0.1 September 19th

Proof. $S \subset \mathbb{Z} \Rightarrow S = m\mathbb{Z}$

Since $S \neq \emptyset$, $\exists a \in S$

Since S is closed under $+, -$, $0 \in S$. We may assume that $S \neq \{0\}$. (if $S = \{0\}$, then $S = 0 \cdot \mathbb{Z}$)

Take any $n \in S$. Then $0 - n = -n \in S$. Thus we may also assume that S has a positive integer.

In all, WLOG[1], we may assume that S has a positive integer.

By WOP, S has a least positive integer m. We want to show that $S = m\mathbb{Z}$.

$A = B \Rightarrow A \subset B$ and $B \subset A$
$A \subset B \Rightarrow$ if $x \in A$ then $x \in B$

1. $m\mathbb{Z} \subset S$
   $m \in S$ and S is closed under $+, -$. So S must have all multiples of m.
2. $S \subset m\mathbb{Z}$
   Take any $a \in S$. By division algorithm, $\exists q, r \in \mathbb{Z}$ such that $a = qm + r$ where $0 \leq r < m$. Since $mq \in S$ and $a \in S$,
   $$r = a - mq \in S$$
   . Thus $r = 0$ by the minimality of m. Hence $a = mq \in m\mathbb{Z}$.
   Remains to show the uniqueness of m. Suppose $m\mathbb{Z} = S = m'\mathbb{Z}$. Then $m = \pm m'$. Since $m, m' > 0$, $m = m'$.

Theorem 1. *Let $d = (a, b)$. Then $d = ax + by$ for some $x, y \in \mathbb{Z}$ and $\{ax + by \mid x, y \in \mathbb{Z}\}$ is the set of all multiples of d. i. e. $a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\}$.*

Proof. We knew that $d = ax + by$ for some $x, y \in \mathbb{Z}$. (by the theorem in the last class)

Define $S := a\mathbb{Z} + b\mathbb{Z}$. Then $a\mathbb{Z} \subset S$ and $b\mathbb{Z} \subset S$. Since S is closed under $+, -$, it follows the previous theorem that
$$\exists m \geq 0 \in \mathbb{Z} \text{ such that } S = m\mathbb{Z}.$$

We want to show that $m = d$. Since $a, b \in S = m\mathbb{Z}$, $m \mid a$, $m \mid b$. If $e \mid a$ and $e \mid b$, then $e \mid m$. ($\because m + as + bt$ for some $s, t \in \mathbb{Z}$)

[1] Without loss of generality

By the definition of GCD, $m = d$.

Remark The GCD of a and b (not both 0) is the least positive integer that is a linear combination of a and b.

Theorem 2 (Euclidean Algorithm). $a, b \in \mathbb{Z}$, $a \neq 0$. *Using the division algorithm,*

$$b = aq_1 + r_1, \text{ where } 0 < r_1 < |a|.$$

If $r_1 = 0$, *terminate process.*

Repeating process,

$$\begin{aligned} a &= r_1 q_2 + r_2 && 0 < r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3 && 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n && 0 < r_n < r_{n-1} \\ r_{n-1} &= r_n q_{n+1} \end{aligned}$$

Then $(a, b) = r_n$.

Proof. Clearly, $r_n > 0$. Note that

$$\begin{gathered} r_n \mid r_{n-1}, r_n \mid r_n \Rightarrow r_n \mid r_{n-2} \\ r_n \mid r_{n-2}, r_n \mid r_{n-1} \Rightarrow r_n \mid r_{n-3} \\ \vdots \\ r_n \mid r_1, r_n \mid r_2 \Rightarrow r_n \mid a \\ r_n \mid a, r_n \mid r_1 \Rightarrow r_n \mid b \end{gathered}$$

Note also that if

$$\begin{gathered} k \mid a, k \mid b \Rightarrow k \mid r_1 \\ k \mid r_1, k \mid a \Rightarrow k \mid r_2 \\ \vdots \\ k \mid r_n, k \mid r_{n-1} \Rightarrow k \mid r_n \end{gathered}$$

Hence we conclude that $r_n = (a, b)$.

Proof (Alternate proof).

$$b = aq + r \Rightarrow (a, b) = (a, r) \qquad r = a(-q) + b, b = aq + r$$

Note that $e \mid a, e \mid b$ iff $e \mid r, e \mid a$. Thus $(a, b) \mid (a, b)$ and $(a, k) \mid (a, b)$.

