Number Theory

Computer Security

February 15, 2023

Number Theory

- Divisibility and Division Algorithm
- Euclidean Algorithm
- Modular Arithmetic
- Groups, Rings and Fields
- Finite Fields of Form $GF(p)$
- Polynomial Arithmetic
- Finite Fields of Form $GF(2^n)$

Divisibility

b divides a $(b|a)$

$$a = m * b \qquad a, b, m \rightarrow \text{integers}$$

Example: $8|40, 5|25$

- If $a|1$, then $a = \pm 1$.
- If $a|b$ and $b|a$, then $a = \pm b$
- Any $b \neq 0$ divides 0.
- if $a|b$ and $b|c$, then $a|c$.
- If $b|g$ and $b|h$, then $b|(mg + nh)$ for arbitrary intereger m, n.

b = 7; g = 14; h = 63; m = 3; n = 2
$7|14$ and $7|63$.
To show $7|(3 * 14 + 2 * 63)$,
we have (3 * 14 + 2 * 63) = 7(3 * 2 + 2 * 9),
and it is obvious that $7|(7(3 * 2 + 2 * 9))$.

The Division Algorithm

Division Algorithm

$$a = qn + r \qquad\qquad 0 \leq rn; \quad q = \lfloor a/n \rfloor$$

$$a = 11; \quad n = 7; \quad 11 = 1 * 7 + 4; \quad r = 4 \quad q = 1$$

$$a = -11; \quad n = 7; \quad -11 = (-2) * 7 + 3; \quad r = 3 \quad q = -2$$

The Euclidean Algorithm

- Finds the **Greatest Common Divisor - GCD** of two integers.
- GCD should be positive

$$\text{gcd(a, b)} = \text{gcd(a, -b)} = \text{gcd(-a, b)} = \text{gcd(-a, -b)}$$
$$\text{gcd(60, 24)} = \text{gcd(60, -24)} = 12$$

- Two integers are **relatively prime** if their only common positive integer factor **(GCD)** is 1. Ex: gcd(8, 15) = 1

$$gcd(x, 1) = 1$$
$$gcd(x, 0) = x$$
$$gcd(a, b) = gcd(b, a \bmod b)$$

Q: Find gcd(324, 266)?

Q: Find gcd(1973, 539)? $\rightarrow$ **Co-prime**

Modular Arithmetic

The Modulus

If a is an integer and n is a positive integer, we define a mod n to be the remainder when a is divided by n. The integer n is called the modulus.

$$a = qn + r \quad 0 \leq r < n; \quad q = \lfloor a/n \rfloor$$
$$a = \lfloor a/n \rfloor * n + (a \bmod n)$$

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

Modular Arithmetic

Congruent Modulo

Two integers a and b are said to be **congruent modulo** n, if (a mod n) = (b mod n). This is written as $a \equiv b \pmod{n}$.

Ex: $73 \equiv 4 \pmod{23}$ if $a \equiv 0 \pmod{n}$, then $n|a$

Congruences have the following properties:

1. $a \equiv b \pmod{n}$ if $n|(a-b)$.
2. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$.
3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$.

Modular Arithmetic Operations

The (mod n) operator maps all integers into the set of integers $\{0, 1, ..., (n-1)\}$

- ((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

What about division?? $\rightarrow$ Modular Inverse (**Extended Euclidean Algorithm**)

The extended Euclidean algorithm not only calculate the greatest common divisor d but also two additional integers x and y that satisfy the following equation. $ax + by = d = gcd(a, b)$

Note: x and y will have opposite signs
Note: Numbers should be coprime to get multiplicative inverse.
Q: Find multiplicative inverse of 24140 mod 40902?

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

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

(c) Additive and multiplicative inverses 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

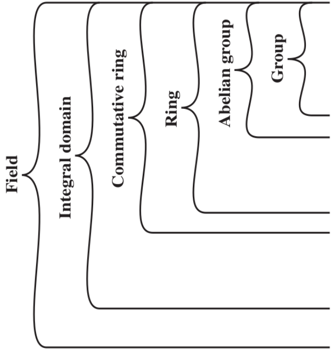
Modular Arithmetic Properties

Define the set Z_n as the set of nonnegative integers less than n: $Z_n = \{0, 1, \ldots, (n - 1)\}$ This is referred to as the set of residues, or residue classes (mod n). To be more precise, each integer in Z_n represents a residue class.

Table 4.3 Properties of Modular Arithmetic for Integers in Z_n

Property	Expression
Commutative Laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x + w) \bmod n$
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 a z such that $w + z \equiv 0 \bmod n$

Group, Ring and Field



(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S; $(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	If a belongs to S and a 0, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Figure 4.2 Groups, Ring, and Field

Set of natural numbers $N \rightarrow$ Not a groups
Set of integers $Z \rightarrow$ Integral Domain
Set of integers modulo a prime?

Finite Galois Fields GF(p)

- Set of integeres $\{0, 1, ..., p-1\}$ with arithmetic operations modulo prime p.
- The binary operations $+$ and $*$ are defined over the set. The operations of addition, subtraction, multiplication, and division can be performed without leaving the set.
- Each element of the set other than 0 has a multiplicative inverse.

+	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

Polynomial Arithmetic

let $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$

1. Ordinary polynomial arithmetic
   $f(x) + g(x) = x^3 + 2x^2 - x + 3$
   $f(x) - g(x) = x^3 + x + 1$
   $f(x) * g(x) = x^5 + 3x^2 - 2x + 2$
2. Poly arithmetic with coefficients mod p (in GF(P))
   Could be modulo any prime, but we are interested in mod 2
   $f(x) + g(x) = x^3 + x + 1$
   $f(x) - g(x) = x^3 + x + 1$
   $f(x) * g(x) = x^5 + x^2$
3. Poly arithmetic with coefficients mod p and polynomials mod m(x)

Polynomial Division & GCD

- Any polynomial can be written in the form:
  $f(x) = q(x)g(x) + r(x)$
- r(x) can be interpretted as being a remainder
  r(x) = f(x) mod g(x)
- If have no remainder say g(x) divides f(x)
- If g(x) has no divisors other than itself & 1 say it is **irreducible** (or prime) polynomial
- Arithmetic modulo an irreducible polynomial forms a field
- Can find greatest common divisor for polys
  $c(x) = GCD(a(x), b(x))$ if c(x) is the poly of greatest degree which divides both a(x), b(x)

Finite Fields of the form $GF(2^n)$

- Polynomials with coefficients modulo 2 whose degree is less than n
- Must reduce modulo an irreducible poly of degree n (for multiplication only)
- Forms a finite field
- Can always find an inverse
- Can extend Euclid's Inverse algorithm to find