Math 4400
Week 2 – Tuesday
The Euclidean Algorithm

Recall: We want to prove

Theorem (Unique Factorization):
If $n \in \mathbb{N}$, then there is exactly one way to write

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

where $p_1 < p_2 < p_3 < \dots < p_k$ are prime numbers and $a_1, \dots, a_k \in \mathbb{N}$.

2 parts: Existence and Uniqueness.

Existence.

Idea: If n is not prime, $n = ab$ for $a, b > 1$.

If a is not prime ..., etc.

$a = cd \quad c, d > 1 \quad n = cdb$

To argue cleanly, use the:

Well-ordered axiom:

Every non-empty subset S of positive integers has a smallest element.

Proof that prime factorizations <u>exist</u>:

Arguing by contradiction.

Suppose there is an integer $n > 1$ that does not factor as a product of prime numbers.

Let S be the set of integers $n > 1$ not admitting prime factorizations. S is non-empty by our assumption.

So by well-ordered axiom, there is a smallest element $n \in S$. n is not a product of primes, so it's not prime, so $n = ab$ $a, b > 1$.

$a, b < n \implies a, b$ not in S.

So a, b have prime factorizations, but then so does $n = ab$. $\lightning$ ← - - contradiction.

For uniqueness, we need to make a digression!

Definition: If $a, b \in \mathbb{Z}$ (a and b are integers), then we say

- b divides a, or
- b is a divisor of a, or
- $b \mid a$

if there is $q \in \mathbb{Z}$ (an integer q) such that $a = qb$.

Example: $3 \mid 12$ because $12 = 4 \cdot 3$

$5 \nmid 12$ (5 does not divide 12).

Division with remainder:

If $a, b \in \mathbb{Z}$, $b \neq 0$, then there are unique integers q and r such that

① $a = qb + r$

② $0 \leq r < |b|$.

(Note: $b \mid a \iff r = 0$).

(I.e. long division
$b \overline{) a}$
q = qoutient
r = remainder)

Example:

- $a = 12$, $b = 3$ $\quad \underset{a}{12} = \underset{q}{4} \cdot \underset{b}{3} + \underset{r}{0}$
- $a = 12$, $b = 5$ $\quad \underset{a}{12} = \underset{q}{2} \cdot \underset{b}{5} + \underset{r}{2}$.
- $a = 107$, $b = 6$

$$\begin{array}{r|l} & \ 17 \text{ remainder } 5 \\ \hline 6 & 107 \\ - & \ 6 \\ & \ 47 \\ & -42 \\ & \quad 5 \end{array}$$

$$\underset{a}{107} = \underset{q}{17} \cdot \underset{b}{6} + \underset{r}{5}$$

Definition: If a, b are integers, not both zero, $\gcd(a, b)$ is the largest positive integer m such that $m \mid a$ and $m \mid b$.

Example: $\gcd(21, 14) = 7.$

$21 = 7 \cdot 3$ $\qquad$ $14 = 7 \cdot 2$

overlap of prime factorizations is 7.

Remark: It's easy to compute $\gcd(a, b)$ if you know the prime factorization of a and b (just take the overlap in the prime factorization).

But,

! WARNING !

Computationally: this depends on ability to factor number, this is hard!

Theoretically: depends on uniqueness of prime factorization, which we haven't proven yet!

The Euclidean algorithm:
A better way to compute gcd's.

gcd(a,b):

$$a = qb + r$$

Key observation: $\gcd(a,b) = \gcd(b,r)$.

Need to check ① if $d \mid b$ and $d \mid r$ then $d \mid a$

$$a = qb + r = q(dc) + (de) = d(qc+e). \checkmark$$

② if $d \mid a$ and $d \mid b$ then $d \mid r$.

Similar by rewriting $a = qb + r$ as $r = qb - a$. $\checkmark$

Example: $\gcd(60, 22)$ $\left[\begin{array}{l} 60 = 2^2 \cdot 3 \cdot 5 \qquad 22 = 2 \cdot 11 \\ \text{so } \gcd(60,22) = 2. \end{array}\right]$

$$60 = 2 \cdot 22 + 16$$

so by above $\gcd(60, 22) = \gcd(22, 16)$

$$\begin{aligned} 22 &= 1 \cdot 16 + 6 & &= \gcd(16, 6) \\ 16 &= 2 \cdot 6 + 4 & &= \gcd(6, 4) \\ 6 &= 1 \cdot 4 + 2 & &= \gcd(4, 2) \\ 4 &= 2 \cdot 2 + 0 & &\cancel{= \gcd(4,0) = 4.} \end{aligned}$$

$\gcd(2,0) = 2$

Corrected 1/17, 10:20am Thanks John Barrus!

Euclidean algorithm in general:

Computing $\gcd(a,b)$

$$\begin{aligned} a &= q_1 b + r_1 & &\gcd(a,b) \\ & & &\quad \| \\ b &= q_2 r_1 + r_2 & &\gcd(b, r_1) \\ & & &\quad \| \\ r_1 &= q_3 r_2 + r_3 & &\gcd(r_1, r_2) \\ & & &\quad \| \\ & & &\gcd(r_2, r_3) \end{aligned}$$

$$r_m = q_3 r_{m-1} + 0 \qquad \gcd(r_{m-1}, 0) = r_{m-1}$$

gcd(a,b) is the last non-zero remainder!

Example:

- $\gcd(756, 360)$

$$756 = 2 \cdot 360 + \underline{\underline{36}}$$
$$360 = 10 \cdot \underline{\underline{36}} + 0$$

so 36 was last non-zero remainder

so $\gcd(756, 360) = 36$.

- $\gcd(144, 89)$

Fibonacci numbers

$$144 = 1 \cdot 89 + 55$$
$$89 = 1 \cdot 55 + 34$$
$$55 = 1 \cdot 34 + 21$$
$$34 = 1 \cdot 21 + 13$$
$$21 = 1 \cdot 13 + 8$$
$$13 = 1 \cdot 8 + 5$$
$$8 = 1 \cdot 5 + 3$$
$$5 = 1 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

$\vdots$

0

$\gcd(144, 89) = 1$

Needed 10 divisions!

Never need more divisions/step than 5 times the number of digits in b.