National Chung Cheng University

Department of Information Management

More Number Theory

Pei-Ju (Julian) Lee

National Chung Cheng University

Information Security

pjlee@mis.ccu.edu.tw

Fall, 2016

Overview

- A number of concepts from number theory are essential in the design of public-key cryptographic algorithms
- A central concern of number theory is the study of prime numbers

Prime Numbers

- Prime numbers only have divisors of ±1 and itself (±p)
  - They cannot be written as a product of other numbers
- Prime numbers are central to number theory
- Any integer $a > 1$ can be factored in a unique way as

$$a = p_1^{a1} * p_2^{a2} * \ldots * p_t^{at}$$

where $p_1 < p_2 < \ldots < p_t$ are prime numbers and where each a_i is a positive integer

- This is known as the fundamental theorem of arithmetic

Cont'd

$$a = p_1^{a_1} \times p_2^{a_2} \times \cdots \times p_t^{a_t} \qquad a = \prod_{p \in P} p^{a_p} \quad \text{where each } a_p \geq 0$$

Ex.

$$91 = 7 \times 13$$
$$3600 = 2^4 \times 3^2 \times 5^2$$
$$11011 = 7 \times 11^2 \times 13$$

Express in another way:

Given $a = \prod_{p \in P} p^{a_p}$, $b = \prod_{p \in P} p^{b_p}$. Define $k = ab$.

$$k = \prod_{p \in P} p^{k_p} \qquad k_p = a_p + b_p \text{ for all } p \in P$$

Ex.

$$k = 12 \times 18 = (2^2 \times 3) \times (2 \times 3^2) = 216$$
$$k_2 = 2 + 1 = 3;\ k_3 = 1 + 2 = 3$$
$$216 = 2^3 \times 3^3 = 8 \times 27$$

Cont'd

- Any integer of the form p^n can be divided only by an integer that is of a lesser or equal power of the same prime number, p^j with $j \leq n$

$$a = \prod_{p \in P} p^{a_p}, b = \prod_{p \in P} p^{b_p} \quad \text{If a}|\text{b, then } a_p \leq b_p \text{ for all } p.$$

$a = 12; b = 36; 12|36$

$12 = 2^2 \times 3; 36 = 2^2 \times 3^2$

$a_2 = 2 = b_2$

$a_3 = 1 \leq 2 = b_3$

Thus, the inequality $a_p \leq b_p$ is satisfied for all prime numbers.

Cont'd

- It is easy to determine the GCD of two positive integers if we express each integer as the product of primes

If $k = \gcd(a, b)$, then $k_p = \min(a_p, b_p)$ for all p.

$$300 = 2^2 \times 3^1 \times 5^2$$
$$18 = 2^1 \times 3^2$$
$$\gcd(18, 300) = 2^1 \times 3^1 \times 5^0 = 6$$

- Determining the prime factors of a large number is no easy task

Primes less than 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	1993
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																			

Fermat's Theorem

- If *p* is prime and *a* is a positive integer not divisible by *p* then

$$a^{p-1} \equiv 1 \pmod{p}$$

  - a.k.a. Fermat's Little Theorem

- An alternate form is:
  - If *p* is prime and *a* is a positive integer then

$$a^{p} \equiv a \pmod{p}$$

The first form of Fermat's theorem requires that *a* be relatively prime to *p*, but the alternative form does not

- Plays an important role in public-key cryptography

Cont'd

- $a^{p-1} \equiv 1 \pmod{p}$

$$
\begin{aligned}
&a = 7, p = 19 \\
&7^2 = 49 \equiv 11 \pmod{19} \\
&7^4 \equiv 121 \equiv 7 \pmod{19} \\
&7^8 \equiv 49 \equiv 11 \pmod{19} \\
&7^{16} \equiv 121 \equiv 7 \pmod{19} \\
&a^{p-1} = 7^{18} = 7^{16} \times 7^2 \equiv 7 \times 11 \equiv 1 \pmod{19}
\end{aligned}
$$

- $a^p \equiv a \pmod{p}$

$$
\begin{aligned}
&p = 5, a = 3 \qquad a^p = 3^5 = 243 \equiv 3 \pmod{5} = a \pmod{p} \\
&p = 5, a = 10 \qquad a^p = 10^5 = 100000 \equiv 10 \pmod{5} \equiv 0 \pmod{5} = a \pmod{p}
\end{aligned}
$$

