SECURITY (COMP0141): MATHEMATICAL BACKGROUND

BASIC MATHEMATICAL NOTATION

Sets: A = {1, 2}, B = {a, b, c}

Cardinality: $|A| = 2$, $|B| = 3$

Set inclusion: $x \in A$ means x belongs to A ($1 \in A$, $3 \notin A$)

Integers: whole numbers (positive or negative)

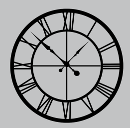
Division: $x \mid y$ means x (evenly) divides y (y = ax for some integer a)

Set conditions: $\{x : 2 \mid x\}$ means all x that are even

Today we're going to see a lot of background mathematics. You may not see today why it's going to be useful but starting next week we'll see it used to construct all sorts of cryptography. Also, you won't be examined on this material explicitly!

MODULAR (“CLOCK”) ARITHMETIC

6 = 6 mod 12
12 = 0 mod 12
14 = 2 mod 12



We technically should use ≡ to denote equivalence but will use = instead

True or false?
14 = 2 mod 12
37 = 26 mod 7
5 = -10 mod 3

14 = 2 mod 12 because 14 = 12 + 2
37 = 2 mod 7 (5*7 + 2), 26 = 5 mod 7 (3*7 + 5)
5 = 2 mod 3 (3 + 2), −10 = 2 mod 3 (−4*3 + 2)

MODULAR ARITHMETIC

Given integers x > 0, y, z we write z ≡ y mod x when $x \mid (z-y)$

More examples: 5 = 1 mod 2, 18 = 3 mod 5

Given x > 0 and z, we can find unique a and $y \in \{0,1,\ldots,x-1\}$ such that

$$z = \underbrace{a}_{\text{quotient}}x + \underbrace{y}_{\text{remainder}}$$

More examples: 5 = 2*2 + 1, 18 = 3*5 + 3

If z = ax + y then z = y mod x (because z - y = ax and $x \mid ax$)

GREATEST COMMON DIVISOR

Greatest common divisor of a and b is the largest number that divides both a and b; i.e., gcd(a, b) = max{d : d | a and d | b}

Bézout's identity: for all a,b there are r,s such that gcd(a,b) = ra + sb

PROOF OF BEZOUT'S IDENTITY

Bézout's identity: for all a,b there are r,s such that gcd(a,b) = ra + sb

Proof:

(1) Define d = min{ra + sb | ra + sb > 0}

(2) Want to show that gcd(a,b) = d, which we can do by showing that (a) gcd(a,b) ≤ d and that (b) d ≤ gcd(a,b)

(2a) Write d = ra + sb. Since gcd(a,b) | a and gcd(a,b) | b we have gcd(a,b) | ra + sb so gcd(a,b) | d

(2b) If d | a and d | b then d ≤ gcd(a,b), so we show this instead. Assume a = kd + t for 0 < t < d (meaning d ∤ a). Then t = a - kd = a - k(ra + sb) = (1 - kr)a - ksb. But this implies that 0 < t = Ra + Sb < d (for R = 1-kr and S = ks) which contradicts the fact that d is minimal

Again, you won't be expected to know this proof and you won't be examined on it – it's just for your own knowledge and interest

EUCLIDEAN ALGORITHM

Euclidean algorithm: used to efficiently compute gcd(a,b) for a > b

-start by finding r_0 such that $a = q_0 b + r_0$ (so r_0 = b mod a)
-then r_1 such that $b = q_1 r_0 + r_1$ (so r_1 = b mod r_0)
-eventually, get to $r_{n-2} = q_n r_{n-1} + 0$
-this final non-zero remainder r_{n-1} is the gcd of a and b

Can read more at https://en.wikipedia.org/wiki/Euclidean_algorithm, and see the demos for an implementation of the algorithm

EUCLIDEAN ALGORITHM

Euclidean algorithm: used to efficiently compute gcd(a,b) for a > b

Example: find gcd(270,192)

-270 = 1*192 + 78

-192 = 2*78 + 36

-78 = 2*36 + 6

-36 = 6*6 + 0

-so gcd(270,192) = 6

EUCLIDEAN ALGORITHM

Why does the algorithm work?

-There are finitely many numbers between a and 0 so it terminates

-Bottom up (r_{n-1} divides a and b):

$r_{n-2} = q_n r_{n-1} + 0 \Rightarrow r_{n-1} = 0 \bmod r_{n-2}$

$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \Rightarrow r_{n-1} = 0 \bmod r_{n-3}$

… $\Rightarrow r_{n-1} = 0$ mod a and 0 mod b (so r_{n-1} is a common divisor)

-Top down (any other divisor divides r_{n-1}):

$a = q_0 b + r_0 \Rightarrow$ c dividing a and b divides r_0

$b = q_1 r_0 + r_1 \Rightarrow$ c divides r_1

… $\Rightarrow$ c divides r_{n-1} (so r_{n-1} is the greatest common divisor)

EXTENDED EUCLIDEAN ALGORITHM

Extended Euclidean algorithm: used to calculate r,s such that gcd(a,b) = ra + sb

In the Euclidean algorithm, focused just on remainders and ignored quotients: equations of the form $r_{i-2} = q_{i-1} r_{i-1} + r_i$, or $r_i = r_{i-2} - q_{i-1} r_{i-1}$

In the extended algorithm, add in two extra variables with the same quotient: $s_i = s_{i-2} - q_{i-1} s_{i-1}$ and $t_i = t_{i-2} - q_{i-1} t_{i-1}$, start with $s_0 = 1$, $s_1 = 0$, $t_0 = 0$, and $t_1 = 1$ (because a = 1*a + 0*b and b = 0*a + 1*b)

