Number Theory and Cryptology

Jayadev Naram

October 28, 2023

Part I
Number Theory

Definition 1 (Binary Operation)**.** *A binary operation on a set S is a function from $S \times S$ to S.*
Eg: $A : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, *i.e,* $(a, b) \mapsto a + b$

Definition 2 (Domain)**.** *A domain is triple $(D, +, \cdot)$, where $|D| > 1$ and $+$ and $\cdot$ are two operations on D such that :*

i) $a + b = b + a$ *and* $a \cdot b = b \cdot a, \forall\, a, b \in D$

ii) $(a + b) + c = a + (b + c)$ *and* $(a \cdot b) \cdot c = a \cdot (b \cdot c), \forall\, a, b, c \in D$

iii) $\exists\, 0, 1 \in D, a + 0 = a$ *and* $a \cdot 1 = a, \forall a \in D$

iv) $a \cdot (b + c) = a \cdot b + a \cdot c, \forall\, a, b, c \in D$

v) $\forall\, a \in D, \exists\ a',\ a + a' = 0$

vi) $a \cdot b = 0 \implies$ *either* $a = 0$ *or* $b = 0$

Eg: $(\mathbb{Z}, +, \cdot)$ *and* $(\mathbb{R}[X], +, \cdot)$, *where* $\mathbb{R}[X]$ *is the Set of real polynomials*

Definition 3 (Field)**.** *If every non-zero elements of a domain D has an inverse, i.e, units are $D - \{0\}$, then D is called a field.*

Division Algorithm

Theorem 1. *Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Then $\exists$ unique q,r $\in \mathbb{Z}$ such that*

$$a = bq + r,\ 0 \leq r < b$$

Proof. If $a = 0$ (trivial). Let's prove for $a \in \mathbb{N}$ by induction. If $a = 1$, take $r = 1$ and $q = 0$ (Base Case). Assume the statement is true $\forall n \in \mathbb{N}, n < a$, then we prove the statement for a. If $a \geq b\, then\ a - b < a$. Then by induction, we have

$$a - b = qb + r,\ 0\ \leq r < b \implies a = (q + 1)b + r$$

If $a < b$, then take $q = 0$ *and* $r = a$. Hence the theorem is proved for $a \in \mathbb{N}$
Now let $a \in \mathbb{Z}_-$. Then $-a \in \mathbb{N}$.

$$\begin{aligned}
&\exists \text{ q and r}, -a = bq + r,\ 0 \le r < b \\
&\implies a = (-q)b + (-r) \\
&\implies a = (-q-1)b + (b-r),\ where\ 0 \le b - r < b
\end{aligned}$$

This ends the existence proof.
Now we prove the uniqueness. Let $(q, r) and (q', r')$ be two pairs that satisfy the theorem. Then,

$$a = bq + r,\ 0 \le r < b$$

$$a = bq' + r',\ 0 \le r' < b$$

WLOG, assume $r' \ge r$, then

$$\begin{aligned}
&\implies 0 \le r' - r < b \\
&\implies bq + r = bq' + r' \\
&\implies b(q - q') = r' - r \\
&\implies b \,|\, (r' - r) \\
&\implies r' = r\ and\ q' = q \qquad (\text{since } r' - r < b)
\end{aligned}$$

This completes the uniqueness proof. ☐

Lemma 2 (Modified Division Algorithm)**.** *Let* $a \in \mathbb{Z}$ *and* $b \in \mathbb{N}$. *Then* $\exists$ *unique* q,$r \in \mathbb{Z}$ *such that*

$$a = bq + r,\ |r| \le \frac{b}{2}$$

Theorem 3. *Let* $a(X)$, $b(X) \in \mathbb{R}[X]$. *Then* $\exists$ *q(X),r(X)* $\in \mathbb{R}[X]$ *such that*