Euler's Totient Function

- Euler's totient function: $\Phi(n)$, phi function
  - The number of positive integers less than *n* and relatively prime to *n*
  - By convention, $\Phi(1) = 1$
  - For a prime number *p*: $\Phi(p) = p - 1$
    - Ex. Determine *Φ(37) and Φ(35)*
      - 37 is prime, all of the positive integers from 1 through 36 are relatively prime to 37. Thus *Φ(37) = 36*
      - All of the positive integers less than 35 that are relatively prime to it: 1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34. So *Φ(35) = 24*

Cont'd

- Euler's totient function: $\Phi(n)$, phi function
  - For two prime numbers p and q with $p \neq q$, then for $n = pq$:

    $\Phi(n) = \Phi(pq) = \Phi(p) \times \Phi(q) = (p-1) \times (q-1)$

    - *Ex.* $\Phi(21) = \Phi(3) \times \Phi(7) = (3-1) \times (7-1) = 2 \times 6 = 12$ where the 12 integers are {1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20}

Euler's Totient Function *ø(n)*

n	$\phi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4

n	$\phi(n)$
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8

n	$\phi(n)$
21	12
22	10
23	22
24	8
25	20
26	12
27	18
28	12
29	28
30	8

Note: Φ(p) = p - 1

Euler's Theorem

- For every *a* and *n* that are relatively prime (i.e. if gcd(a, n) = 1)

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

- An alternative form is

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

Similar to the case with Fermat's theorem, the first form of Euler's theorem requires that *a* be relatively prime to *n*, but the alternative form does not

- Play an important role in public-key cryptography

$$a = 3; n = 10; \phi(10) = 4 \quad a^{\phi(n)} = 3^4 = 81 = 1 \pmod{10} = 1 \pmod{n}$$
$$a = 2; n = 11; \phi(11) = 10 \quad a^{\phi(n)} = 2^{10} = 1024 = 1 \pmod{11} = 1 \pmod{n}$$

Testing for Primary

- Determining whether a given large number is prime
  - Miller-Rabin Algorithm

Properties of Prime Numbers

- First property:
  - If p is prime and a is a positive integer less than p, then $a^2 \bmod p = 1$ if and only if
    - either $a \bmod p = 1$
    - or $a \bmod p = -1 \bmod p = p - 1$.
  - By the rules of modular arithmetic $(a \bmod p)(a \bmod p) = a^2 \bmod p$.
    - If either $a \bmod p = 1$ or $a \bmod p = -1$, then $a^2 \bmod p = 1$.
    - Conversely, if $a^2 \bmod p = 1$, then $(a \bmod p)^2 = 1$, which is true only for $a \bmod p = 1$ or $a \bmod p = -1$.

Cont'd

- Second property:
  - Let p be a prime number greater than 2. We can then 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 two following conditions is true.
    - 1. a^q is congruent to 1 modulo p. That is, $a^q \bmod p = 1$, or equivalently, $a^q \equiv 1 \pmod{p}$.
    - 2. One of the numbers $a^q, a^{2q}, a^{4q}, \ldots, a^{2^{k-1}q}$ is congruent to -1 modulo p. That is, there is some number j in the range $(1 \leq j \leq k)$ such that $a^{2^{j-1}q} \bmod p = -1 \bmod p = p - 1$ or equivalently, $a^{2^{j-1}q} \equiv -1 \pmod{p}$.

Miller-Rabin Algorithm

- Typically used to test a large number for primality
- Algorithm to TEST (n) (n is odd integer and n≥3)

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

Example

- Apply the test to the prime number n=29
  - $(n-1) = 28 = 2^2(7) = 2^k q$. [k=2, q=7]
    - Try a = 10, $a^q \bmod n = 10^7 \bmod 29 = 17$ which is neither 1 nor 28
      - For $j = 0$ to $k - 1$, $a^{2^j q} \bmod n = 10^{2^1 7} \bmod 29 = 10^{14} \bmod 29 = 28$ equal to n-1. The test returns inconclusive (i.e. 29 may be prime)
    - Try a = 2, $a^q \bmod n = 2^7 \bmod 29 = 12$ which is neither 1 nor 28
      - For $j = 0$ to $k - 1$, $a^{2^j q} \bmod n = 2^{2^1 7} \bmod 29 = 2^{14} \bmod 29 = 28$ equal to n-1. The test returns inconclusive
    - If we perform the test for all integers a from 1~28, we get the same inconclusive result, which is compatible with n being a prime number

If continues to return inconclusive for t tests, then for a sufficient large value of t, assume n is prime

