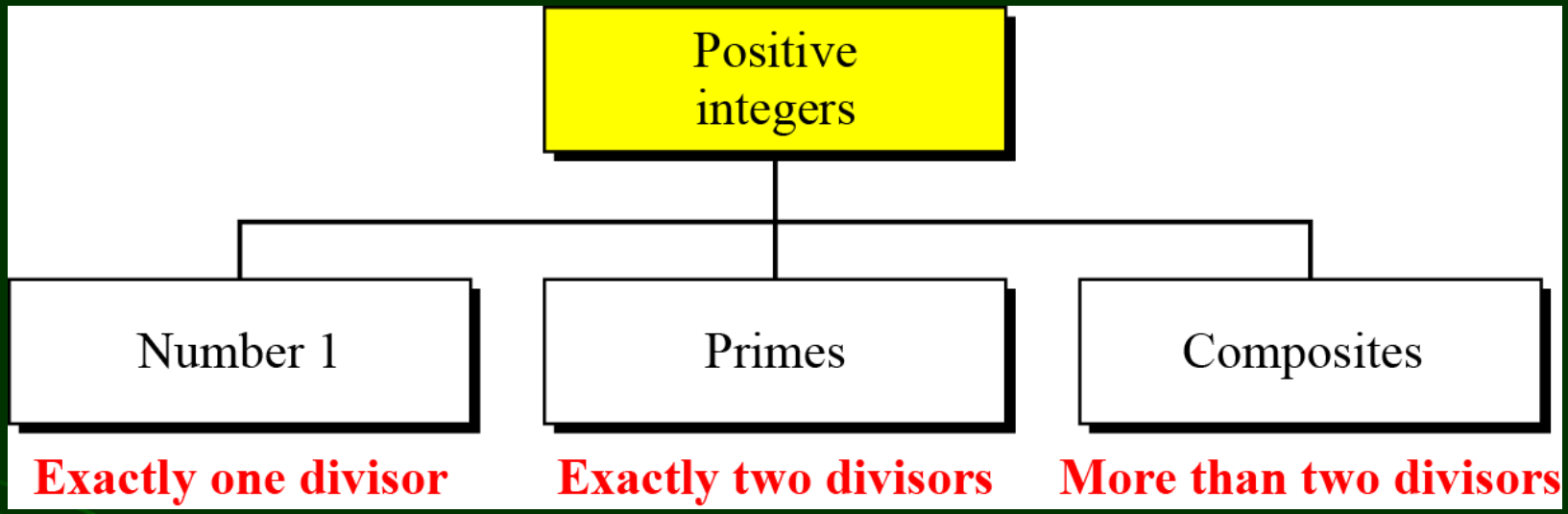
by B . A . Forouzan

Objectives

- To introduce prime numbers and their applications in cryptography.
- To discuss some primality test algorithms and their efficiencies.
- To discuss factorization algorithms and their applications in cryptography.
- To describe the Chinese remainder theorem and its application.
- To introduce quadratic congruence.
- To introduce modular exponentiation and logarithm.

9Definition

Figure *Three groups of positive integers*



Note

A prime is divisible only by itself and 1.

Prime Numbers

- prime numbers only have divisors of 1 and self
  - they cannot be written as a product of other numbers
  - note: 1 is prime, but is generally not of interest
- eg. 2,3,5,7 are prime, 4,6,8,9,10 are not
- prime numbers are central to number theory

