Lecture 8

~~HW 1 Due Tonight~~

Exam 1 Next Thurs Oct 14^{th}

- Can bring 1 double sided cheat sheet
- covers through today, practice posted this weekend, review Tue in class
- topics [sets, logic, functions, bijections, induction, cardinality, simple proofs, divisibility]

Recitation 3 posted on CourseWorks

Last Time

- Ordinary & Strong Induction

Examples, Fund Thm of Arithmetic

Today Fund Thm Arithmetic proof

Euclid's Lemma, Gauss Lemma

Bezout's Identity

Euclidean & Extended Euclidean Algorithm

FTOA

(i) $\forall n \geq 2$, n can be written as $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ p_i prime and $a_i \in \mathbb{N}$; (ii) this is unique up to reordering

$\Rightarrow$ proved (i) by strong induction last class

$\Rightarrow$ Can also prove by contradiction.

Suppose $\exists n$ s.t. n cannot be written as $n = p_1^{a_1} \cdots p_k^{a_k}$ (1)

$\Rightarrow$ There is a smallest such number $M \neq \prod_{i=1}^{k} p_i^{a_i}$ (p_i prime)

$\Rightarrow$ M is composite $\Rightarrow M = x \cdot y$ with $1 < x, y < M$

$\Rightarrow$ Since M is smallest element in $\mathbb{N}$ that does not satisfy (1)

$\Rightarrow x = p_1^{a_1} \cdots p_k^{a_k}$

$y = q_1^{b_1} \cdots q_\ell^{b_\ell}$

$(x, y < M)$

$\Rightarrow$ However $xy = p_1^{a_1} \cdots p_k^{a_k} q_1^{b_1} \cdots q_\ell^{b_\ell}$ which itself is a product of powers of primes $\square$

ii) The factorization $n = p_1^{a_1} \cdots p_k^{a_k}$ is unique up to reordering

Ex: $12 = 2^2 \cdot 3^1 \iff 3^1 \cdot 2^2$ are the same

Lemma (Euclid's Lemma)

If $p | ab$ then $p | a$ or $p | b$ (p prime)

Case 1: Assume $p \nmid a$

$\Rightarrow$ then p and a are coprime

Def $\Rightarrow GCD(p,a) = 1$

Bezouts Identity

If $gcd(\alpha, \beta) = d$, $\exists\, x, y \in \mathbb{Z}$ s.t. $\alpha x \cdot \beta \cdot y = d = gcd(\alpha, \beta)$

$\Rightarrow$ By Bezout's identity

$x \cdot p + y \cdot a = gcd(p,a) = 1$

Multiply by b

$\Rightarrow \quad x \cdot pb + y \cdot ba = b$

if $p | ab \Rightarrow \exists\, K$ s.t. $p \cdot K = a \cdot b$

$\Rightarrow x \cdot bp + y \cdot ab = b$

$x \cdot bp + y \cdot pK = b$

$p(x \cdot b + y \cdot K) = b$

But by definition, $\exists\, r \in \mathbb{Z}$ $(r = x \cdot b + y \cdot K)$ s.t.

$p \cdot r = b \Rightarrow p | b$ $\square$

closer look at Bezout's Identity

If $gcd(\alpha, \beta) = d \Rightarrow \exists x, y \in \mathbb{Z}$ s.t.

$$\alpha \cdot x + \beta \cdot y = d$$

How do we find the x,y coefficients (Bezout Coefficients)?

Euclidean Algorithm

Ex Find gcd(123,45)

To find gcd(123,45), perform long division storing quotients & remainders

writing $a = q_i \cdot b + r_i$

$123 = 2 \cdot 45 + 33$

$45 = 1 \cdot 33 + 12$

$33 = 2 \cdot 12 + 9$

$12 = 1 \cdot 9 + 3$

$9 = 3 \cdot 3 + 0$ $\Rightarrow gcd(123, 45) = 3$

Algorithm gcd(a,b)

```
while b ≠ 0:
    t = b
    b = a mod b
    a = t
return a
```

Def (Modulo). The modulo operator on two integers a, b is defined as (a mod b) the remainder of a divided by b.

Ex 18 Mod 12 = 6

Claim

Last nonzero remainder is the gcd(a,b)

At each iteration, the remainder decreases by at least 1

$\Rightarrow$ Can prove via induction

Euclids Algorithm gives gcd(a,b), can we extend to find coefficients?