Example-2

- Apply the test to the composite number n=13*17=221
  - (n-1) = 220 = $2^2(55) = 2^k q$. [k=2, q=55]
    - Try a = 5, $a^q \bmod n = 5^{55} \bmod 221 = 112$ which is neither 1 nor 220
      - For $j = 0$ to $k - 1$, $a^{2^j q} \bmod n = 5^{2^1 55} \bmod 221 = 5^{110} \bmod 221 = 168$ which is not equal to (n-1)=220. The test returns composite.
    - If we try a = 21, $a^q \bmod n = 21^{55} \bmod 221 = 220$
      - For $j = 0$ to $k - 1$, $a^{2^j q} \bmod n = 21^{2^1 55} \bmod 221 = 21^{110} \bmod 221 = 220$ equal to n-1. The test returns inconclusive.
    - 218 integers from 2~219, four of these will return inconclusive result, namely 21, 47, 174, 220.

Go through every a from $1 < a < n - 1$, make sure no result is composite

Confidence of Whether An Integer is Prime

- Use Miller-Rabin algorithm to determine whether an odd integer *n* is prime with a reasonable degree of confidence
  - [KNUT98]: An odd number *n* that is not prime and a randomly chosen integer, *a* with $1 < a < n - 1$, the probability that TEST will return inconclusive (i.e., fail to detect that n is not prime) is less than ¼
  - Thus, if t different values of a are chosen, the probability that all of them will pass TEST (return inconclusive) for n is less than $(¼)^t$

Cont'd

- The procedure is as follows:
  - Repeatedly invoke TEST (*n*) using randomly chosen values for *a*. If, at any point, TEST returns composite, then *n* is determined to be nonprime. If TEST continues to return inconclusive for *t* tests, then for a sufficiently large value of *t*, assume that *n* is prime.

Distribution of Primes

- A result from number theory (a.k.a. prime number theorem) states:
  - The primes near *n* are spaced on the average one every *ln (n)* integers
    - On average, one would have to test on the order of *ln(n)* integers before a prime is found
    - All even integers can be immediately rejected, the correct figure is *0.5 ln(n)*
      - Ex. Prime around 2^{200}, then about *0.5 ln(2200) = 69* trials would be needed

Chinese Remainder Theorem (CRT)

- To reconstruct integers in a certain range from their residues modulo a set of pairwise relatively prime moduli

> The 10 integers in Z_{10}, that is the integers 0 through 9, can be reconstructed from their two residues modulo 2 and 5 (the relatively prime factors of 10). Say the known residues of a decimal digit x are $r_2 = 0$ and $r_5 = 3$; that is, $x \bmod 2 = 0$ and $x \bmod 5 = 3$. Therefore, x is an even integer in Z_{10} whose remainder, on division by 5, is 3. The unique solution is $x = 8$.

  - 2 and 5 are relatively prime.
  - *x mod 2 = 0, x mod 5 = 3*. Find *x*.

Cont'd

- Let $M = \prod_{i=1}^{k} m_i$ where m_i are pairwise relatively prime; that is, $\gcd(m_i, m_j) = 1$ for $1 \leq i, j \leq k$, and $i \neq j$.
- Represent any integer A in Z_M by a k-tuple whose elements are in Z_{mi} using the following correspondence:
  - $A \leftrightarrow (a_1, a_2, \ldots, a_k)$ where $A \in Z_M$, $ai \in Z_{mi}$, and $a_i = A \bmod mi$ for $1 \leq i \leq k$.

Cont'd

- The CRT makes two assertions.
  - 1. The mapping of Equation $A \leftrightarrow (a_1, a_2, \ldots, a_k)$ is a one-to-one correspondence (called a bijection) between Z_M and the Cartesian product $Z_{m1} * Z_{m2} * \ldots * Z_{mk}$. That is, for every integer A such that $0 \le A \le M$, there is a unique k-tuple $(a_1, a_2, \ldots, a_k)$ with $0 \le a_i < m_i$ that represents it, and for every such k-tuple $(a_1, a_2, \ldots, a_k)$, there is a unique integer A in Z_M.
    - E.g. each a_i is uniquely calculated as $a_i = A \bmod m_i$. Computing A from $(a_1, a_2, \ldots, a_k)$ can be done as follows. Let $M_i = M/m_i$ for $1 \le i \le k$. Note that $M_i = m_1 * m_2 * \ldots * m_{i-1} * m_{i+1} * \ldots * m_k$, so that $M_i \equiv 0 \pmod{m_j}$ for all $j \ne i$.
      Then let $c_i = M_i * (M_i^{-1} \bmod m_i)$ for $1 \le i \le k$
    - By the definition of M_i, it is relatively prime to m_i and therefore has a unique multiplicative inverse mod m_i. So Equation $c_i = M_i * (M_i^{-1} \bmod m_i)$ is well defined and produces a unique value c_i. We can now compute

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

    - To show that the value of A produced by previous Equation is correct, we must show that $a_i = A \bmod m_i$ for $1 \le i \ldots k$. Note that $c_j \equiv M_j \equiv 0 \pmod{mi}$ if $j \ne i$, and that $c_i \equiv 1 \pmod{m_i}$. It follows that $a_i = A \bmod m_i$.

