The group $\mathbb{Z}$.

THM. (Euclid division) Given $n \in \mathbb{N}$, for any $x \in \mathbb{Z}$, there $\exists!$ $q \in \mathbb{Z}$, $r \in \mathbb{Z}$, s.t., $0 \le r < n$, $x = qn + r$.

Proof. (Existence) $x = 0 \rightsquigarrow q = r = 0$.

If $x > 0$, let $A = \{k \in \mathbb{N} \mid kn > x\}$. By well-ordering principle, $\exists!$ q, s.t., $q+1 = \min A$.

So $qn \le x < (q+1)n$. Let $r = x - qn$, then $0 \le r < n$, and $x = qn + r$.

If $x < 0$, then $-x = q'n + r'$, $0 \le r' < n$.

If $r' = 0$, $\Rightarrow x = (-q')n$

If $r' > 0$ $\Rightarrow x = -q'n - r' = (-q'-1)n + (n - r')$.

Altogether, we have, for $\forall x \in \mathbb{Z}$, $\exists$ q, r, s.t., $x = qn + r$, $0 \le r < n$.

(Uniqueness) If $x = q_1 n + r_1 = q_2 n + r_2$, where $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, $0 \le r_1, r_2 < n$, then $(q_1 - q_2)n = r_2 - r_1$.

But $-n < r_2 - r_1 < n$, and $r_2 - r_2 = n(q_1 - q_2)$ is a multiple of n. $\Rightarrow r_2 - r_2 = 0 \Rightarrow r_2 = r_1 \Rightarrow q_2 = q_1$. #

Eg. $\{0\} = 0\mathbb{Z}$, $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ are subgroups of $\mathbb{Z}$.

Lemma. $x \in n\mathbb{Z}$ if and only if $n \mid x$, i.e., $x = nq$ for some $q \in \mathbb{Z}$.

see next page!

THM. Any subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$, where $n \in \{0\} \cup \mathbb{N}$.

Proof. Let $H < \mathbb{Z}$. Consider $H \cap \mathbb{N}$. If $H \cap \mathbb{N} = \emptyset$, then $H = \{0\} = 0\mathbb{Z}$. If $H \cap \mathbb{N} \neq \emptyset$, by Well-ordering, let $n = \min(H \cap \mathbb{N})$. $n \in H \Rightarrow n\mathbb{Z} \subset H$.

If $n\mathbb{Z} \neq H$, then $\exists$ $x \in H \setminus n\mathbb{Z}$. $x = qn + r$, $q, r \in \mathbb{Z}$, $0 < r < n$.

2

$\Rightarrow r = x - qn \in H$. But $0 < r < n$, then $n \neq \min(H \cap \mathbb{N})$.
This is a contradiction. So $H = n\mathbb{Z}$.

Def. If $H_1, H_2 < \mathbb{Z}$, define $H_1 + H_2 = \{x+y \mid x \in H_1, y \in H_2\}$.

THM. $H_1, H_2 < \mathbb{Z} \Rightarrow H_1 + H_2 < \mathbb{Z}$ and $H_1 \cap H_2 < \mathbb{Z}$.

Lemma: $n\mathbb{Z} \subset m\mathbb{Z} \iff n \in m\mathbb{Z} \iff m \mid n$.

THM. If $p, q \in \mathbb{Z} \setminus \{0\}$, then $\exists\, d, m \in \mathbb{N}$, s.t.

$p\mathbb{Z} + q\mathbb{Z} = d\mathbb{Z}$, $\quad p\mathbb{Z} \cap q\mathbb{Z} = m\mathbb{Z}$.

Proof. check $p\mathbb{Z} + q\mathbb{Z} \neq \{0\}$, $p\mathbb{Z} \cap q\mathbb{Z} \neq \{0\}$

Def. $d = \text{g.c.d}(p, q)$, $m = \text{l.c.m}(p, q)$.

THM. g.c.d & l.c.m define here are the usual greatest common divisor and least common multiple.

Proof. $p \in p\mathbb{Z} \subset p\mathbb{Z} + q\mathbb{Z} = d\mathbb{Z} \Rightarrow p = dk \Rightarrow d \mid p$.

