Lecture #4: Number Theory I

Professor Ankur Moitra (moitra@mit.edu)

Readings: 4.1 & 4.2

Number Theory: many simple-to-state, deep questions

e.g Twin primes: there are infinitely many pairs of primes of the form $(p, p+2)$

Applications to error correction, secure communication

(Play Die Hard 2 clip, pause before soln)

(Ask for a volunteer)

(Play rest of clip)

Bruce & Sam's Solution:

$$(0,0) \to (5,0) \to (2,3) \to (2,0)$$

$$\to (0,2) \to (5,2) \to (4,3)$$

Theme: Sequence of steps of an algorithm give a linear relation

Claim: There are integers s, t so that

$$\underbrace{5s + 3t = 4}$$

(integer) linear combination of 5 & 3

Let's keep track of how we got to 4

$(0,0) \to (5,0) \to (5-3, 3) \to (5-3, 0)$

$\to (0, 5-3) \to (5, 5-3) \to (5-\underbrace{(3-(5-3))}_{\text{gallons moved btwn jugs}}, 3)$

Lemma 1: Given jugs with capacities a and b, the amount of water in each jug is always a linear combination of a and b

Formalize the game

start: $(0,0)$

transition rules: $(x, y) \to (0, y)$ empty first jug

(x: amount in jug with capacity a; y: amount in jug with capacity b)

$(x, y) \to (x, 0)$

$(x, y) \to (0, x+y)$ if $x+y \leq b$

(check: sum to p+e) $\to (x-(b-y), b)$ else

$(x, y) \to (x+y, 0)$ if $x+y \leq a$

$(a, y-(a-x))$ else

Proof: (By induction)

$P(n)$ = In each jug, the amount of water at step n is a linear combination of a & b

Base Case: $0 = 0 \cdot a + 0 \cdot b$ ✓

Inductive Step: Check each transition rule

$(sa + tb, s'a + t'b) \to (sa + tb, 0)$ ✓

$(sa + tb, s'a + t'b) \to (0, (s+s')a + (t+t')b)$ ✓

$\to (sa + tb - (b - (s'a + t'b)), b)$

$(s+s')a + (t+t'-1)b$ ✓

other steps are analogous. ∎

(Ask for volunteer to play another game)

Die Hard 9: Jugs of size 6 and 9, can we fill one with exactly 5?

Is there a solution?

Lemma 2: There is no solution to the second water jug problem

Proof: (Proof by contradiction) Suppose there is a solution. Then by Lemma 1:

$$6s + 9t = 5$$

but 3 divides the left hand side and not the right, which is a contradiction. ☒

This takes us to the notion of divisibility

def: $a \mid b$ (read "a divides b".) iff

$b = ka$ for some integer k

(Handout with basic facts abt divisibility)

Theorem (Division Algorithm): For integers n, d with $d > 0$, there is a unique pair of integers q, r so that

$$n = q \cdot d + r \quad \text{and} \quad 0 \leq r < d$$

q = "quotient", r = "remainder"

(we say $r = \text{rem}(n, d)$)

This is from elementary school

def: the greatest common divisor (gcd) of a and b is the largest integer that divides both a and b.

e.g. $\gcd(6, 9) = 3$ $\xRightarrow{\text{lemma 7}}$ can only get multiples of 3 in second jug game

The gcd will play a key role throughout the unit

Question: How can we find the gcd of large numbers a and b?

make progress by decreasing values

This takes us to the Euclidean Algorithm, sometimes called the first algorithm (c. 300 BC)

Lemma 3: If $b \geq a$, $\gcd(a,b) = \gcd(a, b-a)$

Proof: Suppose $k \mid a$ and $k \mid b$, then $k \mid b-a$ (on sheet)

$\gcd(a,b) \leq \gcd(a,b-a)$

Also if $k \mid a$ and $k \mid b-a$ then $k \mid b$ (same reason)

$\gcd(a,b-a) \leq \gcd(a,b)$

Thus $\gcd(a,b) = \gcd(a,b-a)$ ∎

Lemma 4: If $b \geq a$, $\gcd(a,b) = \gcd(a, \text{rem}(b,a))$

Proof: By the Division algorithm,

$$b = qa + r$$

$r = \text{rem}(b,a)$

then by Lemma 3 we have

$$\gcd(a,b) = \gcd(a, b-a) = \gcd(a, b-2a) \cdots$$

$$= \gcd(a, \underbrace{b-qa}_{r}) \quad ∎$$

Euclidean Algorithm by example (example with 7?)

$$\gcd(46,360) = \gcd(46,38)$$

$$= \gcd(8,38)$$

$$= \gcd(8,6)$$

$$= \gcd(2,6)$$

$$= \gcd(2,0) = 2$$

Again, if we keep track of how we got to each state, we get a linear combination

$(46, 360) \to (46, 360 - 7 \cdot 46)$

$\to (46 - (360 - 7 \cdot 46), 360 - 7 \cdot 46)$

$8 \cdot 46 - 360$

$\to (8 \cdot 46 - 360, 360 - 7 \cdot 46 - 4(8 \cdot 46 - 360))$

$\vdots$

$\to 46s + 360t = 2$

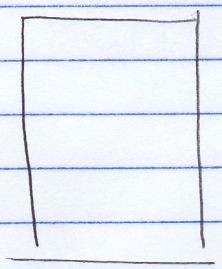
This is called the Extended Euclidean Algorithm

Lemma 5: Given a and b, there are integers s and t so that

$$sa + tb = \gcd(a,b)$$

In fact the gcd is the smallest non-zero linear combination of a and b (see book)

visualization



what is the smallest square you can use to tile? answer: 2x2

Right now, might only sound useful if someone asks you to compute gcd (which we will on tests), but...

and modular arithmetic
the Euclidean Algorithm, underlies much of cryptography.

Let's end with a fun game, foreshadowing things to come:

(Ask for Volunteers)

(Explain Covert Yankee Fan Game)

This is one example of how you can use what's called modular arithmetic to communicate without revealing more than you'd like to