Primes Under 2000

2	101	211	307	401	503	601	701	809	907	1009	1103	1201	1301	1409	1511	1601	1709	1801	1901
3	103	223	311	409	509	607	709	811	911	1013	1109	1213	1303	1423	1523	1607	1721	1811	1907
5	107	227	313	419	521	613	719	821	919	1019	1117	1217	1307	1427	1531	1609	1723	1823	1913
7	109	229	317	421	523	617	727	823	929	1021	1123	1223	1319	1429	1543	1613	1733	1831	1931
11	113	233	331	431	541	619	733	827	937	1031	1129	1229	1321	1433	1549	1619	1741	1847	1933
13	127	239	337	433	547	631	739	829	941	1033	1151	1231	1327	1439	1553	1621	1747	1861	1949
17	131	241	347	439	557	641	743	839	947	1039	1153	1237	1361	1447	1559	1627	1753	1867	1951
19	137	251	349	443	563	643	751	853	953	1049	1163	1249	1367	1451	1567	1637	1759	1871	1973
23	139	257	353	449	569	647	757	857	967	1051	1171	1259	1373	1453	1571	1657	1777	1873	1979
29	149	263	359	457	571	653	761	859	971	1061	1181	1277	1381	1459	1579	1663	1783	1877	1987
31	151	269	367	461	577	659	769	863	977	1063	1187	1279	1399	1471	1583	1667	1787	1879	1999
37	157	271	373	463	587	661	773	877	983	1069	1193	1283		1481	1597	1669	1789	1889	1997
41	163	277	379	467	593	673	787	881	991	1087		1289		1483		1693			1999
43	167	281	383	479	599	677	797	883	997	1091		1291		1487		1697			
47	173	283	389	487		683		887		1093		1297		1489		1699			
53	179	293	397	491		691				1097				1493					
59	181			499										1499					
61	191																		
67	193																		
71	197																		
73	199																		
79																			
83																			
89																			
97																			

Cardinality of Primes

Infinite Number of Primes

Note

There is an infinite number of primes.

Number of Primes

$$[n / (\ln n)] \quad < \quad \pi(n) \quad < \quad [n/(\ln n - 1.08366)]$$

Continued

Example

Find the number of primes less than 1,000,000.

Solution

The approximation gives the range 72,383 to 78,543. The actual number of primes is 78,498.

Checking for Primeness

Given a number n, how can we determine if n is a prime? The answer is that we need to see if the number is divisible by all primes less than

We know that this method is inefficient, but it is a good start.

Continued

Example

Is 97 a prime?

Solution

The floor of $\sqrt{97}$ = 9. The primes less than 9 are 2, 3, 5, and 7. We need to see if 97 is divisible by any of these numbers. It is not, so 97 is a prime.

Example

Is 301 a prime?

Solution

The floor of $\sqrt{301}$ = 17. We need to check 2, 3, 5, 7, 11, 13, and 17. The numbers 2, 3, and 5 do not divide 301, but 7 does. Therefore 301 is not a prime.

Continued

Sieve of Eratosthenes

Table 9.1 *Sieve of Eratosthenes*

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Prime Factorisation

- to **factor** a number `n` is to write it as a product of other numbers: `n=a x b x 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 when its written as a product of primes
  - eg. $91=7x13$; $3600=2^4x3^2x5^2$

$$a = \prod_{p \in \mathrm{P}} p^{a_p}$$

Relatively Prime Numbers & GCD

- two numbers a, b are **relatively prime** if have **no common divisors** apart from 1
  - eg. 8 & 15 are relatively prime since factors of 8 are 1,2,4,8 and of 15 are 1,3,5,15 and 1 is the only common factor
- conversely can determine the greatest common divisor by comparing their prime factorizations and using least powers
  - eg. $300=2^1 \times 3^1 \times 5^2$ $18=2^1 \times 3^2$ hence $GCD(18,300)=2^1 \times 3^1 \times 5^0=6$

Fermat's Theorem

- $a^{p-1} = 1 \pmod p$
  - where p is prime and $\gcd(a,p)=1$
- also known as Fermat's Little Theorem
- also $a^p = p \pmod p$
- useful in public key and primality testing

Fermat's Little Theorem

- Theorem If p is prime and a is a positive integer not divisible by p, then $a^{p-1} \equiv 1 \bmod p$
- Proof

  Start by listing the first p – 1 positive multiples of a:

  a, 2a, 3a, …, (p-1)a

  Suppose that ja and ka are the same modulo p, then we have

  $j \equiv k \bmod p$, so the p-1 multiples of a above are distinct and nonzero; that is, they must be congruent to 1, 2, 3, …, p-1 in some order. Multiply all these congruences together and we find

  $a \times 2a \times 3a \times \cdots \times (p-1)a \equiv 1 \times 2 \times 3 \times \cdots \times (p-1) \bmod p$

  or better, $a^{p-1}(p-1)! \equiv (p-1)! \bmod p$. Divide both side by (p-1)! to complete the proof.