Similarly, $d \mid q$. $\Rightarrow d$ is a common divisor of p and q.

If $d' \mid p$ & q, ($d' > 0$) then $p\mathbb{Z} \subset d'\mathbb{Z}$, $q\mathbb{Z} \subset d'\mathbb{Z} \Rightarrow$

$p\mathbb{Z} + q\mathbb{Z} \subset d'\mathbb{Z} \Rightarrow d\mathbb{Z} \subset d'\mathbb{Z} \Rightarrow d = d'x \Rightarrow d \geq d'$.

So d is the greatest common divisor of p, q.

$m \in m\mathbb{Z} = p\mathbb{Z} \cap q\mathbb{Z} \subset p\mathbb{Z} \Rightarrow p \mid m$.

Similarly, $q \mid m$. $\Rightarrow m$ is a common multiple of p & q.

If m' ($m' > 0$) is a common multiple of p and q, then

$m' \in p\mathbb{Z}$, and $m' \in q\mathbb{Z} \Rightarrow m' \in p\mathbb{Z} \cap q\mathbb{Z} = m\mathbb{Z} \Rightarrow m \mid m'$.

$\Rightarrow m < m'$. So m is the least common multiple of p and q.

Def. $p, q \in \mathbb{Z} \setminus \{0\}$. We say that p and q are coprime if $g.c.d(p, q) = 1$, i.e., $p\mathbb{Z} + q\mathbb{Z} = \mathbb{Z}$.

Def. $H < \mathbb{Z}$ is call a maximal subgroup if the only subgroups of $\mathbb{Z}$ containing H are H and $\mathbb{Z}$.

THM. $p\mathbb{Z}$ is a maximal subgroup of $\mathbb{Z}$ iff p is 1 or a prime.

THM. If p is a prime number, and $q \in \mathbb{Z}$, then $g.c.d(p, q) = 1$ or p.

Proof. Let $d = g.c.d(p, q)$. Then $d\mathbb{Z} = p\mathbb{Z} + q\mathbb{Z} = p\mathbb{Z}$ or $\mathbb{Z}$.

$\Rightarrow d = p$ or 1.

THM. $p \mid ab$ & p is a prime number $\Rightarrow p \mid a$ or $p \mid b$.

Proof. If $p \nmid a$, $p \nmid b$, then $g.c.d(p, a) = g.c.d(p, b) = 1$.

$\Rightarrow p\mathbb{Z} + a\mathbb{Z} = \mathbb{Z}$, $p\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$

$\Rightarrow \exists\, x, y, u, v \in \mathbb{Z}$, s.t., $px + ay = up + vb = 1$

$\Rightarrow 1 = (px + ay)(up + vb) = p^2xu + pxvb + puay + abyv$

$= p(pxu + xvb + uay) + ab(yv) \in p\mathbb{Z} + ab\mathbb{Z}$.

$\Rightarrow \mathbb{Z} \subset p\mathbb{Z} + ab\mathbb{Z} \Rightarrow g.c.d(p, ab) = 1 \Rightarrow p \nmid ab$.

Contradiction!

THM (Unique Factorization) If $n \in \mathbb{N}$, $n \geq 2$, then there is a unique way to write n as a prodution of prime numbers (up to change of the order of the prime factors.)

