Fundamentals of Information & Network Security
ECE 471/571

Lecture #3: Modular Arithmetic and Cryptography

Instructor: Ming Li
Dept of Electrical and Computer Engineering
University of Arizona

Basic Modular Arithmetic

- Divisibility
  - A nonzero b divides a, if a=mb for some m (all are integers)
  - If b|a, then b is a divisor of a

The positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24
13 | 182; - 5 | 30; 17 | 289; - 3 | 33; 17 | 0

- Properties of divisibility
  - If $a \mid b$ and $b \mid c$, then $a \mid c$
  - If $b \mid g$ and $b \mid h$, then $b \mid (mg + nh)$ for arbitrary integers m and n

11 | 66 and 66 | 198 = 11 | 198

- Division algorithm
  - Given any positive integer n, integer a,

    $a = qn+r$, $0\le r<n$, $q=\text{floor}(a/n)$ ---- q: quotient; r: residue

Basic Modular Arithmetic

- Modulus
  - a mod n: the remainder when a is divided by n
  - n is a positive integer and is called the modulus

11 mod 7 = 4; - 11 mod 7 = 3

- Congruence
  - Integers a and b are congruent modulo n, if (a mod n)=(b mod n)
  - Written as $a \equiv b \pmod{n}$

$73 \equiv 4 \pmod{23}$; $21 \equiv -9 \pmod{10}$

- Properties
  - $a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b)$
  - $a \equiv b \pmod{n} \Leftrightarrow b \equiv a \pmod{n}$
  - $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \rightarrow a \equiv c \pmod{n}$

23 = 8 (mod 5) because 23 - 8 = 15 = 5 * 3
- 11 = 5 (mod 8) because - 11 - 5 = - 16 = 8 * (- 2)
81 = 0 (mod 27) because 81 - 0 = 81 = 27 * 3

Basic Modular Arithmetic

- Modular Addition and Multiplication
  - Arithmetic operations within the set $Z_n=\{0,1,\dots,(n-1)\}$
  - Examples: (5+7) mod 10 =? (5*7) mod 10 = ?

- Properties:
  - (a + b) mod n = [(a mod n) + (b mod n)] mod n
  - (a - b) mod n = [(a mod n) - (b mod n)] mod n
  - (a * b) mod n = [(a mod n) * (b mod n)] mod n

- More examples
  - (978 + 1047) mod 10 =?
  - (111 * 112) mod 10 =?

- Modular Exponentiation
  - Can be done by repeated multiplication
  - 11^7 mod 13 =?

Properties of Modular Arithmetic for Integers in Z_n

- Arithmetic Modulo 8

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

Properties of Modular Arithmetic for Integers in Z_n

- Multiplication Modulo 8

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

Additive and Multiplicative Inverse

- Additive and Multiplicative Identities
  - 0 : 0+w=w mod n;
  - 1 : 1*w = w mod n;

- Additive and Multiplicative Inverses
  - Each w within Z_n has an additive inverse
  - An integer has a mult. Inverse in Z_n if and only if it is relatively prime to n.

Q: Will there be more than one multiplicative inverse for a given number?

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

E.g.: Inverses Modulo 8

Properties of Modular Arithmetic for Integers in Z_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 $w + z \equiv 0 \bmod n$

(This table can be found on page 38 in the textbook)

Euclidean Algorithm

- One of the basic techniques of number theory
- Procedure for determining the greatest common divisor of two positive integers
- Two integers are **relatively prime** if their only common positive integer factor is 1

Greatest Common Divisor (GCD)

- The **greatest common divisor** of a and b is the largest integer that divides both a and b ---- gcd(a,b)

- Positive integer c is said to be the gcd of a and b if:
  - c is a divisor of a and b
  - Any divisor of a and b is a divisor of c

- An equivalent definition is:

$$\gcd(a,b) = \max[k, \text{ such that } k \mid a \text{ and } k \mid b]$$

GCD

- Because we require that the greatest common divisor be positive, gcd(a,b) = gcd($a,-b$) = gcd($-a,b$) = gcd($-a,-b$)
- In general, gcd(a,b) = gcd($|a|, |b|$)

gcd(60, 24) = gcd(60, - 24) = 12

- Also, because all nonzero integers divide 0, we have gcd(a,0) = | a |

- It is equivalent to saying that a and b are relatively prime if gcd(a,b) = 1

8 and 15 are relatively prime because the positive divisors of 8 are 1, 2, 4, and 8, and the positive divisors of 15 are 1, 3, 5, and 15. So 1 is the only integer on both lists.