- Corollary If p is prime and a is a positive integer, then $a^p \equiv a \bmod p$
- Corollary If p is prime and a is a positive integer not divisible by p, then a^{p-2} is an inverse of a modulo p

Euler's Phi-Function

Euler's phi-function, $\phi(n)$, which is sometimes called the Euler's totient function plays a very important role in cryptography.

The function finds number of integer that are smaller than n and relativly prime to n.

1. $\phi(1) = 0$.
2. $\phi(p) = p - 1$ if p is a prime.
3. $\phi(m \times n) = \phi(m) \times \phi(n)$ if m and n are relatively prime.
4. $\phi(p^e) = p^e - p^{e-1}$ if p is a prime.

Euler Totient Function ø(n)

- when doing arithmetic modulo n
- **complete set of residues** is: `0..n-1`
- **reduced set of residues** is those numbers (residues) which are relatively prime to n
  - eg for n=10,
  - complete set of residues is {0,1,2,3,4,5,6,7,8,9}
  - reduced set of residues is {1,3,7,9}
- number of elements in reduced set of residues is called the **Euler Totient Function ø(n)**

Euler Totient Function ø(n)

- to compute ø(n) need to count number of residues to be excluded
- in general need prime factorization, but
  - for p (p prime) ø(p) = p-1
  - for p.q (p,q prime) ø(pq) =(p-1)x(q-1)
- eg.

  ø(37) = 36

  ø(21) = (3-1)x(7-1) = 2x6 = 12

Continued

We can combine the above four rules to find the value of ϕ (n). For example, if n can be factored as

$$n = p_1^{e_1} \times p_2^{e_2} \times \ldots \times p_k^{e_k}$$

then we combine the third and the fourth rule to find

$$\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \times (p_2^{e_2} - p_2^{e_2-1}) \times \cdots \times (p_k^{e_k} - p_k^{e_k-1})$$

Note

The difficulty of finding ϕ(n) depends on the difficulty of finding the factorization of *n*.

Continued

Example

What is the value of $\phi(13)$?

Solution

Because 13 is a prime, $\phi(13) = (13 - 1) = 12$.

Example

What is the value of $\phi(10)$?

Solution

We can use the third rule: $\phi(10) = \phi(2) \times \phi(5) = 1 \times 4 = 4$, because 2 and 5 are primes.

Continued

Example

What is the value of $\phi(240)$?

Solution

Example

Can we say that $\phi(49) = \phi(7) \times \phi(7) = 6 \times 6 = 36$?

Solution

Continued

Example

What is the value of $\phi(240)$?

Solution

We can write $240 = 2^4 \times 3^1 \times 5^1$. Then

$$\phi(240) = (2^4 - 2^3) \times (3^1 - 3^0) \times (5^1 - 5^0) = 64$$

Example

Can we say that $\phi(49) = \phi(7) \times \phi(7) = 6 \times 6 = 36$?

Solution

No. The third rule applies when *m* and *n* are relatively prime. Here $49 = 7^2$. We need to use the fourth rule: $\phi(49) = 7^2 - 7^1 = 42$.

Continued

Example

What is the number of elements in Z_{14}^*?

Solution

The answer is $\phi(14) = \phi(7) \times \phi(2) = 6 \times 1 = 6$. The members are 1, 3, 5, 9, 11, and 13.

