Theorem.
Let $a, b \in \mathbb{Z}$, not both 0.
Let $d = \gcd(a,b)$. Then:
(1) If $n = as + bt$ for $s, t \in \mathbb{Z}$, then $d \mid n$ (hence $d \leq n$).
(2) d is the least positive integer that can be expressed in the form $as + bt$ ($s, t \in \mathbb{Z}$).

proof of (1).
$n = as + bt$, but $d \mid a$ and $d \mid b$.
So $a = dx$, $b = dy$, $x, y \in \mathbb{Z}$.
So $n = dxs + dyt = d(xs + yt)$.
Thus, $d \mid n$. □

proof of (2).
If $n = as + bt$, then $d \mid n$ so $d \leq n$.
So d is least that can be written this way. □

def. If $\gcd(a,b) = 1$, then a, b called coprime (or relatively prime).
Fact:
So a, b coprime $\Leftrightarrow$ $1 = as + bt$ some $s, t \in \mathbb{Z}$.

Proposition.
$\forall n \in \mathbb{N}$, n and $n+1$ are coprime.
proof.
$1 \cdot (n+1) + (-1) \cdot n = 1$.
"s" "t"
Hence, $\gcd(n, n+1) = 1$. □

Primes

def. Let $n \in \mathbb{N}$.
(i) n is prime if $n \geq 2$ and the only positive divisors of n are 1 and n.
(ii) n is composite if $n \geq 3$ and $\exists\, a, b \in \mathbb{N}$ $a \geq 2$, $b \geq 2$ such that $n = ab$.

Theorem. Prime Divisibility.
(1) If p prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.
(2) If p prime and $p \mid a_1 a_2 \cdots a_n$ then $p \mid a_i$ for some i.
(3) If $n \mid ab$ and n, a are coprime then $n \mid b$.

proof of (3).
We know $ab = nx$ for some $x \in \mathbb{Z}$ and $1 = ns + at$ for some $s, t \in \mathbb{Z}$.
Then $b = b(ns + at) = bns + bat = bns + nxt = n(\underbrace{bs + xt}_{\in \mathbb{Z}})$. So $n \mid b$. □

proof of (1).
p prime, $p \mid ab$. Want to prove $p \mid a$ or $p \mid b$.
Note on logic: $P \vee Q \equiv \neg P \Rightarrow Q \equiv \neg Q \Rightarrow P$. Assume $\neg P$, prove Q.
Assume $p \nmid a$.
Then, $\gcd(p, a) = 1$. (since only 1, p divide p, $p \nmid a$).
So by (3), $p \mid ab$ and p, a coprime so $p \mid b$. □

proof of (2).
$p \mid a_1 \cdots a_n \Rightarrow p \mid a_i$ some i.
By induction on n.
(i) If $n = 1$, then $p \mid a_1 \Rightarrow p \mid a_1$. Clearly true.
(ii) Let $n \geq 1$. Assume statement holds for n.
Then $p \mid a_1 a_2 \cdots a_{n+1}$. So $p \mid a_1 \underbrace{(a_2 \cdots a_{n+1})}_{b}$.

By (1), $p \mid a_1$ or $p \mid a_2 \cdots a_{n+1}$.
If $p \mid a_1$, done.
If $p \mid a_2 \cdots a_n$, then since $a_2 \cdots a_{n+1}$ has n factors, $p \mid a_i$ for some $i = 2, \cdots, n+1$ by inductive assumption.
Hence, $p \mid a_i$ for some i. □

Theorem.
(1) If p_1, p_2 are primes, $p_1 \neq p_2$, and $p_1 \mid a$ and $p_2 \mid a$, then $p_1 p_2 \mid a$.
(2) If $b \mid a$ and $c \mid a$ and b, c are coprime then $bc \mid a$.
proof of (2).
$b \mid a$ so $a = bx$.
$c \mid a$ so $a = cy$.
b, c coprime so $1 = bs + ct$ some $s, t, x, y \in \mathbb{Z}$.
Then,
$a = a(bs + ct) = abs + act$
$= cybs + bxct = bc(ys + xt)$ so $bc \mid a$. □
proof of (1).
p_1, p_2 coprime so by (2), $p_1 p_2 \mid a$. □

