$\mathbb{Z}$: set of integers

$\mathbb{N} = \mathbb{Z}^+ = \{1, 2, 3, \dots\}$ natural numbers

$\mathbb{N}_0 = \mathbb{Z}_{\geq 0} = \{0, 1, 2, 3, \dots\}$

Fundamental Theorem of Arithmetic

$\Rightarrow$ prime numbers are important

Fermat : $x^n + y^n = z^n$, $n \geq 3$

Twin primes : $(p, p+2)$ when both are primes

Are there infinitely many twin primes? (Open)

Goldbach's Conjecture : even numbers are sum of two primes (Open)

Main goal this week: Solving linear diophantine equations.

finding all integer solutions x, y.

a, b, c integer

$ax + by = c$

- $x + y = 0$ $\{(n, -n) : n \in \mathbb{Z}\}$

- $2x - 4y = 0$.

Divide by 2 $\Rightarrow$ $x - 2y = 0$ $\{(2n, n) : n \in \mathbb{Z}\}$

- $3x + 5y = 7$ This one is harder

- $4x + 6y = 3$. No solution because 2 divides $4x + 6y$, but not 3.

Definition: a, b are integers. We say "a divides b" or "b is a multiple of a" if $b = k \cdot a$ for an integer k. We write $a \mid b$ in that case and $a \nmid b$ otherwise

- $a \mid 0$ • $a \mid a$ • $a \mid -a$ • $1 \mid a$ for every a.

Next, we prove some properties

- $a \mid b$ and $b \mid c \Rightarrow a \mid c$

Proof: $a \mid b \Rightarrow b = k \cdot a$, $k \in \mathbb{Z}$

$b \mid c \Rightarrow c = \ell \cdot b$, $\ell \in \mathbb{Z}$

$\Rightarrow c = \ell \cdot b = (\ell \cdot k) \cdot a \Rightarrow a \mid c$.

- $a \mid b$ and $c \mid d \Rightarrow ac \mid bd$

Exercise.

Disprove $a \mid b \Leftrightarrow ma \mid mb$. ($m$ integer)

We need a counter example: $a = 2$, $b = 1$, $m = 0$

- $m \neq 0$. $a \mid b \Leftrightarrow ma \mid mb$

$(\Rightarrow)$: If $a \mid b$, then $b = k \cdot a \Rightarrow mb = k \cdot (ma)$
$\Rightarrow ma \mid mb$.

$(\Leftarrow)$: If $ma \mid mb$, then $mb = k \cdot ma$
$\underset{(m \neq 0)}{\Rightarrow} b = k \cdot a \Rightarrow a \mid b$.

- $x \mid a$ and $x \mid b \Rightarrow x \mid ma + nb$

$x \mid a \Rightarrow a = k \cdot x$

$x \mid b \Rightarrow b = \ell \cdot x$

$\Rightarrow ma + nb = mkx + n\ell x = x(mk + n\ell)$
$\Rightarrow x \mid ma + nb$

Can generalize: $x \mid a$, $x \mid b$, $x \mid c \Rightarrow x \mid \ell a + mb + nc$ etc.

- $a \mid b$ and $b \mid a \Rightarrow a = \pm b$
- $a \mid b \Rightarrow |a| \leq |b|$ unless $b = 0$.

Division Algorithm: $b \neq 0$. There are unique integers k and r such that $a = k \cdot b + r$ and $0 \leq r < |b|$

Proof: Let's just focus on $b > 0$ because $b < 0$ is not very different: $24 = 4 \cdot 5 + 4$ and $24 = (-4) \cdot (-5) + 4$.

Two things to prove: existence, uniqueness

Existence: S = set of all non-negative integers of the form $a - kb$ ($a, a \pm b, a \pm 2b, a \pm 3b, \dots$)

Obviously $S \neq \emptyset$, so it has a smallest element, say $r_0 = a - k_0 \cdot b$ (well-ordering principle)

$a - (k_0 + 1) b$ is smaller than $r_0 \Rightarrow a - (k_0 + 1) b \notin S$

$\Rightarrow a - (k_0 + 1) b < 0 \Rightarrow a < (k_0 + 1) \cdot b$

$\Rightarrow r_0 = a - k_0 b < b$.

Uniqueness: Say $a = k_0 b + r_0$ and $a = k_1 b + r_1$ with $0 \leq r_0, r_1 < b$.

$k_0 b + r_0 = k_1 b + r_1 \Rightarrow r_0 - r_1 = k_1 b - k_0 b$

$\Rightarrow r_0 - r_1 = (k_1 - k_0) \cdot b \Rightarrow b \mid r_0 - r_1$ $\quad -b < r_0 - r_1 < b$

$\Rightarrow r_0 - r_1 = 0$ or $|r_0 - r_1| \geqslant b$ (not possible)

$\Rightarrow r_0 = r_1$

Now $k_0 b + r_0 = k_1 b + r_1$ and $r_0 = r_1$

$\Rightarrow k_0 b = k_1 b \Rightarrow k_0 = k_1$.

We can partition the integers into several classes using Division Algorithms

- $\underset{\text{even}}{2k}$, $\underset{\text{odd}}{2k+1}$
- $3k$, $3k+1$, $3k+2$
- $4k$, $4k+1$, $4k+2$, $4k+3$
- $2k$, $4k+1$, $4k+3$

<u>Question:</u> What are the possible remainders when a square n^2 is divided by 8?

$1^2 \longrightarrow 1$	$5^2 \longrightarrow 1$	$9^2 \longrightarrow 1$
$2^2 \longrightarrow 4$	$6^2 \longrightarrow 4$	$10^2 \longrightarrow 4$
$3^2 \longrightarrow 1$	$7^2 \longrightarrow 1$	$11^2 \longrightarrow 1$
$4^2 \longrightarrow 0$	$8^2 \longrightarrow 0$	$12^2 \longrightarrow 0$

... continue

Pattern: $(4k)^2 \to 0$

$(4k+1)^2 \to 1$

$(4k+2)^2 \to 4$

$(4k+3)^2 \to 1$

Proof: $(4k)^2 = 16k^2 = (2k^2)\cdot 8 + 0$

$(4k+1)^2 = 16k^2 + 8k + 1 = (2k^2 + k)\cdot 8 + 1$

$(4k+2)^2 = 16k^2 + 16k + 4 = (2k^2 + 2k)\cdot 8 + 4$

$(4k+3)^2 = 16k^2 + 24k + 9 = (2k^2 + 3k + 1)\cdot 8 + 1$

G.C.D and L.C.M

c is a common divisor of a and b if $c \mid a$ and $c \mid b$

d is a common multiple of a and b if $a \mid d$ and $b \mid d$.

We define

- gcd(a, b) (or simply (a, b)) as the greatest common divisor of a and b (except $a = b = 0$)
- lcm(a, b) (or simply $[a, b]$) as the smallest (positive) common multiple of a and b ($a \neq 0, b \neq 0$)

- $(10, 12) = 2$ and $[10, 12] = 60$
- $(5, 7) = 1$ and $[5, 7] = 35$.

Can generalize to define (a, b, c), $[a, b, c]$ etc.