Note

Interesting point: If $n > 2$, the value of $\phi(n)$ is even.

Euler's Theorem

- a generalisation of Fermat's Theorem
- $a^{\phi(n)} = 1 \pmod{n}$
  - for any a, n where $\gcd(a,n)=1$
- eg.

  $a=3; n=10; \phi(10)=4;$

  hence $3^4 = 81 = 1 \bmod 10$

  $a=2; n=11; \phi(11)=10;$

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

Euler's Theorem

- Generalization of Fermat's little theorem
- Theorem For every a and n that are relatively prime,

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

- Proof
  - The proof is completely analogous to that of the Fermat's Theorem except that instead of the set of residues {1,2,...,n-1} we now consider the set of residues $\{x_1,x_2,...,x_{\phi(n)}\}$ which are relatively prime to n. In exactly the same manner as before, multiplication by a modulo n results in a permutation of the set $\{x_1, x_2, ..., x_{\phi(n)}\}$. Therefore, two products are congruent:

$$x_1x_2 \ldots x_{\phi(n)} \equiv (ax_1)(ax_2) \ldots (ax_{\phi(n)}) \bmod n$$

  dividing by the left-hand side proves the theorem.
- Corollary

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

  (2) If gcd(a,n) = 1, then $a^{\phi(n)-1}$ is an inverse of a modulo n

Primality Testing

- often need to find large prime numbers
- traditionally **sieve** using **trial division**
  - ie. 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 tests based on properties of primes
  - for which all primes numbers satisfy property
  - but some composite numbers, called pseudo-primes, also satisfy the property
- can use a slower deterministic primality test

Miller Rabin Algorithm

- a test based on Fermat's Theorem for odd integer number p.
- algorithm is:

TEST (p) is:

1. Find integers b,c such that b > 0, c is odd, so that $(p-1)=2^b*c$
2. Select a random integer a, $1<a<p-1$
3. **if** $a^c \bmod p = r = \pm 1$ **then** return ("maybe prime");
4. **for** j = 0 **to** b– 1 **do**
5. **if** ($r^{2^j} \bmod p = n-1=-1$)**then**

return(" maybe prime ")

else

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 < $^1/_4$
- 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

Example

- Apply the Miller Rabin Test to P=23.
- Step 1:- (p-1) =2= $2^1 * 11$

  b=1,c=11.
- Step 2:- select random number a=15.
- Step 3:-compute 15^{11} mod 23
- 15^{11} mod 23 =22 ≡ -1mod 23

thus 23 may be a prime number.

Example

- Apply the Miller Rabin Test to P=143.
- Step 1:- (p-1) =144= $2^4 * 9$
  b=4,c=9, j=1,2,3.
- Step 2:- select random number a=47.
- Step 3:-compute 47^9 mod 143
- 47^9 mod 143 =125
- Step 4:-compute r^{2j} mod 143 where r=125,j=1,2,3.
  for j =1 , r^2 mod 143 =125^2 mod 143 =38≠ -1
  for j =2 , r^4 mod 143 =38^2 mod 143 =14≠ -1
  for j =3 , r^6 mod 143 =14^2 mod 143 =53≠ -1

Thus we can say that p is not a prime number definitely

CHINESE REMAINDER THEOREM

The Chinese remainder theorem (CRT) is used to solve a set of congruent equations with one variable but different moduli, which are relatively prime, as shown below:

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\cdots$$
$$x \equiv a_k \pmod{m_k}$$

Continued

Example

The following is an example of a set of equations with different moduli:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

The solution to this set of equations is given in the next section; for the moment, note that the answer to this set of equations is x = 23. This value satisfies all equations: 23 ≡ 2 (mod 3), 23 ≡ 3 (mod 5), and 23 ≡ 2 (mod 7).

