Lecture 26, Oct. 28

26.1 Theorem (Properties of GCD)**.** *Let $a, b, c \in \mathbb{Z}$*

1. *if $c \mid a$ and $c \mid b$ then $c \mid gcd(a, b)$*
2. *there exist $x, y \in \mathbb{Z}$ such that $ax + by = c$ iff $gcd(a, b) \mid c$*
3. *there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$ iff $gcd(a, b) = 1$*
4. *if $d = gcd(a, b) \neq 0$ (which is the case unless $a = b = 0$) then $gcd(a/d, b/d) = 1$*
5. *if $a \mid bc$ and $gcd(a, b) = 1$ then $a \mid c$*

Proof. 5. Let $a, b, c \in \mathbb{Z}$. Suppose $a \mid bc$ and $gcd(a, b) = 1$. Since $a \mid bc$, choose $k \in \mathbb{Z}$ such that $bc = ak$. Since $gcd(a, b) = 1$, we can choose $s, t \in \mathbb{Z}$ such that $as + bt = 1$. Then $c = c \cdot 1 = c \cdot (as + bt) = acs + bct = acs + akt = a(cs + kt)$. So $a \mid c$

□

26.2 Definition (Prime)**.** Let $n \in \mathbb{Z}$. We say that n is a **prime** when $n > 1$ and n has no factors $a \in \mathbb{Z}$ with $1 < a < n$.

We say n is composite when $n > 1$ and n does have a factor $a \in \mathbb{Z}$ with $1 < a < n$.

Note. If $n > 1$ and $n = ab$ with $1 < a < n$ then we also have $1 < b < n$.

26.3 Theorem. *Every composite number n has a prime factor p with $p \leq \sqrt{n}$.*

Proof. We claim that every integer $n \geq 2$ has a prime factor.

Let $n \geq 2$. Suppose, inductively, that for every $a \in \mathbb{Z}$ with $2 \leq a < n$, a has a prime factor. If n is prime, then since $n \mid n$, n has a prime factor. Suppose n is not prime, say $n = ab$ with $1 < a < n$ and $1 < b < n$. Since $1 < a < n$ we have $2 \leq a < n$, so a has a prime factor, say $p \mid a$ and p is prime. Since $p \mid a$ and $a \mid n$ then $p \mid n$, so p has a prime factor.

By induction, every integer $n \geq 2$ does have a prime factor.

Let $n \geq 2$ be arbitrary. Suppose n is composite, say $n = ab$ with $1 < a < n$ and $1 < b < n$. Say $a \leq b$ (the case $b \leq a$ is similar). Note that $a \leq \sqrt{n}$ since if $a > \sqrt{n}$ then we have $n = ab \geq aa > \sqrt{n}\sqrt{n} = n$ which is not possible. Since $1 < a < n$, we have $a \geq 2$. So a has a prime factor. Let p be a prime factor of a. Since $p \mid a$ and $a \mid n$ then $p \mid n$. Since $p \mid a$ we have $p \leq a \leq \sqrt{n}$. □

Note. There is a method for listing all prime numbers $p \leq n$, where $n \geq 2$ is a given integer, called the **Sieve of Eratosthenes**.

It works as follows:

We begin by listing all the numbers from 1 to n. We cross off the number 1. We circle the smallest remaining number (namely $p_1 = 2$). Cross off all the other multiples of $p_1 = 2$ (they are composites). Circle the smallest remaining number (namely $p_2 = 3$). Cross off all the other multiples of $p_2 = 3$ (they are composites). Repeat this procedure until we have circled a prime p_l with $p_l \geq \sqrt{n}$ and crossed off the other multiples of p_l.

Note that after we have circled $p_1, p_2, \cdots, p_k$ and crossed off all their multiples, the smallest remaining numbers p_{k+1} must be prime since if it were composite it would have a prime factor $p < p_{k+1}$, but we have already found and crossed off all multiples of all primes p with $p < p_{k+1}$.

Also note that after we have found $p_l \geq \sqrt{n}$ and circled all multiples, all reaming numbers $m \leq n$ are prime since if $m \leq n$ is composite, then m has a prime factor with $p \leq \sqrt{m} \leq \sqrt{n}$, but we have already crossed off all multiples of all such primes.

26.4 Example. Find all primes $p \leq 100$

Solution.

2, 3, 5, 7, ~~9~~, 11, 13, ~~15~~, 17, 19, ~~21~~, 23, ~~25~~, ~~27~~, 29, 31, ~~33~~, ~~35~~, 37, ~~39~~, 41, 43, ~~45~~, 47, ~~49~~

~~51~~, 53, ~~55~~, ~~57~~, 59, 61, ~~63~~, ~~65~~, 67, ~~69~~, 71, 73, ~~75~~, ~~77~~, 79, ~~81~~, 83, ~~85~~, ~~87~~, 89, ~~91~~, ~~93~~, ~~95~~, 97, ~~99~~

26.5 Theorem (The Infinitude of Primes)**.** *There are infinitely many primes.*

Proof. Suppose, for a contradiction, that there are finitely many primes, say $p_1, p_2, \cdots, p_l$, consider the number

$$n = p_1 p_2 \cdots p_l + 1.$$

Since n has a prime factor, we know that one of the primes is a factor of n, say $p_k \mid n$. So $gcd(p_k, n) = p_k$

But

$$\begin{aligned} gcd(p_k, n) &= gcd(n, p_k) \\ &= gcd(p_1 p_2 \cdots p_l + 1, p_k) \\ &= gcd(1, p_k) \\ &= 1 \end{aligned}$$

$\square$