Hence $(a, b) = (a, r)$, since $(a, b) > 0$ and $(a, k) > 0$. Therefore we can see that

$$(a, b) = (a, r) = (r_1, r_2) = \cdots = (r_{n-1}, r_n).$$

Example

$$\begin{aligned}
(68, 710) &= 2 \\
710 &= 68 \cdot 10 + 30 \\
68 &= 30 \cdot 2 + 8 \\
30 &= 8 \cdot 3 + 6 \\
8 &= 6 \cdot 1 + 2 \\
6 &= 2 \cdot 3
\end{aligned}$$

$$\begin{aligned}
2 &= 8 - 6 \cdot 1 \\
&= 8 - (30 - 8 \cdot 3) \\
&= 8 \cdot 4 + 30 \cdot (-1) \\
&= (68 - 30 \cdot 2) \cdot 4 + 30 \cdot (-1) \\
&= 68 \cdot 4 + 30 \cdot (-1) \\
&= 68 \cdot 4 + (710 - 68 \cdot 10) \cdot (-9) \\
&= 68 \cdot 94 + 710 \cdot (-9)
\end{aligned}$$

Definition 1 (Diophantine Equation). *A **Diophantine equation** is a polynomial equation that allows two or more variables to take integer values only.*

e. g.

$$ax + by = c$$

$$x^n + y^n = z^n$$

$$x^2 - dy^2 = 1$$

Theorem 3. *$a \neq 0$, $b \neq 0$.*

1. *The equation $ax + by = c$ has integer solutions if and only if $(a, b) \mid c$.*
2. *Suppose that $(a, b) \mid c$. Then the general solution of the equation $ax + by = c$ has form the of*

$$\left\{ x_0 + \frac{b}{(a, b)} t, \, y_0 - \frac{a}{(a, b)} t \right\}$$

where $t \in \mathbb{Z}$ and (x_0, y_0) is an arbitrary solution of the equation.

General solution for
$y'' - 4y' + 3y = 0$?
$\Rightarrow c_1 e^x + c_2 e^{3x}$
– 2 bases

0.2 September 24th

Proof. Note that

$$a \mid b, a \mid c \Rightarrow a \mid (bx + cy) \qquad \forall x, y \in \mathbb{Z}$$
$$m \mid ab, (m, a) = 1 \Rightarrow m \mid b \qquad \because (m, a) = 1, \exists s, t \in \mathbb{Z} \qquad as + mt = 1$$

Then $bas + bmt = b$.

Since $m \mid ab$, it follows that $m \mid b$.

1. $(\Rightarrow)$ $(a, b) \mid a$, $(a, b) \mid b \Rightarrow (a, b) \mid (ax + by) = c$
   $(\Leftarrow)$ Let $(a, b) = d$ and $c = c_1 d$. Then $\exists s, t \in \mathbb{Z}$ such that $as + bt = d$. thus

$$\begin{aligned} c = c_1 d &= c_1 (as + bt) \\ &= ac_1 s + bc_1 t \end{aligned}$$

   hence $(c_1 s, c_1 t)$ is a solution.

2. Note that

$$\begin{aligned}
& a\left(x_0+\frac{b}{d}t\right)+b\left(y_0-\frac{a}{d}t\right) \\
=& ax_0+\frac{ab}{d}t+by_0-\frac{ba}{d}t \\
=& ax_0+by_0=c
\end{aligned}$$

Suppose that (x, y) is an arbitrary solution of $ax+by=c$. Since $ax+by=c=ax_0+by_0$, we have

$$a(x-x_0)=b(y_0-y).$$

Let $a=a_1d$, $b=b_1d$, where $d=(a, b)$. Then

$$a_1(x-x_0)=b_1(y_0-y).$$

Since $(a, b)=1$, $b_1 \mid (x-x_0)$. Then $\exists t\in\mathbb{Z}$ such that $x-x_0=b_1t$, and similarily $y_0-y=a_1t$. Hence

$$x=x_0+\frac{b}{(a, b)}t, y=y_0-\frac{a}{(a, b)}t.$$

Example

$$710x+68y=6$$

[2] Recall

$$710\cdot(-9)+68\cdot 94=2$$
$$710\cdot(-9\times 3)+68\cdot(94\times 3)=2\times 3=6$$

Hence

$$\begin{aligned}
x&=-27+\frac{68}{2}t=-27+34t \\
x&=282-\frac{710}{2}t=282-355t
\end{aligned}$$

Definition 2 (Least Common Multiple). *The* ***least common multiple*** *of two nonzero integers a and b, denoted* $[a, b]$ *or* $\operatorname{lcm}(a, b)$ *is the integer l satisfying the followings:*

[2] Maybe an eaxm problem?