Continued

Solution To Chinese Remainder Theorem

1. Find $M = m_1 \times m_2 \times \ldots \times m_k$. This is the common modulus.
2. Find $M_1 = M/m_1$, $M_2 = M/m_2$, …, $M_k = M/m_k$.
3. Find the multiplicative inverse of M_1, M_2, …, M_k using the corresponding moduli (m_1, m_2, …, m_k). Call the inverses M_1^{-1}, M_2^{-1}, …, M_k^{-1}.
4. The solution to the simultaneous equations is

$$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \cdots + a_k \times M_k \times M_k^{-1}) \bmod M$$

Continued

Example

Find the solution to the simultaneous equations:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

Solution

We follow the four steps.

1. $M = 3 \times 5 \times 7 = 105$

2. $M_1 = 105 / 3 = 35$, $M_2 = 105 / 5 = 21$, $M_3 = 105 / 7 = 15$

3. The inverses are $M_1^{-1} = 2$, $M_2^{-1} = 1$, $M_3^{-1} = 1$

4. $x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105 = 23 \bmod 105$

Continued

Example

Find an integer that has a remainder of 3 when divided by 7 and 13, but is divisible by 12.

Solution

This is a CRT problem. We can form three equations and solve them to find the value of x.

$$x = 3 \bmod 7$$
$$x = 3 \bmod 13$$
$$x = 0 \bmod 12$$

If we follow the four steps, we find x = 276. We can check that 276 = 3 mod 7, 276 = 3 mod 13 and 276 is divisible by 12 (the quotient is 23 and the remainder is zero).

Chinese Remainder Theorem

- used to speed up modulo computations
- if working modulo a product of numbers
  - eg. $\mod M = m_1 m_2 .. m_k$
- Chinese Remainder theorem lets us work in each moduli m_i separately
- since computational cost is proportional to size, this is faster than working in the full modulus M

Chinese Remainder Theorem

- can implement CRT in several ways
- to compute $A \pmod{M}$
  - first compute all $a_i = A \bmod m_i$ separately
  - determine constants c_i below, where $M_i = M/m_i$
  - then combine results to get answer using:

$$A \equiv \left(\sum_{i=1}^{k} a_i c_i \right) \pmod{M}$$

$$c_i = M_i \times (M_i^{-1} \bmod m_i) \quad \text{for } 1 \leq i \leq k$$

Chinese Remainder Theorem

- Chinese Remainder Theorem (CRT)

  Suppose $m_1, \ldots, m_k$ are pairwise relatively prime positive integers, and suppose $a_1, \ldots, a_k$ are integers. Then the system of k congruences $x \equiv a_i \pmod{m_i}$ $(1 \le i \le k)$ has a unique solution modulo $M = m_1 \times \cdots \times m_k$, which is given by

$$x = \sum_{i=1}^{k} a_i c_i \mod M,$$

  where $c_i = M_i (M_i^{-1} \bmod m_i)$ and $M_i = M / m_i$, for $1 \le i \le k$.

Chinese Remainder Theorem

Proof

- Let $M = m_1 \times m_2 \times \ldots \times m_k$, where m_i's are pairwise relatively prime, i.e., $\gcd(m_i, m_j) = 1$, $1 \le i \ne j \le k$
- $A \leftrightarrow (a_1, a_2, \ldots, a_k)$, where $A \in Z_M$, $a_i \in Z_{m_i}$, and $a_i = A \bmod m_i$ for $1 \le i \le k$
- One to one correspondence (bijection) between Z_M and the Cartesian product $Z_{m_1} \times Z_{m_2} \times \ldots \times Z_{m_k}$
  - For every integer A such that $0 \le A < M$, there is a unique k-tuple $(a_1, a_2, \ldots, a_k)$ with $0 \le a_i < m_i$
  - For every such k-tuple $(a_1, a_2, \ldots, a_k)$, there is a unique A in Z_M
    - Computing A from $(a_1, a_2, \ldots, a_k)$ is done as follows:
    - Let $M_i = M/m_i$ for $1 \le i \le k$, i.e., $M_i = m_1 \times m_2 \times \ldots \times m_{i-1} \times m_{i+1} \times \ldots \times m_k$
    - Note that $M_i \equiv 0 \pmod{m_j}$ for all $j \ne i$ and $\gcd(M_i, m_i) = 1$
    - Let $c_i = M_i \times (M_i^{-1} \bmod m_i)$ for $1 \le i \le k$
    - Then $A \equiv (a_1c_1 + a_2c_2 + \cdots + a_kc_k) \bmod M$