$$a(X) = b(X)q(X) + r(X),\ either\ r(X) = 0\ or\ deg(r(X)) < deg(b(X))$$

Proof. Proof by induction on deg(a(X)). If $deg(a(X)) < deg(b(X))$, then take $q(X) = 0$ *and* $r(X) = a(X)$. If $deg(b(X)) = 0$, i.e, $b(X) = b_0$, then take $q(X) = {b_0}^{-1}a(X)$ and $r(X) = 0$.
Now assume $deg(b(X)) > 0$ and $deg(a(X)) \ge deg(b(X))$ and also assume the theorem is true $\forall\ h(X) \in \mathbb{R}[X],\ deg(h(X)) < deg(a(X))$.
Then if $deg(a(X)) = m\ and\ deg(b(X)) = n$,

$$\begin{aligned}
\implies\ & a(X) = a_0 + a_1X + \cdots + a_mX^m \\
and\quad & b(X) = b_0 + b_1X + \cdots + b_nX^n, \qquad (m \ge n)
\end{aligned}$$

Now consider the polynomial $g(X) = a(X) - {b_n}^{-1}a_mX^{m-n}b(X)$. It can be easily verified that $deg(g(X)) < m$. Then,

$$\exists\ q(X), r(X) \in \mathbb{R}[X], g(X) = b(X)q(X) + r(X),$$

$$where\ r(X) = 0\ \ or\ deg(r(X)) \le deg(b(X))$$

$$\begin{aligned}
&\implies a(X) - {b_n}^{-1}a_mX^{m-n}b(X) = b(X)q(X) + r(X) \\
&\implies a(X) = b(X)(q(X) + {b_n}^{-1}a_mX^{m-n}) + r(X),
\end{aligned}$$

$$where\ r(X) = 0\ or\ deg(r(X)) \leq deg(b(X)))$$

□

Definition 4 (Unit). *The multiplicatively invertible elements in a domain are caleed units of a domain.*
Eg: Units in $\mathbb{Z} = \{\pm 1\}$ *and Units in* $\mathbb{R}[X] = \{c \mid c \in \mathbb{R} - \{0\}\}$

Definition 5 (Prime). *a is prime if* $a = uv \implies$ *either u or v is a unit, but not both.*

Definition 6 (Associate). *b is an associate of a if* $a \mid b$ *and* $b \mid a$ *or equivalently* $a = ub$*, where u is a unit.*

Theorem 4. *If x is a prime and u is a unit, then ux is also a prime.*

Proof. Suppose $ux = st$. Since u is a unit, $x = (u^{-1}s)t$. But we know, x is a prime, then either of $u^{-1}s$ *or* t is a unit. If t is unit, proof is completed. Else $u^{-1}s$ must be a unit. We know that the product of two units is again a unit. So is $uu^{-1}s$, i.e, s is a unit. □

Definition 7 (Greatest Common Divisor). *d is said to be gcd of a and b if* $d \mid a$ *and* $d \mid b$ *and every common divisor c of a and b must divide d, i.e, if* $c \mid a$ *and* $c \mid b$*, then* $c \mid d$*. It is written as d = (a,b).*

Remark. *If d is a gcd a and b and then an associate of d is also a gcd of a and b, i.e, if u is a unit, then* $d = (a, b) = ud$.

Definition 8. *If a and* $b \in \mathbb{Z}$*, then we define*

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

Remark. *It can be seen that* $a, b \in a\mathbb{Z} + b\mathbb{Z}$ *and if* s_1 *and* $s_2 \in a\mathbb{Z} + b\mathbb{Z}$ *then* $s_1x + s_2y \in a\mathbb{Z} + b\mathbb{Z}$*,* $\forall x, y \in \mathbb{Z}$*. Therefore* $a\mathbb{Z} + b\mathbb{Z} \cap \mathbb{N} \neq \emptyset$.

Theorem 5. *If* $a,\ b \in \mathbb{Z}$*, then* $\exists d \in \mathbb{Z}, a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$*, where* $d = (a, b)$.