Proof. (i) (Existance of the factorization.)
Induct on n. If $n=2$, then $2=2$ is a factorization.
Assume any $n \leq m$ has a factorization. Consider $m+1$.
If $m+1$ is prime, then $m+1 = m+1$ is a factorization.
If $m+1$ is not prime, then $\exists$ a, b, s.t. $2 \leq a, b \leq m$,
$m+1 = ab$. By induction hypothesis, $a = P_1 P_2 \cdots P_k$, $b = q_1 \cdots q_l$,
where $P_1, \cdots, P_k, q_1, \cdots q_l$ are prime numbers.
So $m+1 = ab = P_1 \cdots P_k q_1 \cdots q_l$ is a factorization.
Thus, factorization of n exists if $n \geq 2$.
(ii) (Uniqueness of the factorization.)
Induct on n. If $n=2$, then $2=2$ is the only factorization.
Assume any $n \leq m$ has only one factorization. Consider $m+1$.
If $m+1$ is prime, then $m+1 = m+1$ is the only factorization.
If $m+1$ is not prime, assume $m+1 = x_1 \cdots x_k = y_1 \cdots y_l$ are two factorizations of $m+1$ with $x_1, \cdots, x_k, y_1, \cdots, y_l$ being prime numbers.
By the previous THM, $x_1 \mid y_i$ for some $i = 1, 2, \cdots, l$.
But y_i is also a prime number, so $y_i = x_1$.
Let $n = (m+1)/x_1$. Then $2 \leq n \leq m$, and $n = x_2 \cdots x_k = y_1 \cdots y_{i-1} y_{i+1} \cdots y_l$
$\Rightarrow$ $k-1 = l-1$, and $x_2 \cdots x_k$ and $y_1 \cdots y_{i-1} y_{i+1} \cdots y_l$ are the same factorization of n. $\Rightarrow$ $k = l$, and $x_1 \cdots x_k$ and $y_1 \cdots y_l$ are the same factorization of $m+1$.

Thus, any integer $n \geq 2$ admits a unique factorization into prime numbers.

Recall $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$, and $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

$\mathbb{Z}_n = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\}$

$= \{n\mathbb{Z}, 1+n\mathbb{Z}, 2+n\mathbb{Z}, \cdots, (n-1)+n\mathbb{Z}\}$.

So $|\mathbb{Z}_n| = n$.

Def. We say $a \equiv b \pmod n$ if $a-b$ is a multiple of n.

THM. $a \equiv b \pmod n \iff a + n\mathbb{Z} = b + n\mathbb{Z}$

$\iff$ a and b have the same remainder when (Euclid) divided by n.

Proof. (i) $a \equiv b \pmod n \Rightarrow a - b = nk$ wher $k \in \mathbb{Z}$

$\Rightarrow a = b + nk \in b + n\mathbb{Z} \Rightarrow (a+n\mathbb{Z}) \cap (b+n\mathbb{Z}) \neq \emptyset$

$\Rightarrow a + n\mathbb{Z} = b + n\mathbb{Z}$ (See Lemma 3.1 of Bill's notes).

(ii) $a + n\mathbb{Z} = b + n\mathbb{Z} \Rightarrow a \in b + n\mathbb{Z} \Rightarrow a = b + nk$.

If $b = qn + r$, $q, r \in \mathbb{Z}$, $0 \le r < n$, then

$a = b + nk = (q+k)n + r$.

So a and b have the same remainder when divided by n.

(iii) Assume a & b have the same remainder when divided by n, i.e., $a = q_1 n + r$, $b = q_2 n + r$, where $q_1, q_2, r \in \mathbb{Z}$, and $0 \le r < n$. Then $a - b = (q_1 - q_2)n$ is a multiple of n. $\Rightarrow a \equiv b \pmod n$. □

THM. $\cdot \equiv \cdot \pmod n$ is an equivalence relation on $\mathbb{Z}$.

Proof. Check that (i) $a \equiv a \pmod n$ $\forall a \in \mathbb{Z}$, (ii) $a \equiv b \pmod n \Rightarrow b \equiv a \pmod n$ $\forall a, b \in \mathbb{Z}$ and (iii) $a \equiv b \pmod n$, $b \equiv c \pmod n \Rightarrow a \equiv c \pmod n$. $\forall a, b, c \in \mathbb{Z}$. □

Clearly, $a+n\mathbb{Z}$ is the equivalence class of $\equiv (\mathrm{mod}\ n)$ containing a. We call $a+n\mathbb{Z}$ the modulo n class of a.

Def. (i) $(a+n\mathbb{Z})+(b+n\mathbb{Z}) = (a+b)+n\mathbb{Z}$

(ii) $(a+n\mathbb{Z})\cdot(b+n\mathbb{Z}) = ab+n\mathbb{Z}$.

THM. The "+" and "·" in the above definition is well defined, i.e., depends only on the cosets $a+n\mathbb{Z}$, $b+n\mathbb{Z}$, not on the elements a, b.

