Week 9-2: Number Theory

Contents

- Prime and Relative Prime Numbers
- Modular Arithmetic
- Fermat's and Euler's Theorem
- Extended Euclid's Algorithm

Divisors

- *$b|a$ ("b divides a", "b is a divisor of a")*
  if $a = kb$ for some k,
  where a, b, and k are integers, and
  $b \neq 0$
  - *If $a|1$, then $a = \pm 1$*
  - *If $a|b$ and $b|a$, then $a = \pm b$*
  - *Any $b \neq 0$ divides 0*
  - *If $b|g$ and $b|h$, then $b|(mg + nh)$ for arbitrary integers m and n*

Prime Numbers

- *An integer $p > 1$ is a prime number if its only divisors are ± 1 and $\pm p$*
- *Prime Factorization*
  - *Any integer $a>1$ can be factored in a unique way as*
    $a = p_1^{\alpha 1} p_2^{\alpha 2} \dots p_t^{\alpha t}$ *where $p_1 < p_2 < \dots < p_t$ are prime numbers and where each $\alpha_i > 0$*
  - *If P denotes the set of all prime numbers, then any positive integer can be written uniquely in the following form*

$$a = \prod_{p} p^{a_p} \text{ where each } a_p \geq 0$$

  - *Multiplication of two numbers is equivalent to adding two corresponding exponents:*
    - $k = mn \rightarrow k_p = m_p + n_p$ *for all p*
  - $a|b \rightarrow a_p \leq b_p$ *for all p*

Primes less than 2000, How many ?

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																			

(Note) The # of prime numbers less than *x* is about *x*/ln(*x*).

Relatively Prime Numbers

- *Greatest Common Divisor*
  - *c = gcd(a, b) if c|a and c|b and ∀d that divides a and b: d|c*
  - *Equivalently, gcd(a, b) = max{c: c|a and c|b}*
- $k = gcd(a, b) \rightarrow k_p = min(a_p, b_p)$ *for all p*

- *a and b are relatively prime if gcd(a, b) = 1*

Modular Arithmetic

- *For any integer a and positive integer n, if a is divided by n, the following relationship holds:*
  - $a = qn + r \quad 0 \le r \le n; \quad q = \lfloor a/n \rfloor$ *(q: quotient, r: remainder or residue)*
- *If a is an integer and n is a positive integer, a mod n is defined to be the remainder when a is divided by n*
  - $a = \lfloor a/n \rfloor \times n + (a \bmod n)$
- *Two integers a and b are said to be congruent modulo n if (a mod n) = (b mod n), and this is written* $a \equiv b \bmod n$
- *Properties of modulo operator*
  - $a \equiv b \bmod n$ *if* $n | (a - b)$
  - $(a \bmod n) = (b \bmod n)$ *implies* $a \equiv b \bmod n$
  - $a \equiv b \bmod n$ *implies* $b \equiv a \bmod n$
  - $a \equiv b \bmod n$ *and* $b \equiv c \bmod n$ *implies* $a \equiv c \bmod n$

Groups, Rings, Fields

- *Group*
  - *A set of numbers with some addition operation whose result is also in the set (closure).*
  - *Obeys associative law, has an identity, has inverses.*
  - *If group is commutative, we say Abelian group. Otherwise Non-Abelian group*
- *Ring*
  - *Abelian group with a multiplication operation.*
  - *Multiplication is associative and distributive over addition.*
  - *If multiplication is commutative, we say a commutative ring.*
  - *e.g., integers mod N for any N.*
- *Field*
  - *An Abelian group for addition.*
  - *A ring.*
  - *An Abelian group for multiplication (ignoring 0).*
  - *e.g., integers mod P where P is prime.*

Modular Arithmetic Operations

- *Modulo arithmetic operation over Z_n = {0, 1, …, n-1}*
- *Properties*
  - *[(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 = (a × b) mod n*

Table 7.2 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

(a) Addition 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

(b) Multiplication modulo 8

Properties of Modular Arithmetic

- Modulo arithmetic over $Z_n = \{0, 1, \ldots, n-1\}$ (called a set of residues of modulo n)
- Integers modulo n with addition and multiplication form a commutative ring
  - *Commutative laws* $(a + b) \bmod n = (b + a) \bmod n$
    $(a \times b) \bmod n = (b \times a) \bmod n$
  - *Associative laws* $[(a + b) + c] \bmod n = [a + (b + c)] \bmod n$
    $[(a \times b) \times c] \bmod n = [a \times (b \times c)] \bmod n$
  - *Distributive laws* $[a \times (b + c)] \bmod n = [(a \times b) + (a \times c)] \bmod n$
  - *Identities* $(a + 0) \bmod n = a \bmod n$
    $(a \times 1) \bmod n = a \bmod n$
  - *Additive inverse (-a)* $\forall a \in Z_n\ \exists b$ s.t. $a + b \equiv 0 \bmod n$
  - *Multiplicative inverse (a^{-1})* $\forall a\ (\neq 0) \in Z_n$, if a is relative prime to n, $\exists b$ s.t. $a \times b \equiv 1 \bmod n$
- ***(Note) If n is not prime, Z_n is a ring, but not a field. Z_p is a field if p is prime.***

Modular 7 Arithmetic

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

(a) Addition modulo 7

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

(b) Multiplication modulo 7

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

(c) Additive and multiplicative inverses modulo 7

Fermat's Little 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:*

      $$a, 2a, 3a, \ldots, (p-1)a$$

      Suppose that ra and sa are the same modulo p, then we have $r \equiv s \bmod p$, 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

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

      or better,

      $a^{p-1}(p-1)! \equiv (p-1)! \bmod p$. Divide both side by $(p-1)!$. qed.