Proof. We first prove the existence of such a d. Since $a\mathbb{Z} + b\mathbb{Z} \cap \mathbb{N} \neq \emptyset$, let d be is least natural number in $a\mathbb{Z} + b\mathbb{Z}$. Then $d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$. Now let $s \in a\mathbb{Z} + b\mathbb{Z}$, then by division algorithm on $\mathbb{Z}$,

$$\begin{aligned}
&\exists\, q, r \in \mathbb{Z}, s = qd + r, 0\ \leq r < d.\\
&\implies r = s - qd \in \mathbb{Z}\\
&\implies r = 0,\ i.e,\ s = qd\\
&\implies a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}\\
&Therefore,\ a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}.
\end{aligned}$$

Now we prove that $d = (a, b)$. Since $a, b \in a\mathbb{Z} + b\mathbb{Z}$, $d \mid a$ *and* $d \mid b$. But $d \in a\mathbb{Z} + b\mathbb{Z}$, *so* $d = ax + by$ for some $x, y \in \mathbb{Z}$. Suppose $c \mid a$ *and* $c \mid b$, then $a = a_1c$ *and* $b = b_1c$. Then $d = c(xa_1 + yb_1)$, implies $c \mid d$. □

Corollary 5.1. *If* $a \mid bc$ *and* $(a, b) = 1$*, then* $a \mid c$.

Theorem 6. *$\mathbb{Z}$ is a UFD (Unique factorization Domain), i.e, every non-zero, non-unit can be written as product of primes and this factorzation is unique upto order and association, i.e, if n is a non-zero, non-unit in $\mathbb{Z}$, and $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, where $p_i{}'s$ and $q_i{}'s$ are primes, then $r = s$ and every p_i is an associate of some q_j and vice versa.*

Proof. The exitence of such factorization can be proved by using stroing induction for non-negative integers and using this result, we can multiply by a -1 (unit) and show it's true for negative integers as well.
Now, we prove the uniqueness by induction. Suppose n is a non-zero, non-unit.

$$Suppose\ n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s.$$

If $r = 1$ $(Base\ Case),\ then\ n = p_1 = q_1 q_2 \cdots q_s$. But p_1 is a prime, therefore, $s = 1\ and\ n = p_1 = uq_1$, where u is a unit. Assume the statement is true $\forall\ a \in \mathbb{N},\ a < n$. Now we prove the statement for n.

$$p_r \mid n,\ i.e,\ p_r \mid q_1(q_2 \cdots q_s).$$
$$\text{If } (p_r, q_1) = 1 \implies p_r \mid q_2(q_3 \cdots q_s)$$

This way, we get some q_j which is an associate of p_r. WLOG, we can assume p_r is an associate of q_s, i.e, $up_r = q_s$.

$$\begin{aligned}
&\implies p_1 p_2 \cdots p_r - uq_1 q_2 \cdots q_{s-1} p_r = 0 \\
&\implies p_r(p_2 \cdots p_{r-1} - uq_1 q_2 \cdots q_{s-1}) = 0 \\
&\implies p_2 \cdots p_{r-1} = uq_1 q_2 \cdots q_{s-1} < n
\end{aligned}$$

□

Definition 9 ($\mathbb{Z}[\omega]$)**.** $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$, *where* $\omega = \frac{-1 \pm i\sqrt{3}}{2}$.

$$and\ N(\alpha) = \alpha\bar{\alpha}.$$

Remark. *If* $\alpha = a + b\omega$, *then*

$$\begin{aligned}
N(a + b\omega) &= (a + b\omega)(\overline{a + b\omega}) \\
&= (a + b\omega)(a + b\omega^2) \\
&= a^2 - ab + b^2 \\
&= \frac{(2a - b)^2 + 3b^2}{4}
\end{aligned}$$

Remark. *The only element whose norm is 0 is 0.*

Proposition. $\alpha \in \mathbb{Z}[\omega]$ *is a unit iff* $N(\alpha) = 1$.