Proof. If $a'+n\mathbb{Z} = a+n\mathbb{Z}$, and $b'+n\mathbb{Z} = b+n\mathbb{Z}$, then $a'-a = nk$, $b'-b = nl$, $k, l \in \mathbb{Z}$.

So $(a'+b') = (a+b) + n(k+l)$.

$\Rightarrow a'+b' \in (a+b)+n\mathbb{Z} \Rightarrow ((a'+b')+n\mathbb{Z}) \cap ((a+b)+n\mathbb{Z}) \neq \emptyset$.

$\Rightarrow (a'+b')+n\mathbb{Z} = (a+b)+n\mathbb{Z}$

Also, $a'b' = (a+nk)(b+nl) = ab + anl + bnk + n^2kl$

$= ab + n(al+bk+nkl) \in ab+n\mathbb{Z}$.

$\Rightarrow a'b'+n\mathbb{Z} = ab+n\mathbb{Z}$.

Thus, "+", "·" do not depend on the choice of a and b.

THM. $(\mathbb{Z}_n, +)$ is an abelian group.

Proof. (i) $(n\mathbb{Z}) + (a+n\mathbb{Z}) = (a+n\mathbb{Z}) + (n\mathbb{Z}) = (a+0)+n\mathbb{Z} = a+n\mathbb{Z}$.

(ii) $(a+n\mathbb{Z}) + (-a+n\mathbb{Z}) = (-a+n\mathbb{Z}) + (a+n\mathbb{Z}) = n\mathbb{Z}$.

(iii) $((a+n\mathbb{Z})+(b+n\mathbb{Z}))+(c+n\mathbb{Z}) = (a+n\mathbb{Z}) + ((b+n\mathbb{Z})+(c+n\mathbb{Z}))$

$= (a+b+c)+n\mathbb{Z}$.

(iv) $(a+n\mathbb{Z}) + (b+n\mathbb{Z}) = (b+n\mathbb{Z}) + (a+n\mathbb{Z}) = (a+b)+n\mathbb{Z}$.

THM. If p is a prime number, let $X_p = \mathbb{Z}_p - \{p\mathbb{Z}\}$, then $(X_p, \cdot)$ is an abelian group.

Proof. Need check (i) X_p is closed under "$\cdot$".

(ii) There is a unit element in X_p.

(iii) Any element of X_p has an inverse.

(iv) "$\cdot$" is associative and commutative.

(i) If $a+p\mathbb{Z}$, $b+p\mathbb{Z} \in X_p$, then $a+p\mathbb{Z}$, $b+p\mathbb{Z} \neq p\mathbb{Z}$, i.e., $p \nmid a$ and $p \nmid b$. Assume $(a+p\mathbb{Z})\cdot(b+p\mathbb{Z}) \notin X_p$. Then $(a+p\mathbb{Z})\cdot(b+p\mathbb{Z}) = p\mathbb{Z}$, i.e., $ab \equiv 0 \pmod{p}$, i.e., $p \mid ab$. Since p is a prime number, we have $p \mid a$ or $p \mid b$. This is a contradiction. Thus, $(a+p\mathbb{Z})\cdot(b+p\mathbb{Z}) \in X_p$.

(ii) Clearly $(1+p\mathbb{Z})(a+p\mathbb{Z}) = (a+p\mathbb{Z})(1+p\mathbb{Z}) = a+p\mathbb{Z}$ $\forall a \in \mathbb{Z}$.