- *Corollary*
  - *If p is prime and a is any positive integer, then*

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

Euler's Totient Function (1/2)

- *Euler's totient function $\phi(n)$ is the number of positive integers less than n (including 1) and relatively prime to n*

  $\phi(p) = p-1$ where p is prime.
- *(Definition) $\phi(1) = 1$*

- *Let p and q be distinct prime numbers, $n = p \times q$, then $\phi(p \times q) = \phi(p)\phi(q) = (p-1)(q-1)$*
  - *Proof*
    - *Consider $Z_n = \{0, 1, \ldots, pq-1\}$*
    - *The residues not relatively prime to n are 0, $\{p, 2p, \ldots, (q-1)p\}$, and $\{q, 2q, \ldots, (p-1)q\}$*
    - *So $\phi(pq) = pq - (1 + (q-1) + (p-1)) = pq - p - q + 1 = (p-1)(q-1)$*

Euler's Totient Function (2/2)

Table 7.4 Some Values of Euler's Totient Function $\phi(n)$

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

Euler's Theorem (1/2)

- *Generalization of Fermat's little 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* $\{x_1, x_2, \ldots, x_{\phi(n)}\}$ *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* $\{x_1, x_2, \ldots, x_{\phi(n)}\}$*. Therefore, two products are congruent:*

    $x_1 x_2 \ldots x_{\phi(n)} \equiv (ax_1)(ax_2) \ldots (ax_{\phi(n)}) \bmod n$

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

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

Euler's Theorem (2/2)

- Corollaries
  - Given two prime numbers, p and q, and integers $n = pq$ and m, with $0 < m < n$,

$$m^{\phi(n)+1} = m^{(p-1)(q-1)+1} \equiv m \bmod n$$

(Demonstrate the validity of the RSA algorithm)

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

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

Euclid's Algorithm: Finding GCD(1/2)

- *Based on the following theorem*
  - *gcd(a, b) = gcd(b, a mod b)*
  - *Proof*
    - *If d = gcd(a, b), then d|a and d|b*
    - *For any positive integer b, a = kb + r ≡ r mod b, a mod b = r*
    - *a mod b = a – kb (for some integer k)*
      - *because d|b, d|kb*
      - *because d|a, d|(a mod b)*

    ∴ *d is a common divisor of b and (a mod b)*
    - *Conversely, if d is a common divisor of b and (a mod b), then d|kb and d|[kb+(a mod b)]*
    - *d|[kb+(a mod b)] = d|a*

    ∴ *Set of common divisors of a and b is equal to the set of common divisors of b and (a mod b)*
    - *ex) gcd(18,12) = gcd(12,6) = gcd(6,0) = 6*

      gcd(11,10) = gcd(10,1) = gcd(1,0) = 1

Euclid's Algorithm: Finding GCD(2/2)

- *Recursive algorithm*

  Function Euclid (a, b) / assume $a \geq b \geq 0$ */*

  if b = 0 then return a

  else return Euclid(b, a mod b)

- *Iterative algorithm*

  Euclid(d, f) / assume $d > f > 0$ */*

  1. *$X \leftarrow d$; $Y \leftarrow f$*
  2. *if $Y=0$ return $X = gcd(d, f)$*
  3. *$R = X \bmod Y$*
  4. *$X \leftarrow Y$*
  5. *$Y \leftarrow R$*
  6. *goto 2*

Extended Euclid's Alg. : Finding Multiplicative Inverse(1/2)

- *If gcd(d, f) =1, d has a multiplicative inverse modulo f*
- *Euclid's algorithm can be extended to find the multiplicative inverse*
  - *In addition to finding gcd(d, f), if the gcd is 1, the algorithm returns multiplicative inverse of d (modulo f)*

Extended Euclid(d, f)

1. $(X_1, X_2, X_3) \leftarrow (1, 0, f)$; $(Y_1, Y_2, Y_3) \leftarrow (0, 1, d)$
2. If $Y_3 = 0$ return $X_3 = gcd(d, f)$; no inverse
3. If $Y_3 = 1$ return $Y_3 = gcd(d, f)$; $Y_2 = d^{-1} \bmod f$
4. $Q = \lfloor X_3 / Y_3 \rfloor$
5. $(T_1, T_2, T_3) \leftarrow (X_1 - QY_1, X_2 - QY_2, X_3 - QY_3)$
6. $(X_1, X_2, X_3) \leftarrow (Y_1, Y_2, Y_3)$
7. $(Y_1, Y_2, Y_3) \leftarrow (T_1, T_2, T_3)$
8. goto 2

Note: Always $f \times Y_1 + d \times Y_2 = Y_3$

Extended Euclid's Alg. : Finding Multiplicative Inverse(2/2)

Table 7.5 Extended-Euclid (550, 1769)

Q	X_1	X_2	X_3	Y_1	Y_2	Y_3
—	1	0	1769	0	1	550
3	0	1	550	1	-3	119
4	1	-3	119	-4	13	74
1	-4	13	74	5	-16	45
1	5	-16	45	-9	29	29
1	-9	29	29	14	-45	16
1	14	-45	16	-23	74	13
1	-23	74	13	37	-119	3
4	37	-119	3	-171	550	1

Note: Extended (d, f) yields $f \times Y_1 + d \times Y_2 = Y_3$
-> 769*(-171) + 550*550=1