Proof. Suppose $N(\alpha) = 1$, then $\alpha\overline{\alpha} = 1$. Therefore α is a unit in $\mathbb{Z}[\omega]$.
Conversely, suppose α is a unit $\mathbb{Z}[\omega]$.

$$\begin{aligned}
&\exists \alpha' \in \mathbb{Z}[\omega], \alpha\alpha' = 1 \\
&\implies N(\alpha\alpha') = 1 \\
&\implies N(\alpha)N(\alpha') = 1 \\
&\implies N(\alpha) = 1 \qquad (since,\ N(\alpha) \in \mathbb{N}, \forall\ \alpha \in \mathbb{Z}[\omega]).
\end{aligned}$$

□

Theorem 7. *The units in* $\mathbb{Z}[\omega]$ *are* $\pm 1,\ \pm\omega,\ \pm\omega^2$.

Theorem 8. *There is no element in* $\mathbb{Z}[\omega]$ *with norm 2.*

Theorem 9. *The only elements in* $\mathbb{Z}[\omega]$ *with norm 3 are* $\pm\pi,\ \pm\pi\omega,\ \pm\pi\omega^2$, *where* $\pi = 1-\omega$.

Theorem 10. $\mathbb{Z}[\omega]$ *is a Euclidean Domain, i.e,*

$$\forall \alpha, \beta \in \mathbb{Z}[\omega],\ \beta \neq 0,\ \exists \gamma, \delta \in \mathbb{Z}[\omega], \alpha = \beta\gamma + \delta, N(\delta) < N(\beta).$$

Proof. Let $\alpha = a + b\omega,\ \beta = c + d\omega, a, b, c, d \in \mathbb{Z}[\omega],\ \beta \neq 0$, then $c, d \neq 0$.

Case i) Let $d = 0$. Then by Modified Division Algorithm, we have

$$\begin{aligned}
a &= cq_1 + r_1, \qquad (q_1, r_1 \in \mathbb{Z} \text{ and } |r_1| \leq \frac{c}{2}) \\
b &= cq_2 + r_2, \qquad (q_2, r_2 \in \mathbb{Z} \text{ and } |r_2| \leq \frac{c}{2}) \\
\implies \quad \alpha &= a + b\omega = c(q_1 + q_2\omega) + (r_1 + r_2\omega) \\
\implies N(\delta) &= N(r_1 + r_2\omega) \\
&= {r_1}^2 - r_1r_2 + {r_2}^2 \\
&\leq |r_1|^2 + |r_1||r_2| + |r_2|^2 \\
&= \frac{c^2}{4} + \frac{c^2}{4} + \frac{c^2}{4} \\
&= \frac{3c^2}{4} < c^2 = N(b) = N(\beta)
\end{aligned}$$

Case ii) If $d \neq 0$, consider $\alpha' = \alpha\overline{\beta},\ \beta' = \beta\overline{\beta}$, then $\beta' \in \mathbb{Z}$, then by Case i),

$$\exists \gamma', \delta' \in \mathbb{Z}[\omega], \alpha' = \beta'\gamma' + \delta', N(\delta') < N(\beta') = (N(\beta))^2.$$

Let $\delta = \alpha - \beta\gamma$, then $\delta\overline{\beta} = \alpha\overline{\beta} - \beta\overline{\beta}\gamma = \delta'.N(\delta\beta') = N(\delta') < (N(\beta))^2$

$$\begin{aligned}
&\implies N(\delta)N(\beta) < (N(\beta))^2 \\
&\implies N(\delta) < N(\beta).
\end{aligned}$$

□

Theorem 11. *If* $\alpha, \beta \in \mathbb{Z}[\omega]$, *then* $\exists\ \delta \in \mathbb{Z}[\omega], \alpha\mathbb{Z}[\omega] + \beta\mathbb{Z}[\omega] = \delta\mathbb{Z}[\omega]$, *where* $\delta = (\alpha, \beta)$.