      $\leftarrow a_i = A \bmod m_i$, since $c_j \equiv M_j \equiv 0 \pmod{m_i}$ if $j \ne i$ and $c_i \equiv 1 \pmod{m_i}$

Chinese Remainder Theorem

- Operations performed on the elements of Z_M can be equivalently performed on the corresponding k-tuples by performing the operation independently in each coordinate position
  - ex) $A \leftrightarrow (a_1, a_2, \ldots, a_k)$, $B \leftrightarrow (b_1, b_2, \ldots, b_k)$

    $(A + B) \bmod M \leftrightarrow ((a_1 + b_1) \bmod m_1, \ldots, (a_k + b_k) \bmod m_k)$

    $(A - B) \bmod M \leftrightarrow ((a_1 - b_1) \bmod m_1, \ldots, (a_k - b_k) \bmod m_k)$

    $(A \times B) \bmod M \leftrightarrow ((a_1 \times b_1) \bmod m_1, \ldots, (a_k \times b_k) \bmod m_k)$

- CRT provides a way to manipulate (potentially large) numbers mod M in term of tuples of smaller numbers

Chinese Remainder Theorem

- Example
  - Let $m_1 = 37$, $m_2 = 49$, $M = m_1 \times m_2 = 1813$, $A = 973$, $B = 678$
  - $M_1 = 49$, $M_2 = 37$
  - Using the extended Euclid's algorithm
    - $M_1^{-1} \bmod m_1 = 34$, and $M_2^{-1} \bmod m_2 = 4$
  - Taking residues modulo 37 and 49
    - $973 \leftrightarrow (11, 42)$, $678 \leftrightarrow (12, 41)$
  - Add the tuples element-wise
    - $(11 + 12 \bmod 37, 42 + 41 \bmod 49) = (23, 34)$
  - To verify, we compute
    - $(23, 34) \leftrightarrow (a_1c_1 + a_2c_2) \bmod M = (a_1M_1M_1^{-1} + a_2M_2M_2^{-1}) \bmod M$
      $= [(23)(49)(34) + (34)(37)(4)] \bmod 1813 = 1651$
    - which is equal to $(678 + 973) \bmod 1813 = 1651$

Primitive Roots

- from Euler's theorem have $a^{\phi(n)} \bmod n = 1$
- consider $a^m = 1 \pmod n$, $\gcd(a,n) = 1$
  - must exist for $m = \phi(n)$ but may be smaller
  - once powers reach m, cycle will repeat
- if smallest is $m = \phi(n)$ then a is called a **primitive root**
- if p is prime, then successive powers of a "generate" the group $\bmod p$
- these are useful but relatively hard to find

Powers of Integers, modulo 19

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

a : primitive root

Discrete Logarithms

- the inverse problem to exponentiation is to find the **discrete logarithm** of a number modulo p
- that is to find x such that $y = g^x \pmod p$
- this is written as $x = \log_g y \pmod p$
- if g is a primitive root then it always exists, otherwise it may not, eg.
  - $x = \log_3 4 \bmod 13$ has no answer
  - $x = \log_2 3 \bmod 13 = 4$ by trying successive powers
- whilst exponentiation is relatively easy, finding discrete logarithms is generally a **hard** problem

Powers of Integers, modulo 19

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

a : primitive root

Summary

- have considered:
  - prime numbers
  - Fermat's and Euler's Theorems & ø(n)
  - Primality Testing
  - Chinese Remainder Theorem
  - Discrete Logarithms