Theorem. Fundamental Theorem of Arithmetic.
Let $n \geq 2$, $n \in \mathbb{N}$. Then there exists primes $p_1 < p_2 < p_3 < \cdots < p_m$ and $s_1, s_2, s_3, \cdots, s_m \in \mathbb{N}$ all $s_i \geq 1$ such that
$$n = p_1^{s_1} p_2^{s_2} p_3^{s_3} \cdots p_m^{s_m}.$$
Further, this expression is unique.
proof.
Two things to prove.
(1) Existence of factorization.
By strong induction.
(i) If $n = 2$, then $n = 2^1$ is the factorization.
(ii) Let $n \geq 3$. Assume factorization exists for all $2 \leq m < n$.
Two cases:
Case 1. n prime, $n = p^1$ $(p = n)$ is factorization.
Case 2. n composite. So $\exists\ a \geq 2$, $b \geq 2$ such that $n = ab$.
Then a, b both less than n so inductive assumption applies to a, b. So,
$$n = ab = \underbrace{(q_1^{s_1} q_2^{s_2} \cdots q_m^{s_m})}_{a} \underbrace{(r_1^{t_1} r_2^{t_2} \cdots r_\ell^{t_\ell})}_{b}$$
where q_i, r_j are primes.
If any $q_i = r_j$, combine these to obtain factorization for n.
(2) Factorization is unique. Omit.
□

Problem.
Let $n \in \mathbb{N}$. If $n = a^2$, $n = b^3$ for some $a, b \in \mathbb{N}$ then $n = c^6$ some $c \in \mathbb{N}$.
ex.
$n = 2^{12}3^6 = (2^6 3^3)^2 = (2^4 3^2)^3 = (2^2 3^1)^6$.
proof.
By Fundamental Theorem,
$n = p_1^{s_1} \cdots p_m^{s_m}$
$a = q_1^{t_1} \cdots q_l^{t_l}$
$b = r_1^{u_1} \cdots r_w^{u_w}$
Then,
$n = a^2$ so $p_1^{s_1} \cdots p_m^{s_m} = q_1^{2t_1} \cdots q_l^{2t_l}$.
By uniqueness of factorization,
$p_1 = q_1$, $p_2 = q_2$, $m = l$, $p_m = q_l$ and $s_i = 2t_i$ for $i = 2, \cdots, m$.
Hence $2 | s_i$ all i.
Also $n = b^3$ so $p_1^{s_1} \cdots p_m^{s_m} = r_1^{3u_1} \cdots r_w^{3u_w}$ by uniqueness.
$m = w$ all $p_i = r_i$, $s_i = 3u_i$.
So $3 | s_i$ all $i = 1, \cdots, m$.
Then,
$2 | s_i$, $3 | s_i$ and 2, 3 coprime so $6 | s_i$ (by previous theorem).
So $s_i = 6v_i$ some $v_i \in \mathbb{N}$ all i.
Hence,
$$n = (\underbrace{p_1^{v_1} \cdots p_m^{v_m}}_{c})^6.$$

Theorem.
There are infinitely many primes.
proof.
By contradiction.
Assume only finitely many primes.
Can denote all primes by $p_1, p_2, \cdots, p_n$.
Let $m = p_1 p_2 \cdots p_n$ (product of all primes).
Then $m, m+1$ are (always) coprime.
But by Fundamental Theorem, $m+1$ factorizes into primes so it has a prime divisor which must be p_i for some $i \in \{1, \cdots, n\}$.
But clearly $p_i | m$ so p_i is common divisor of $m, m+1$, contradicts $m, m+1$ coprime.
Hence, infinitely many primes. □

Alison Li

Modular Arithmetic

def. Fix $n \geq 1$, $n \in \mathbb{N}$. Two integers a, b are congruent modulo n if they have the same remainder when divided by n. (i.e. if $a = nq_1 + r_1$, $b = nq_2 + r_2$, $0 \leq r_1, r_2 \leq n$ then $r_1 = r_2$). If so, write $a \equiv b \pmod{n}$.

ex. $11 \equiv -4 \pmod{3}$ since $11 = 3 \cdot 3 + 2$ and $-4 = (-2)(3) + 2$.

Proposition.
$a \equiv b \pmod{n} \Leftrightarrow n \mid a-b$.

proof.
($\Rightarrow$). Assume $a \equiv b \pmod{n}$.
That is, $a = nq_1 + r$, $b = nq_2 + r$ (same r). $0 \leq r < n$.
Then $a - b = (nq_1 + r) - (nq_2 + r) = n(q_1 - q_2)$.
So $n \mid a-b$.
($\Leftarrow$). Assume $n \mid a-b$.
So $a - b = nx$ some $x \in \mathbb{Z}$.
By division algorithm,
$a = nq_1 + r_1$
$b = nq_2 + r_2$
Proof by contradiction. Assume $r_1 \neq r_2$.
Then $nx = a - b = (nq_1 + r_1) - (nq_2 + r_2)$.
$nx - nq_1 + nq_2 = r_1 - r_2$
$n(x - q_1 + q_2) = r_1 - r_2$.
Then $r_1 - r_2 \neq 0$, $n \mid r_1 - r_2$.
Hence $n \leq |r_1 - r_2|$.
But $0 \leq r_1 < n$ and $0 \leq r_2 < n$ so $|r_1 - r_2| < n$.
Contradiction, so $r_1 = r_2$.
Therefore $a \equiv b \pmod{n}$.