Cont'd

- 2. 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 in the appropriate system.
  - E.g. If
    $A \leftrightarrow (a_1, a_2, \ldots, a_k)$
    $B \leftrightarrow (b_1, b_2, \ldots, b_k)$
  - Then
    $(A + B) \bmod M \leftrightarrow ((a_1 + b_1) \bmod m_1, \ldots, (a_k + b_k) \bmod m_k)$
    $(A - B) \bmod M \leftrightarrow ((a_1 - b_1) \bmod m_1, \ldots, (a_k - b_k) \bmod m_k)$
    $(A * B) \bmod M \leftrightarrow ((a_1 * b_1) \bmod m_1, \ldots, (a_k * b_k) \bmod m_k)$

Discrete Logarithms

- Fundamental to a number of public-key algorithms, including
  - Diffie-Hellman key exchange
  - Digital signature algorithm (DSA)
- Recall:
  - Euler's theorem, for every *a* and *n* that are relatively prime, $a^{\phi(n)} \equiv 1 \pmod{n}$
  - $\Phi(n)$, Euler's totient function, is the number of positive integers less than *n* and relatively prime to *n*

Cont'd

- Consider the more general expression:
  - $a^m \equiv 1 \pmod{n}$
  - If *a* and *n* are relatively prime, then there is at least one integer *m* that satisfies this equation, namely, $M = \Phi(n)$.
  - The least positive exponent *m* holds is referred to in several ways:
    - The **order** of *a (mod n)*
    - The **exponent** to which *a* belongs *(mod n)*
    - The **length** of the period generated by *a*
  - Ex. The power of 7, modulo 19:
    - $7^1 \equiv 7 \pmod{19}$
    - $7^2 \equiv 49 = 2 * 19 + 11 \equiv 11 \pmod{19}$
    - $7^3 \equiv 343 = 18 * 19 + 1 \equiv 1 \pmod{19}$
    - $7^4 \equiv 2401 = 126 * 19 + 7 \equiv 7 \pmod{19}$
    - $7^5 \equiv 16807 = 884 * 19 + 11 \equiv 11 \pmod{19}$

So $7^{3+j} \equiv 7^3 7^j \equiv 7^j \pmod{19}$. The length of the period is the smallest positive exponent *m* such that $7^m \equiv 1 \pmod{19}$.

Cont'd

- All the powers of *a*, modulo 19 for all positive *a* < *19.* *Ex.* $7^3 \equiv 1 \pmod{19}$
- Length for each base value: indicated by shading

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

Cont'd

- Note the following:
  - 1. All sequences end in 1.
  - 2. The length of a sequence divides $\Phi(19) = 18$.
    - That is, an integral number of sequences occur in each row of the table.
  - 3. Some of the sequences are of length 18. i.e. the base integer *a* generates (via powers) the set of nonzero integers modulo 19.
    - Each such integer is called a primitive root of the modulus 19.
      - Ex. Primitive roots for 19: 2, 3, 10, 13, 14, 15.
- More generally, the highest possible exponent to which a number can belong (mod *n*) is $\Phi(n)$

Cont'd

- More generally, the highest possible exponent to which a number can belong (mod *n*) is $\Phi(n)$
- If *a* is a primitive root of *n*, then its powers a, $a^2,\ldots,a^{\Phi(n)}$ are distinct (mod n) and are all relatively prime to *n*
  - Ex. Primitive roots for 19: 2, 3, 10, 13, 14, 15 are relatively prime to 19
- Not all integers have primitive roots.
  - The only integers with primitive roots are those of the form 2, 4, p^a, and $2p^a$, where *p* is any odd prime and *a* is a positive integer

Logarithms for Modular Arithmetic

- With ordinary positive real numbers, the logarithm function is the inverse of exponentiation
  - An analogous function exists for modular arithmetic
- Briefly review the properties of ordinary logarithms:
  - The logarithm of a number is defined to be the power to which some positive base (except 1) must be raised in order to equal the number. That is, for base x and for a value y,