Rewrite each eq to solve for remainder

(i) $123 = 2 \cdot 45 + 33 \Rightarrow 33 = 123 - 2 \cdot 45$

(ii) $45 = 1 \cdot 33 + 12 \Rightarrow 12 = 45 - 1 \cdot 33$

(iii) $33 = 2 \cdot 12 + 9 \Rightarrow 9 = 33 - 2 \cdot 12$

(iv) $12 = 1 \cdot 9 + 3 \Rightarrow 3 = 12 - 1 \cdot 9$

(v) $9 = 3 \cdot 3 + 0$

We see by (i) that 33 is expressed as a linear combination of 123 and 45.

Let's substitute until we find 3 as a linear combination of 123, 45

(ii) $12 = \underline{45} - 1 \cdot (\underline{123} - 2 \cdot \underline{45})$

$= \underline{45} - 1 \cdot 123 + 2 \cdot \underline{45}$

$12 = 3 \cdot \underline{45} - 1 \cdot \underline{123}$

(iii) $9 = 33 - 2 \cdot 12$

$= (\underline{123} - 2 \cdot \underline{45}) - 2 \cdot (3 \cdot \underline{45} - 1 \cdot \underline{123})$

$= \underline{123} - 2 \cdot \underline{45} - 6 \cdot \underline{45} + 2 \cdot \underline{123}$

$= 3 \cdot \underline{123} - 8 \cdot \underline{45}$

(iv) $3 = (3 \cdot \underline{45} - 1 \cdot \underline{123}) - 1 \cdot (3 \cdot \underline{123} - 8 \cdot \underline{45})$

$3 = 3 \cdot \underline{45} - 1 \cdot 123 - 3 \cdot \underline{123} + 8 \cdot \underline{45} = 11 \cdot 45 - 4 \cdot 123$

$$3 = 11 \cdot 45 - 4 \cdot 123$$

$$3 = x \cdot 45 + y \cdot 123 \qquad x = 11,\ y = -4$$

Def $ax + by = c$ define a linear diophantine eqn

w, x, y, z are unknowns, other letters given.

$\Rightarrow$ Are there more than 1 solution?

Ex 2

Find all $x, y \in \mathbb{Z}$ s.t. $878x + 252y = \gcd(878, 252)$

$$878 = 3 \cdot 252 + 122 \Rightarrow 122 = 878 - 3 \cdot 252$$

$$252 = 2 \cdot 122 + 8 \Rightarrow 8 = 252 - 2 \cdot 122$$

$$122 = 15 \cdot 8 + 2 \qquad 2 = 122 - 15 \cdot 8$$

$$8 = 4 \cdot 2 + 0$$

$$8 = 252 - 2 \cdot 122 = 252 - 2 \cdot (878 - 3 \cdot 252)$$

$$= 252 - 2 \cdot 878 + 6 \cdot 252$$

$$= 7 \cdot 252 - 2 \cdot 878$$

$$2 = 122 - 15 \cdot 8$$

$$= (878 - 3 \cdot 252) - 15 \cdot (7 \cdot 252 - 2 \cdot 878)$$

$$= 878 - 3 \cdot 252 - 105 \cdot 252 + 30 \cdot 878$$

$$2 = \cancel{878 + 8}\ 31 \cdot 878 - 108 \cdot 252$$

$$x = 31,\ y = -108$$

Claim

$$LCM(a,b) = \frac{ab}{gcd(a,b)}$$

$$LCM(878, 252) = \frac{878 \cdot 252}{2}$$

$$= 878 \cdot \frac{252}{2} = \underline{878} \cdot 126 \quad \text{or} \quad 252 \cdot \frac{878}{2} = \underline{252} \cdot 439$$

$$878(126) + 252(-439) = 0$$

or equivalently $878(126) = 252(439)$

$\Rightarrow$ Multiply by K

$$878(126K) + 252(-439K) = 0 \qquad K \in \mathbb{Z} \quad (i)$$

$$878 \cdot 31 + 252 \cdot (-108) = 2 \qquad (ii)$$

Adding (i) and (ii)

$$878(126K+31) + 252(-439K-108) = 2$$

This is true for all $K \in \mathbb{Z}$

$\Rightarrow$ Infinitely many solutions can be obtained this way

Proof of Bezouts Identity

Given any nonzero $a, b \in \mathbb{Z}^+$, Define

$$S = \{ax+by \mid x, y \in \mathbb{Z} \text{ and } ax+by > 0\}$$

$\Rightarrow$ S is non empty since it contains a or $-a$ with $x = \pm 1$ and $y = 0$

