Lecture 29, Nov. 2

29.1 Theorem (Linear Diophantine Equation Theorem)**.** *Let $a, b, c \in \mathbb{Z}$ with $(a, b) \neq (0, 0)$. Let $d = gcd(a, b)$. Consider the equation*

$$ax + by = c.$$

The equation has a solution (x, y) with $x, y \in \mathbb{Z}$ if and only if $d \mid c$. In this case if (u, v) is a solution with $u, v \in \mathbb{Z}$, then the general solution is

$$(x, y) = (u, v) + k(-\frac{b}{d}, \frac{a}{d})$$

Proof. Suppose that the equation has a solution. Choose $x, y \in \mathbb{Z}$ so that $ax + by = c$. Since $d \mid a$ and $d \mid b$, $d \mid ax + by$, so $d \mid c$.

Conversely, Suppose that $d \mid c$, say $c = dl$. Use EA with BS to obtain $s, t \in \mathbb{Z}$ such that

$$as + bt = d$$

. Then

$$asl + btl = dl = c.$$

So we have

$$ax + by = c$$

with $x = sl$ and $y = tl$

Suppose that $d \mid c$ and suppose that $u, v \in \mathbb{Z}$ with $au + bv = c$. We need to show that

1. for all $k \in \mathbb{Z}$, if we let $(x, y) = (u, v) + k(-\frac{b}{d}, \frac{a}{d})$, then $ax + by = c$
2. for all $x, y \in \mathbb{Z}$, if $ax + by = c$, then there exists $k \in \mathbb{Z}$ such that $(x, y) = (u, v) + k(-\frac{b}{d}, \frac{a}{d})$

To prove 1, let $k \in \mathbb{Z}$ and let $(x, y) = (u, v) + k(-\frac{b}{d}, \frac{a}{d})$, that is $x = u - k\frac{b}{d}$ and $y = v + k\frac{a}{d}$. Then

$$\begin{aligned} ax + by =& a(u - k\frac{b}{d}) + b(v + k\frac{a}{d}) \\ =& au + bv - k\frac{ab}{d} + k\frac{ab}{d} \\ =& au + bv \\ =& c \end{aligned}$$

To prove 2, let $x, y \in \mathbb{Z}$. Suppose $ax + by = c$. Since $ax + by = c$ and $au + bv = c$,

$$a(x - u) + b(y - v) = 0$$

so

$$\frac{a}{d}(x - u) = -\frac{b}{d}(y - v)$$

and note that $\frac{a}{d} \in \mathbb{Z}$ and $\frac{b}{d} \in \mathbb{Z}$. It follows that

$$\frac{a}{d} \mid (y - v).$$

Choose $k \in \mathbb{Z}$ so that

$$y - v = k\frac{a}{d}.$$

Since $y - v = k\frac{a}{d}$ and

$$\frac{a}{d}(x-u) = -\frac{b}{d}(y-v)$$

we have

$$\frac{a}{d}(x-u) = -\frac{b}{d}k\frac{a}{d}$$

so

$$x - u = -k\frac{b}{d}.$$

So we have

$$x = u - k\frac{b}{d} \text{ and } y = v + k\frac{a}{d}$$ □

29.2 Theorem (Unique Prime Factorization)**.** *Every integer $n \geq 2$ can be expressed uniquely in the form*

$$n = \prod_{i=1}^{l} p_i = p_1 p_2 \cdots p_l$$

for some $l \in \mathbb{Z}^+$ and some primes $p_1, p_2, \cdots, p_l$ with $p_1 \leq p_2 \leq \cdots \leq p_l$.

Alternatively, every integer $n \geq 2$ can be written uniquely in the form

$$n = \prod_{i=1}^{l} p_i^{k_i}$$

with $l \in \mathbb{Z}^+$ and p_i are distinct primes with $p_1 < p_2 < \cdots < p_l$ and each $k_i \in \mathbb{Z}^+$.

Alternatively, given an integer $n \geq 1$ if every prime factor of n is included in the set $\{p_1, p_2, \cdots, p_l\}$ where the p_i are distinct primes, then n can be written uniquely in the form

$$n = \prod_{i=1}^{l} p_i^{k_i}$$

with each $k_i \in \mathbb{N}$

When

$$n = \prod_{i=1}^{l} p_i^{k_i}$$

where the p_i are distinct primes and each $k_i \in \mathbb{N}$, the positive divisor of n are the integers a of the form

$$a = \prod_{i=1}^{l} p_i^{d_i}$$

such that $0 \leq d \leq k_i$ for all indices i.

29.3 Theorem. *The number of positive divisors of n is*

$$\tau(n) = \prod_{i=1}^{l}(k_i + 1)$$

The sum of the positive divisors of n is

$$\sigma(n) = \prod_{i=1}^{l} \frac{p_i^{n+1} - 1}{p - 1}.$$

29.4 Theorem. *The product of all the positive divisors of n is*

$$p(n) = n^{\tau(n)/2}$$

Proof. exercise □

29.5 Definition. For $n = \prod_{i=1}^{l} p_i^{k_i}$ the exponent of p in n

$$\begin{cases} k_i & \text{if } p = p_i \\ 0 & \text{if } p \notin \{p_1, p_2, \cdots, p_l\} \end{cases}$$