Definition 10. *If* $a, b, m \in \mathbb{Z}$ *and* $m \neq 0$, *we say thata is congruent to b modulo m if* $m \mid b - a$. *This relation is written* $a \equiv b\ (m)$.

Definition 11 $(\mathbb{Z}_n,\ +_n,\ \cdot_n)$**.** *-FILL IN-*

Theorem 12. *If* $a \in \mathbb{Z}_n - \{0\}$ *is a unit iff* $(a, n) = 1$.

Proof. Let $a \in \mathbb{Z}_n - \{0\}$ be a unit. Then $\exists\, a' \in \mathbb{Z}_n - \{0\}$, such that $a \cdot_n a' = 1$, i.e, $\exists\ q,\ aa' = qn + 1$.

$$\implies (a, n) = 1.$$

Now let $(a,n) = 1$, then $\exists\, u, v \in \mathbb{Z},\ au + nv = 1$. By Division Algorithm, $\exists\, q, r,\ such\ that\ u = qn + r,\ r \in \mathbb{Z}_n$.

$$\begin{aligned}
&\implies a(qn + r) + nv = 1\\
&\implies ar = n(-aq - v) + 1\\
&\implies a \cdot_n r = 1 \qquad (Since,\ a, r \in \mathbb{Z}_n).
\end{aligned}$$

Therefore, a is a unit in $\mathbb{Z}_n$. □

Definition 12. *We define U_n to be the set of all units in $\mathbb{Z}_n$ and $\phi(n)$ to be the cardinality of U_n, where ϕ_n is called Euler totient function, i.e,*

$$U_n = \{a \in \mathbb{Z}_n - \{0\} \mid (a,n) = 1\},\ \phi(n) = |U_n|.$$

We define $\phi(1) = 1$.

Remark. *If $n = p$, p is prime, then every element is relatively prime to p, i.e, $U_p = \mathbb{Z}_p - \{0\} = \{1, 2, \cdots, p-1\}$. And also $(\mathbb{Z}_p, +_p, \cdot_p)$ is a field. If $n = p^t$, $\phi(n) = p^{t-1}(p-1)$. If $n = pq$, $\phi(n) = (p-1)(q-1)$.*

Theorem 13 (Euler's Theorem)**.** *If $(a,n) = 1$, then $a^{\phi(n)} \equiv 1\, (mod\, n)$.*

Proof. Let's prove it for elements in U_n first and then for any element in general. Let $U_n = \{a_1, a_2, \cdots, a_{\phi(n)}\}$ and let $a \in U_n$. Then,

$$a \cdot_n U_n = \{a \cdot_n a_1, a \cdot_n a_2, \cdots, a \cdot_n a_{\phi(n)}\} \subseteq U_n$$

Claim. All elements of $a \cdot_n U_n$ are distinct, i.e, $a \cdot_n U_n = U_n$.
We prove this by contradiction. Assume, $a \cdot_n a_i = a \cdot_n a_j,\ such\ that\ i \neq j$. Then $a^{-1} \cdot_n a \cdot_n a_i = a^{-1} \cdot_n a \cdot_n a_j$, hence $a_i = a_j$. Therefore, $a \cdot_n U_n = U_n$.

$$\begin{aligned}
&\implies \prod_{i=1}^{\phi(n)} a \cdot_n a_i = \prod_{j=1}^{\phi(n)} a_j\\
&\implies a^{\phi(n)} \left(\prod_{i=1}^{\phi(n)} a_i \right) = \prod_{j=1}^{\phi(n)} a_j\\
&\implies a^{\phi(n)} b = b,\ where\ b = \prod_{i=1}^{\phi(n)} a_i \in U_n\\
&\implies a^{\phi(n)} = 1\ in\ (\mathbb{Z}_n,\ +_n,\ \cdot_n).
\end{aligned}$$