$\Rightarrow$ Since S nonempty set of positive integers, it has a minimum element by the Well-Ordering Principle

$$d = as + bt$$

Def Well-Ordering Principle: Every nonempty set of positive integers contains a least element

$\Rightarrow$ Euclidean ~~Algorithm~~ Division can be written

$$a = d \cdot q + r \qquad 0 \leq r < d$$

$\Rightarrow$ remainder r is in $S \cup \{0\}$ because

$$r = a - qd$$
$$= a - q(\underbrace{as+bt}_{\text{the def of } d}) = a(1-qs) - bqt$$

$\Rightarrow$ r is of the form $ax+by$ hence $r \in S \cup \{0\}$

$\Rightarrow$ However $0 \leq r < d$ and d is smallest positive integer in S

$\Rightarrow$ remainder r cannot be in S, making $r = 0 \Rightarrow$ d is a divisor of a

$\Rightarrow$ d is a divisor of b $\Rightarrow$ d is a common divisor of a and b.

$\Rightarrow$

Now let c be any common divisor of a and b

$\Rightarrow \exists\, u,v$ s.t $a = cu$ and $b = cv$

$\Rightarrow d = as + bt$

$= cus + cvt$

$= c(us + vt)$

$\Rightarrow c$ is a divisor of d and therefore $c \leq d$

$\Rightarrow d$ is greatest common divisor.

$\square$

Can talk about polynomial gcds and extensions of Bezout's identity

irreducible polynomials akin to prime numbers que

Suppose $p_1^{a_1} \cdots p_k^{a_k} = q_1^{b_1} \cdots q_l^{b_l}$

In other words some number can be represented as two products of primes

Need to show

i) $k = l$ (we have same # of primes in factorization)

ii) $p_i = q_i \ \forall i$

Notice $p_i | LHS \Rightarrow p | p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ by lemma 2 and def LHS constructed from p_i's

$\Rightarrow p_i | LHS \ \forall i$ since p_i LHS built from p_i's

$\Rightarrow p_i | RHS$ since LHS = RHS

$\Rightarrow p_i | q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}$

$\Rightarrow p_i | q_r^{b_r}$ for some r

$\Rightarrow p_i | q_r \Rightarrow p_i = q_r$ since p_i, q_r are prime

It follows that $k = l$ and $p_i = q_r$ for some r

Not only do we have the same length of primes, but we have the same primes exhibited

After reordering and renaming $(p_i = q_i) \Rightarrow p_1^{a_1} \cdots p_k^{a_k} = p_1^{b_1} \cdots p_k^{b_k}$

Need to show exponents the same

$\Rightarrow p_1^{a_1} \cdots p_k^{a_k} = p_1^{b_1} \cdots p_k^{b_k}$

Either $a_1 = b_1$, etc $a_i = b_i$ $\forall i$ or are different

in which case done

BWOC

Suppose $a_i \neq b_i$

Assume $a_i > b_i$

Divide by p^{b_i}

$\cancel{p_i^{a_i}}$ $p_i^{b_i}$ divides RHS and LHS

$\Rightarrow p_1^{a_1} \cdots p_{i-1}^{a_{i-1}} \underline{p_i^{a_i - b_i}} p_{i+1}^{a_{i+1}} \cdots p_k^{a_k} = p_1^{b_1} \cdots p_{i-1}^{b_{i-1}} p_{i+1}^{b_{i+1}} \cdots p_k^{b_k}$

products are same except for this spot

$p_i | LHS$ b/c we assumed $a_i > b_i$

$\Rightarrow p_i | RHS \Rightarrow p_i | p_j$ for $i \neq j$

we have two primes but p_i | one of the primes not equal to itself

$\rightarrow$ Contradiction (that $a_i > b_i$)

$\Rightarrow$ Contradict $a_i \neq b_i \Rightarrow a_i = b_i$ $\forall i$