1. $l > 0$.
2. $a \mid l$, $b \mid l$.
3. $a \mid c$, $b \mid c \Rightarrow m \mid c$.

Theorem 4. *For $a \neq 0, b \neq 0 \in \mathbb{Z}$, $[a, b]$ uniquely exists. Moreover, $a\mathbb{Z} \cap b\mathbb{Z} = [a, b]\,\mathbb{Z}$.*

Proof. Let $S = a\mathbb{Z} \cap b\mathbb{Z}$. Since $ab \in S$, $S \neq \emptyset$. Clearly, S is closed under $+, -$.

By theorem, $\exists l$ such that $S = l\mathbb{Z}$.

We want to show that $l = [a, b]$. Since $l \in S$, $a \mid l$, $b \mid l$. If $a \mid c$, $b \mid c$, then $c \in S = l\mathbb{Z}$ and $l \mid c$.

Remains to show the uniqueness of l. Suppose l_1 and l_2 are both the LCMs of a and b. Then $l_1 \mid l_2$ and $l_2 \mid l_1$. By (2), (3), $l_1 = l_2$, since $l_1 > 0, l_2 > 0$.

Remark

$$(a, b)\,\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\}$$

Recall

1. $(0, 0) := 0$
2. $(a, 0) := |a|$
3. $[0, 0] := 0$
4. $[a, 0] := 0$

Theorem 5. *For $a > 0, b > 0 \in \mathbb{Z}$,*

$$(a, b)\,[a, b] = ab$$

.

Proof. (Proof left for homework – due September 26th.)

Theorem 6. *Let b be a positive integer with $b > 1$. Then every positive integer n can be expressed in unique form of*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b^1 + a_0$$

where $a_i \in \mathbb{Z}$, $0 \leq a_i \leq b-1$ for $i = 0, 1, \cdots, k$ and $a_k \neq 0$.

$b \Rightarrow$ base.

Proof. We use the division algorithm. (Proof left for homework – due September 26th.)

Definition 3 (Prime Numbers). *A **prime** is an integer p such that*

1. $p > 1$.
2. $a \mid p \Rightarrow a = \pm 1$ *or* $\pm p$.

Remark p is prime.

1. $\forall a \in \mathbb{Z}$, $(a, p) = 1$ or $(a, p) = p$. (iff p is prime)
2. $p \mid ab \Rightarrow p \mid a$ or $p \mid b$. (iff p is prime)

Theorem 7 (Infinitude of Primes). *There exists infinitely many primes.*

Proof (Euclid's).

Lemma 1. *Every positive integer $n \geq 2$ has a prime factor.*

Proof. Consider the set $S = \{m \mid m \text{ is a divisor of } n\}$. Then $S \neq \emptyset$.

By WOP, $\exists$ least positive integer $p \in S$. Note that every divisor of p is also a divisor of n. Thus p is a prime number by the minimality of p.

Suppose there exists finitely many primes

$$p_1, p_2, \cdots, p_k.$$

Let

$$n := p_1 p_2 \times \cdots \times p_k.$$

Then $n > 1$ and $\exists$ prime p such that $p \mid n$ by Lemma.

Thus $p = p_i$ for some $1 \le i \le k$, hence $p \mid p_1 p_2 \times \cdots \times p_k$, thus

$$p \mid (n - p_1 p_2 \times \cdots \times p_k) \Rightarrow p \mid 1.$$

Which is a contradiction to the definition of prime numbers. Thus there exists infinitely many primes.

Theorem 8. *There are arbitrary large gaps between successive primes. i. e. For any positive integer n, there exists at least n consecutive composite positive integers.*

Proof. Consider n consecutive integers

$$(n+1)! + 2,\, (n+1)! + 3,\, \cdots,\, (n+1)! + (n+1)\,.$$

For $2 \le j \le n+1$, it is clear that $j \mid (n+1)!$. Thus $j \mid ((n+1)! + j)$.

Hence $\exists n$ consecutive integers which are all composites.

Definition 4 (Mersenne Primes). *A* ***Mersenne prime*** *is a Mersenne number*[3] *which is also prime.*

e. g. $M_2 = 2^2 - 1 = 3$, $M_3 = 2^3 - 1 = 7$, $M_5 = 2^5 - 1 = 31$, $M_7 = 2^7 - 1 = 127$, $\cdots$ but $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$

[3] $M_n = 2^n - 1$