(iii) If $a+p\mathbb{Z} \in X_p$, define $f_{a+p\mathbb{Z}}: X_p \to X_p$ by $f_{a+p\mathbb{Z}}(b+p\mathbb{Z}) = (a+p\mathbb{Z})\cdot(b+p\mathbb{Z})$. From (i), we have $f_{a+p\mathbb{Z}}(b+p\mathbb{Z}) \in X_p$ for any $b+p\mathbb{Z} \in X_p$. So $f_{a+p\mathbb{Z}}$ is well defined. Assume $f_{a+p\mathbb{Z}}(b_1+p\mathbb{Z}) = f_{a+p\mathbb{Z}}(b_2+p\mathbb{Z})$, where $b_1+p\mathbb{Z}$, $b_2+p\mathbb{Z} \in X_p$. Then $ab_1 \equiv ab_2 \pmod{p}$. So $p \mid a(b_1-b_2)$. But p is a prime number, and $p \nmid a$ (since $a+p\mathbb{Z} \in X \Rightarrow a \not\equiv 0 \pmod{p}$). So $p \mid b_1 - b_2$, and $b_1+p\mathbb{Z} = b_2+p\mathbb{Z}$. This shows $f_{a+p\mathbb{Z}}$ is injective. But $|X_p| = p-1$ is finite, So $f_{a+p\mathbb{Z}}$ is also surjective. $\Rightarrow \exists\, b \in \mathbb{Z}$, s.t., $b+p\mathbb{Z} \in X_p$, and $f_{a+p\mathbb{Z}}(b+p\mathbb{Z}) = 1+p\mathbb{Z}$, i.e., $(a+p\mathbb{Z})\cdot(b+p\mathbb{Z}) = 1+p\mathbb{Z}$.

(iv) "$\cdot$" is associative and commutative by its definition and the associativity and commutativity of the regulare multiplication $\square$
$(ab = ba,\ (ab)c = a(bc),\ \forall\, a, b, c \in \mathbb{Z})$

Fermat's Little THM. If p is a prime number, and $n \in \mathbb{Z}$ with $p \nmid n$, then $n^{p-1} \equiv 1 \pmod{p}$.

Proof. $p \nmid n \Rightarrow n + p\mathbb{Z} \in X_p$.

$$\Rightarrow n^{p-1} + p\mathbb{Z} = (n+p\mathbb{Z})^{p-1} = (n+p\mathbb{Z})^{|X_p|} = 1 + p\mathbb{Z},$$

where we used Corollary 3.37 of Bill's notes.

$$\Rightarrow n^{p-1} \equiv 1 \pmod{p}.$$

Wilson's THM. If p is a prime number, then $(p-1)! \equiv -1 \pmod{p}$.

Proof. Consider the mod equation $x^2 \equiv 1 \pmod{p}$.

$x^2 \equiv 1 \pmod{p} \Leftrightarrow p \mid x^2 - 1 \Leftrightarrow p \mid (x-1)(x+1)$

$\Leftrightarrow p \mid x+1$ or $p \mid x-1 \Leftrightarrow x \equiv \pm 1 \pmod{p}$.

So the only solutions of $x^2 \equiv 1 \pmod{p}$ is $x \equiv \pm 1 \pmod{p}$, i.e., for any $x + p\mathbb{Z} \in X_p$, $(x+p\mathbb{Z})^2 = 1 + p\mathbb{Z} \Leftrightarrow x + p\mathbb{Z} = (\pm 1) + p\mathbb{Z}$.

If $p = 2$, then $(2-1)! = 1 \equiv -1 \pmod{2}$.

Now assume p is prime number > 2.

For $x = 2, 3, \ldots, p-2$, we have $x \not\equiv \pm 1 \pmod{p}$

$\Rightarrow x^2 \not\equiv 1 \pmod{p} \Rightarrow (x+p\mathbb{Z})^2 \neq 1 + p\mathbb{Z}$.

$\Rightarrow (x + p\mathbb{Z}) \neq (x+p\mathbb{Z})^{-1}$.

So the elements $2+p\mathbb{Z}, \ldots, (p-2)+p\mathbb{Z}$ appear in pairs of elements that are inverses of each other.

$$\Rightarrow (2+p\mathbb{Z}) \cdot (3+p\mathbb{Z}) \cdots ((p-2)+p\mathbb{Z}) = 1 + p\mathbb{Z}.$$

$$\Rightarrow (p-1)! + p\mathbb{Z} = (1+p\mathbb{Z})(2+p\mathbb{Z}) \cdots ((p-2)+p\mathbb{Z}) \cdot ((p-1)+p\mathbb{Z})$$

$$= (1+p\mathbb{Z}) \cdot (1+p\mathbb{Z}) \cdot ((p-1)+p\mathbb{Z})$$

$$= (p-1) + p\mathbb{Z} = (-1) + p\mathbb{Z}.$$

$$\Rightarrow (p-1)! \equiv -1 \pmod{p}.$$