Now, let's prove the theorem for any $a \in \mathbb{Z},\ such\ that\ (a,n) = 1$. By Division Algorithm, $\exists\, q, r,\ such\ that\ a = qn + r,\ r \in \mathbb{Z}_n$. Since $(a,n) = 1$, we have $(r,n) = 1$.

$$\begin{aligned}
\implies a^{\phi}(n) &= (qn + r)^{\phi(n)}\\
&= r^{\phi(n)} + \binom{\phi(n)}{1}(nq) + \cdots + (nq)^{\phi(n)}\\
&= r^{\phi(n)} + nk
\end{aligned}$$

$$\implies a^{\phi}(n) - 1 = r^{\phi(n)} - 1 + nk$$

$$But\ n \mid r^{\phi(n)} - 1,\ then\ n \mid a^{\phi(n)} - 1$$

$$\implies a^{\phi(n)} \equiv 1\, (mod\, n)$$

□

Notation: $\mathbb{Z}_p{}^x = \mathbb{Z}_p - \{0\}$ *and* $\mathbb{Z}_p{}^{x^2}$ to be set of elements in $\mathbb{Z}_p{}^x$ which are square. Here p is a prime.

Proposition. $|\mathbb{Z}_p{}^{x^2}| = \frac{p-1}{2}$*, therefore* $\exists\, u \in \mathbb{Z}_p{}^x$ *which is a non-sqaure. Then* $u\mathbb{Z}_p{}^{x^2}$ *will be the set of all non-square in* $\mathbb{Z}_p{}^x$*.*

Proof. First, we prove that $|\mathbb{Z}_p{}^{x^2}| = \frac{p-1}{2}$. Consider the following mapping:

$$\begin{aligned} \mathbb{Z}_p{}^x &\mapsto \mathbb{Z}_p{}^{x^2} \\ x &\mapsto x^2 \\ \implies p - x &\mapsto (p-x)^2 = p^2 - 2px + x^2 = x^2 + pk \\ \implies p - x &\mapsto x^2 \ in \ (\mathbb{Z}_p, +_p, \cdot_p) \end{aligned}$$

Therefore this mapping is a 2-1 mapping and hence $|\mathbb{Z}_p{}^{x^2}| = \frac{p-1}{2}$. There are $\frac{p-1}{2}$ non-sqaure elements in $\mathbb{Z}_p{}^x$. Let u be a non-square. Then consider the following mapping:

$$\begin{aligned} \mathbb{Z}_p{}^{x^2} &\mapsto u\mathbb{Z}_p{}^{x^2} \\ x^2 &\mapsto ux^2 \end{aligned}$$

We prove that this mapping is bijective. It is enough to show that all the elements in $u\mathbb{Z}_p{}^{x^2}$ are distinct and non-squares. Consider two elements $ux^2, uy^2 \in u\mathbb{Z}_p{}^{x^2}$.

$$\begin{aligned} &\text{If } ux^2 = uy^2 \\ \implies &u^{-1}ux^2 = u^{-1}uy^2 \qquad (\text{since } \mathbb{Z}_p \text{ is a field}) \\ &\implies x^2 = y^2 \end{aligned}$$

This shows that all the elements of $u\mathbb{Z}_p{}^{x^2}$. Now we show that elements of $u\mathbb{Z}_p{}^{x^2}$ are all the non-sqaure elements in $\mathbb{Z}_p{}^x$. Suppose some element in $u\mathbb{Z}_p{}^{x^2}$ is a square, i.e,

$$\begin{aligned} &\implies ux^2 = y^2 \\ &\implies ux^2x^{-2} = y^2x^{-2} \\ &\implies u = (yx^{-1})^2 \in \mathbb{Z}_p{}^{x^2} \end{aligned}$$

