Introduction to Number Theory

CSS 322 – Security and Cryptography

Modular Arithmetic

- Use non-negative integers less than n
  - Perform normal addition/multiplication
  - Replace answer with its remainder when divided by n
- Result is called: “modulo n” or “mod n”
- Example (mod 10):
  - Addition: $5 + 5 = 0$ $\quad 3 + 9 = 2$ $\quad 2 + 2 = 4$
  - Multiply: $5 \times 5 = 5$ $\quad 3 \times 9 = 7$ $\quad 2 \times 2 = 4$
  - Exponent: $5^5 = 5$ $\quad 3^9 = 3$ $\quad 2^2 = 4$
  - Subtraction: add –x; -x is additive inverse of x
  - Division: multiplicative inverse
    - There is only an inverse for some values – found by Euclids algorithm
    - All multiplicative inverse are relatively prime to modulo (e.g. 10)
  - Inverse exponentiation
    - There is only an inverse for some values

Modular Addition (mod 10)

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

Modular Multiplication (mod 10)

×	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Modular Exponentiation (mod 10)

x^y	0	1	2	3	4	5	6	7	8	9	10	11	12
0		0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	6	2	4	8	6	2	4	8	6
3	1	3	9	7	1	3	9	7	1	3	9	7	1
4	1	4	6	4	6	4	6	4	6	4	6	4	6
5	1	5	5	5	5	5	5	5	5	5	5	5	5
6	1	6	6	6	6	6	6	6	6	6	6	6	6
7	1	7	7	3	1	7	9	3	1	7	9	3	1
8	1	8	8	2	6	8	4	2	6	8	4	2	6
9	1	9	9	9	1	9	1	9	1	9	1	9	1

Number Theory

- Prime Numbers
  - A positive integer is a prime number if and only if it is evenly divisible by exactly two positive integers (itself and 1)
  - Any integer can be factored only by primes
  - Two numbers are relatively prime if they have no prime factors in common
    - Or their greatest common divisor is 1
- Fermat's Theorem
  - If p is prime and a is a positive integer not divisible by p, then

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

  - Or alternatively: if p is prime and a is a positive integer then

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

Some Prime Numbers

2	101	211	307	401	503	601	701	809	0	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																			

Number Theory

- Relatively Prime
  - Two numbers that don't share any common factors
    - 7 is relatively prime to 10 – both have common divisor of 1
    - 9 is relatively prime to 10 – both have common divisor of 1
    - 6 is NOT relatively prime to 10 – both have common divisor of 2 and 1
- Euler's Totient Function: $\phi(n)$
  - Number of integers less than *n* and relatively prime to *n*
  - For a prime, *p*, $\phi(p) = p - 1$
  - For two primes, *p* and *q*, $\phi(p \times q) = \phi(p) \times \phi(q)$
- Euler's Theorem:
  - For every *a* and *n* that are relatively prime: $a^{\phi(n)} \equiv 1 (\bmod n)$
  - Alternatively, $a^{\phi(n)+1} \equiv a (\bmod n)$

Euler's Totient Function Values

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

Testing for Primality

- Many cryptographic algorithms need very large prime numbers
- How do we find very large prime numbers?
  - There is no simple, efficient algorithm known
- Miller-Rabin Algorithm
  - Does not give definite result
    - Returns “composite” or “inconclusive”
  - Running the test many times can increase confidence that number is prime
  - Efficient algorithm
    - There are some deterministic algorithms, but not as efficient