Number Theory

CSS322: Security and Cryptography

Sirindhorn International Institute of Technology
Thammasat University

Prepared by Steven Gordon on 16 February 2015

css322y13s2l06, Steve/Courses/2013/s2/css322/lectures/number.tex, r3574

Contents

Divisibility

- b divides a if $a = mb$ for some m, where a, b and m are integers
  - $b|a$
  - b is a divisor of a
- $\gcd(a, b)$: greatest common divisor of a and b
  - Euclidean algorithm can find gcd
- Two integers, a and b, are relatively prime if $\gcd(a, b) = 1$

Prime Numbers

- An integer $p > 1$ is a prime number if and only if its only divisors are ± 1 and $\pm p$
- Any integer $a > 1$ can be factored as:

$$a = p_2^{a_1} \times p_2^{a_2} \times \cdots \times p_t^{a_t}$$

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

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	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																			

Contents

Modular Arithmetic

- If a is an integer and n is a positive integer, we define $a \bmod n$ to be the remainder when a is divided by n
- n is called the modulus
- Two integers a and b are congruent modulo n if $(a \bmod n) = (b \bmod n)$, which is written as

$$a \equiv b \pmod{n}$$

- $\pmod{n}$ operator maps all integers into the set of integers $Z_n = \{0, 1, \ldots, (n-1)\}$
- Modular arithmetic performs arithmetic operations within confines of set Z_n

Properties of Modular Arithmetic

- Rules of ordinary arithmetic involving addition, subtraction, and multiplication also apply in modular arithmetic

$$[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$$

$$[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$$

$$[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$$

Property	**Expression**
Commutative Laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative Laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive Law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive Inverse $(-w)$	For each $w \in Z_n$, there exists a z such that $w + z \equiv 0 \bmod n$

Division in Modular Arithmetic

- a is additive inverse of b if $a + b \equiv 0 \pmod{n}$
  - All integers have an additive inverse
- a is multiplicative inverse of b if $a \times b \equiv 1 \pmod{n}$
  - Not all integers have a multiplicative inverse
  - a has a multiplicative inverse in $\pmod{n}$ if a is relatively prime to n
- Division: $a \div b \equiv a \times MultInverse(b) \pmod{n}$

Fermat's Theorem

- Fermat's Theorem (1): if p is prime and a is a positive integer not divisible by p, then

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

- Fermat's Theorem (2): if p is prime and a is a positive integer, then

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

Euler's Theorem

- Euler's Totient Function, $\phi(n)$: the number of positive integers less than n and relatively prime to n
  - $\phi(1) = 1$
  - For prime p, $\phi(p) = p - 1$
  - For a relatively prime to b, and $n = ab$, $\phi(n) = \phi(a) \times \phi(b)$
  - For different primes p and q, and $n = pq$, $\phi(n) = (p-1) \times (q-1)$
- Euler's Theorem (1): For every a and n that are relatively prime:

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

- Euler's Theorem (2): For positive integers a and n:

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

Logarithms in Modular Arithmetic

- Exponentiation $\pmod{n}$: repeated multiplication
- Logarithms in ordinary arithmetic:

$$b = a^i$$

$$i = \log_a(b)$$

- Logarithms in modular arithmetic (discrete logarithm):

$$b = a^i \pmod{p}$$

$$i = \mathrm{dlog}_{a,p}(b)$$

- A unique exponent i can be found if a is a primitive root of prime p
  - If a is a primitive root of p then $a, a^2, a^3, \ldots, a^{p-1}$ are distinct $(\bmod\, p)$
  - Only integers with primitive roots: 2, 4, p^α, $2p^\alpha$ where p is any odd prime and *alpha* is positive integer

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

Credit: Table 8.3 in Stallings, *Cryptography and Network Security*, 5th Ed., Pearson 2011

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

Credit: Table 8.4 in Stallings, *Cryptography and Network Security*, 5th Ed., Pearson 2011

Complexity

Certain problems are computationally hard . . .

Integer Factorisation

- If p and q are unknown primes, given $n = pq$, find p and q
- Largest RSA number factored into two primes is 768 bits (232 decimal digits)

Euler's Totient

- Given composite n, find $\phi(n)$
- Harder than integer factorisation

Discrete Logarithms

- Given b, a and p, find i such that $i = \mathrm{dlog}_{a,p}(b)$
- Comparable to integer factorisation