But u is a non-square, which is a contradiction. Therefore, this mapping is not just a bijection, but none of the elements in one set belongs to other. Hence, $u\mathbb{Z}_p{}^{x^2}$ is the set of all non-squares in $\mathbb{Z}_p{}^x$. □

Remark. *From the above proposition it can be concluded that*

$$\mathbb{Z}_p{}^x = u\mathbb{Z}_p{}^{x^2} \oplus \mathbb{Z}_p{}^{x^2}.$$

Definition 13. *We define a mapping such that,*

$$\begin{aligned} &\mathbb{Z} \to \mathbb{Z}_n \\ &x \mapsto \bar{x}, \bar{x} = x(mod\ n) \end{aligned}$$

Theorem 14. *The following properties hold for $x,\, y \in \mathbb{Z}$:*

$$i)\ \overline{x+y} = \bar{x} +_n \bar{y} \qquad\qquad ii)\ \overline{xy} = \bar{x} \cdot_n \bar{y}$$

Define the following mapping from $\mathbb{Z}_{mn} \to \mathbb{Z}_n$ in the similar way as above. Then the following properties hold:

$$i)\ \overline{x +_{mn} y} = \bar{x} +_n \bar{y} \qquad\qquad ii)\ \overline{x \cdot_{mn} y} = \bar{x} \cdot_n \bar{y}$$

Theorem 15 (Chinese Remainder Theorem)**.** *Suppose $(m,n) = 1$. Let $\bar{x} = x(mod\ m)$ and $\bar{\bar{x}} = x(mod\ n)$, $x \in \mathbb{Z}$. Then the following mapping is bijection which preserves operation:*

$$\begin{aligned} \mathbb{Z}_{mn} &\to \mathbb{Z}_m \times \mathbb{Z}_n \\ x &\mapsto (\bar{x}, \bar{\bar{x}}) \end{aligned}$$

Proof. Since the sets are finite, by pigeon hole principle, it is enough to show the mapping $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, x \mapsto (\bar{x}, \bar{\bar{x}})$ is onto for it to be bojective, i.e, if $\forall\ (u,v) \in \mathbb{Z}_m \times \mathbb{Z}_n\ \exists\ x \in \mathbb{Z}_{mn}$, such that $\bar{x} = x(mod\ m)$ and $\bar{\bar{x}} = x(mod\ n)$. We will first show that $\exists\ x \in \mathbb{Z}$ satisfying the above conditions. Since $(m,n) = 1,\ \exists\ M, N \in \mathbb{Z}, Mm + nN = 1$. Let $x = mMv + nNu$, then $x - u = mMv + (nN-1)u = mM(v-u) = mq \implies x = mq+u \implies \bar{x} = u$. Similarly, $\bar{\bar{x}} = v$. So $\exists\ x \in \mathbb{Z},\ \bar{x} = u, \bar{\bar{x}} = v$, then by division algortihm, $\exists\ r \in \mathbb{Z}_{mn}, q,\ x = mnq + r$. Notice that $u = \bar{x} = \overline{mnq+r} = \overline{mnq} +_m \bar{r} = \bar{r}$ and similarly $\bar{\bar{r}} = v$. Therefore,

$$\exists\ x \in \mathbb{Z},\ \bar{x} = x(mod\ m)\ and\ \bar{\bar{x}} = x(mod\ n).$$

We know,

$$\begin{aligned} &i)\ \overline{x +_{mn} y} = \bar{x} +_m \bar{y} &\qquad &ii)\ \overline{x \cdot_{mn} y} = \bar{x} \cdot_m \bar{y} \\ &i)\ \overline{\overline{x +_{mn} y}} = \bar{\bar{x}} +_n \bar{\bar{y}} &\qquad &ii)\ \overline{\overline{x \cdot_{mn} y}} = \bar{\bar{x}} \cdot_n \bar{\bar{y}} \end{aligned}$$

$$\begin{aligned} f(x +_{mn} y) &= (\overline{x +_{mn} y}, \overline{\overline{x +_{mn} y}}) \\ &= (\bar{x} +_m \bar{y}, \bar{\bar{x}} +_n \bar{\bar{y}}) \\ &= (\bar{x}, \bar{\bar{x}}) + (\bar{y}, \bar{\bar{y}}) \\ &= f(x) + f(y). \end{aligned}$$