Euclidean Algorithm

If a>=b>=0, then gcd(a,b) = gcd(b, a mod b)

Examples: gcd(55,22)
gcd(18.12)
gcd(11,10)

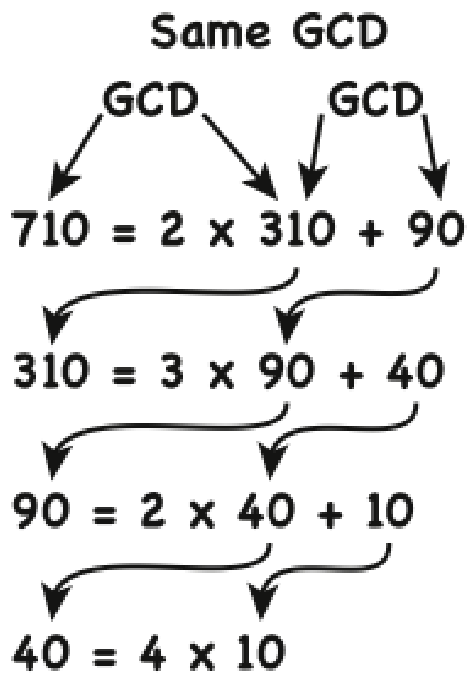

Figure 2.3 Euclidean Algorithm Example: gcd(710, 310)

Extended Euclidean Algorithm (EEA)

Given integers a and b, EEA calculates integers x and y, such that:

$$ax + by = d = \gcd(a,b)$$

We have:

$$a=q_1*b+r_1; \quad r_1=a*x_1+ b*y_1;$$
$$b=q_2*r_1+r_2; \quad r_2=a*x_2+b*y_2;$$
$$\vdots$$
$$r_{n-2}=q_n*r_{n-1}+r_n; \quad r_n=a*x_n+b*y_n;$$

Where,

$$x_i = x_{i-2} - q_i*x_{i-1}\ ,\ y_i = y_{i-2} - q_i*y_{i-1}$$

Initial values: $X_{-1}=1; y_{-1}=0$

Examples:
a=42, b=30;
a=75, b=28

Can be used to calculate the multiplicative inverse of b mod a, if a and b are relatively prime

Extended Euclidean Algorithm Example

a=1759,   b=550

i	r_i	q_i	x_i	Y_i
–1	1759		1	0
0	550		0	1
1	109	3	1	–3
2	5	5	–5	16
3	4	21	106	–339
4	1	1	–111	355
5	0	4		

Result: d = 1; x = –111; y = 355

(This table can be found on page 43 in the textbook)

Q: What is b's multiplicative inverse modulo 1759?

Prime Numbers

- Prime numbers only have divisors of 1 and itself
  - They cannot be written as a product of other numbers
- Any integer a > 1 can be factored in a unique way as

$$a = {}_{p1}{}^{a1} * p_2{}^{a2} * \ldots * p_{p1}{}^{a1}$$

  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

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																			

(This table can be found on page 44 in the textbook)

Euler's Totient Function *ø(n)*

- Number of positive integers less than n and relatively prime to n.
- If n=p*q, where p and q are primes, then $ø(n)=(p-1)(q-1)$

n	$\phi(n)$	n	$\phi(n)$	n	$\phi(n)$
1	1	11	10	21	12
2	1	12	4	22	10
3	2	13	12	23	22
4	2	14	6	24	8
5	4	15	8	25	20
6	2	16	8	26	12
7	6	17	16	27	18
8	4	18	6	28	12
9	6	19	18	29	28
10	4	20	8	30	8

(This table can be found on page 48 in the textbook)

Reading Assignment for Next Class

- [W. Stallings] Chapter 2.4-2.5, and Chapter 3 (3.1 – 3.2).