Can read more at https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm, and again see the demos for an implementation

EXTENDED EUCLIDEAN ALGORITHM

Example: find s and t such that gcd(18,13) = s*18 + t*13

18 mod 13

-(r) 5 = 18 - 1*13, (s) 1 - 0 = 1, (t) 0 - 1 = -1

13 mod 5

-(r) 3 = 13 - 2*5, (s) 0 - 2*1 = -2, (t) 1 - 2*(-1) = 3

5 mod 3

-(r) 2 = 5 - 1*3, (s) 1 - 1*(-2) = 3, (t) -1 - 1*(3) = -4

3 mod 2

-(r) 1 = 3 - 1*2, (s) -2 - 1*(3) = -5, (t) 3 - 1*(-4) = 7

2 mod 1

-(r) 0 = 2 - 2*1

So 1 = -5*18 + 7*13

MODULAR ARITHMETIC

Many of the usual laws of the integers also apply when computing modulo N

Associativity (both for + and *):

-(a + b mod N) + c mod N

= a + (b + c mod N) mod N

= a + b + c mod N

-(ab mod N)c mod N

= a(bc mod N) mod N

= abc mod N

MODULAR EXPONENTIATION

We often use modular exponentiations g^x mod p ($\underbrace{g*g*...*g}_{\text{x times}}$ mod p)

Again, usual exponentiation rules apply

- $g^x g^y = g^{x+y}$ mod p
- $(g^x)^y = g^{xy}$ mod p

COMMUTATIVE RING Z/NZ

Associative: (a + b) + c = a + (b + c) mod N
(ab)c = a(bc) mod N

Distributive: a(b+c) = ab + ac mod N
(a+b)c = ac + bc mod N

Commutative: a + b = b + a mod N
ab = ba mod N

Additive identity: a + 0 = 0 + a = a mod N

Multiplicative identity: 1a = a1 = a mod N

Additive inverse: a + (-a) + (-a) + a = 0 mod N

Multiplicative inverse?

MULTIPLICATIVE INVERSES

In general, some numbers have inverses but not all

Example: 3 mod 10

- 3 * 7 = 21 = 1 + 20 = 1 + 2*10 = 1 mod 10
- so 3 = 7^{-1} mod 10

Example: 2 mod 10

- there is no number b such that 2b = 1 mod 10

We define (Z/NZ)* to be all invertible elements in Z/NZ

When does a number have an inverse?

MULTIPLICATIVE INVERSES

Element a has multiplicative inverse mod N if and only if gcd(a,N) = 1

Proof:

- if gcd(a,N) = 1 we can write ra + sN = 1 (by Bézout's identity) so ra = 1 mod N, meaning r = a^{-1}
- if a has an inverse r, then ra = 1 mod N, which means ra + sN = 1 for some s, which means gcd(a,N) = 1

The inverse a^{-1} is unique modulo N and can be efficiently computed using the Extended Euclidean algorithm

See the demos for an implementation

EXERCISE

What is Z/12Z?

What is (Z/12Z)*?

For each element in (Z/12Z)*, find its inverse.

ANSWERS

What is Z/12Z? {0,1,2,3,…,11}

What is (Z/12Z)*? {1,5,7,11}

For each element in (Z/12Z)*, find its inverse.

- $1^{-1} = 1$
- $5^{-1} = 5$ ($5*5 = 25 = 2*12 + 1 = 1 \bmod 12$)
- $7^{-1} = 7$ ($7*7 = 49 = 4*12 + 1 = 1 \bmod 12$)
- $11^{-1} = 11$ ($11*11 = 121 = 10*12 + 1 = 1 \bmod 12$)

MULTIPLICATIVE INVERSES

Element a has multiplicative inverse mod N if and only if gcd(a,N) = 1

When could we guarantee this to be the case?

PRIME NUMBERS

A natural number N is prime if its only divisors are 1 and N

Examples: 2, 3, 5, 7, 11, 13, 17, 19, …

If p is a prime and $p \mid ab$ then $p \mid a$ or $p \mid b$

Any natural number N has unique factorisation $N = p_1^{r_1} p_2^{r_2} \dots p_s^{r_s}$

This means $\gcd(a, p) \in \{1, p\}$ when p is prime

Corollary of Bézout's identity: if p is prime then for any $a \in \{1,\dots,p-1\}$ there is an inverse r such that 1 = ra mod p

Primes are amazing and have tons of interest properties

FINITE FIELDS

What is $(Z/pZ)^*$ when p is a prime?

The elements that have $\gcd(x,p) = 1$, but for a prime this is all x not divisible by p, so $F_p^* = \{1,2,3,\ldots,p-1\}$

A field is a commutative ring where all non-zero elements are (multiplicatively) invertible

F_p is a field with p elements (or **order** p) so is called a finite field

PRIME-ORDER FINITE FIELDS

Associative: $(a + b) + c = a + (b + c) \bmod N$
$(ab)c = a(bc) \bmod N$
Distributive: $a(b+c) = ab + ac \bmod N$
$(a+b)c = ac + bc \bmod N$
Commutative: $a + b = b + a \bmod N$
$ab = ba \bmod N$
Additive identity: $a + 0 = 0 + a = a \bmod N$
Multiplicative identity: $1a = a1 = a \bmod N$
Additive inverse: $a + (-a) + (-a) + a = 0 \bmod N$
Multiplicative inverse: $a * a^{-1} = 1 \bmod N$