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

Cont'd

- The properties of logarithms:
  - $log_x(1) = 0$
  - $log_x(x) = x$
  - $log_x(yz) = log_x(y) + log_x(z)$
  - $log_x(y^r) = r \times log_x(y)$
- Many texts refer to the discrete logarithm as the index. There is no generally agreed notation for this concept, much less an agreed name

Cont'd

- Consider a primitive root *a* for some prime number *p*
  - We know that
    - The powers of *a* from 1 through *(p - 1)* produce each integer from 1 through *(p - 1)* exactly once
    - Any integer *b* satisfies ***b ≡ r(mod p)*** for some r, where *0 ≤ r ≤ (p-1)*
  - It follows that for any integer *b* and a primitive root *a* of prime number *p*, we can find a unique exponent *i* such that $b \equiv a^i \pmod p$ where *0 ≤ i ≤ (p-1)*
  - This exponent *i* is referred to as the discrete logarithm of the number *b* for the base *a (mod p)*. We denote this value as $\text{dlog}_{a,p}(b)$

Cont'd

- Again, for any integer *b* and a primitive root *a* of prime number *p*, we can find a unique exponent *i* such that $b \equiv a^i \pmod p$ where $0 \leq i \leq (p-1)$
- The exponent *i* is referred to as the discrete logarithm of the number *b* for the base *a (mod p)*. We denote this value as $\text{dlog}_{a,p}(b)$
- Some properties
  - $\text{dlog}_{a,p}(1) = 0$ because $a^0 \bmod p = 1 \bmod p = 1$
  - $\text{dlog}_{a,p}(a) = 1$ because $a^1 \bmod p = a$

Example

- A nonprime modulus, $n = 9$. Here $\Phi(n) = 6$ and $a = 2$ is a primitive root. We compute the various powers of a and find

$2^0 = 1$	$2^4 \equiv 7 \pmod 9$
$2^1 = 2$	$2^5 \equiv 5 \pmod 9$
$2^2 = 4$	$2^6 \equiv 1 \pmod 9$
$2^3 = 8$	

$b \equiv a^i \pmod p$

-> $i = dlog_{a,p}(b)$

Logarithm	0	1	2	3	4	5
Number	1	2	4	8	7	5

-> b

Rearrange the table:

Number	1	2	4	5	7	8
Logarithm	0	1	2	5	4	3

For Modular Multiplication

Consider

$$x = a^{\text{dlog}_{a,p}(x)} \bmod p$$
$$y = a^{\text{dlog}_{a,p}(y)} \bmod p$$
$$xy = a^{\text{dlog}_{a,p}(xy)} \bmod p$$

Using the rules of modular multiplication

$$xy \bmod p = [(x \bmod p)(y \bmod p)] \bmod p$$

$$a^{\text{dlog}_{a,p}(xy)} \bmod p = \left[\left(a^{\text{dlog}_{a,p}(x)} \bmod p \right) \left(a^{\text{dlog}_{a,p}(y)} \bmod p \right) \right] \bmod p$$
$$= \left(a^{\text{dlog}_{a,p}(x) + \text{dlog}_{a,p}(y)} \right) \bmod p$$

For Euler's theorem

Euler's theorem states that, for every *a* and *n* that are relatively prime

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

Any positive integer *z* can be expressed in the form $z = q + k\Phi(n)$, with $0 \leq q \leq \Phi(n)$. Therefore

$$a^z \equiv a^q \pmod{n} \qquad \text{if } z \equiv q \bmod \phi(n)$$

Applying this to the foregoing equality,

$$\text{dlog}_{a,p}(xy) \equiv [\text{dlog}_{a,p}(x) + \text{dlog}_{a,p}(y)] (\text{mod} \phi(p))$$

$$\text{dlog}_{a,p}(y^r) \equiv [r \times \text{dlog}_{a,p}(y)] (\text{mod } \phi(p))$$

- Unique discrete logarithms mod *m* to some base *a* exist only if *a* is a primitive root of *m*.

Recall

- All the powers of *a*, modulo 19 for all positive *a* < *19.* *Ex.* $7^3 \equiv 1 \pmod{19}$
- Length for each base value: indicated by shading

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

Discrete Logarithms, Modulo 19

Table 8.4 Tables of Discrete Logarithms, Modulo 19

(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

Calculation of Discrete Logarithms

- Consider the equation

$$y = g^x \bmod p$$

  - Given g, x, and p, it is a straightforward matter to calculate y

- However, given y, g, and p, it is, in general, very difficult to calculate x (take the discrete logarithm)
- The difficulty seems to be on the same order of magnitude as that of factoring primes required for RSA