Similarly, $f(x \cdot_{mn} y) = f(x) \times f(y)$. Here addition$(+)$ and mutliplication$(\times)$ are component-wise. Therefore, f is onto and hence bijective(???). $\square$

Theorem 16. *If $(m,n) = 1$, then $\phi(m) = \phi(m)\phi(n)$.*

Proof. First we show that under this bijection mapping defined above the elements of U_{mn} group map bijetively to the elements of $U_m \times U_n$, i.e,

i) if $x \in U_{mn}$, then $\bar{x} \in U_m$ *and* $\bar{\bar{x}} \in U_n$. If $x \in \mathbb{Z}_{mn}$, then $(x, mn) = 1$, i.e, $ax + bmn = 1$, this implies $(x,m) = 1$ *and* $(x,n) = 1$, i.e, $\bar{x} \in \mathbb{Z}_m$ *and* $\bar{\bar{x}} \in \mathbb{Z}_n$.

ii) if $\bar{x} \in U_m$ *and* $\bar{\bar{x}} \in U_n$, then $x \in U_{mn}$. Then $\exists\ u \in \mathbb{Z}_m$ and $v \in \mathbb{Z}_n$, such that $\bar{x} \cdot_m u = 1$ and $\bar{\bar{x}} \cdot_n v = 1$. Since f is onto, $\exists\ y \in \mathbb{Z}_{mn},\ \bar{y} = u$ *and* $\bar{\bar{y}} = v$. Then $\overline{x \cdot_{mn} y} = \bar{x} \cdot_m \bar{y} = 1$ and $\overline{\overline{x \cdot_{mn} y}} = \bar{\bar{x}} \cdot_m \bar{\bar{y}} = 1$. Therefore, $f(x \cdot_{mn} y) = (\bar{1}, \bar{\bar{1}}) = f(1)$. Since f is one-to-one, $x \cdot_{mn} y = 1$, i.e, $x \in U_{mn}$.

Therefore,

$$\begin{aligned} U_{mn} &\leftrightarrow U_m \times U_n \\ \implies |U_{mn}| &= |U_m||U_n| \\ \implies \phi(mn) &= \phi(m)\phi(n). \end{aligned}$$

□

Theorem 17. *Some important facts from group theory that are used later.*

i) If order of an element in the group is equal to order of the group, then the group is cyclic.

ii) Let $(G, *)$ be a finite group and $(H, *)$ be a subgroup of G, then $|H| \mid |G|$.

iii) In a finite group the order of an element must divide the order of the group.

iv) If $a \in G$, $(G, *)$ be a finite group, then $a^{|G|} = e$.

v) If $a \in G$, $(G, *)$ be a finite group and if $a^i = e$, then $o(a) \mid i$.

vi) If $a \in G$, $(G, *)$ be a finite group, then $o(a^i) = \frac{o(a)}{(i, o(a))}$ and $o(a^i) = o(a)$ iff $(i, o(a)) = 1$. Therefore, there are $\phi(n)$ generators in a cyclic group of order n.

Lemma 18. $\sum_{d|n} \phi(d) = n \; \forall \; n \in \mathbb{N}$.

Proof. Define $f(n) = \sum_{d|n} \phi(d)$. We show that if $(m, n) = 1$, then $f(mn) = f(m)f(n)$. Let $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ and $n = q_1^{e_1} q_2^{e_2} \cdots q_s^{e_s}$. If $d \mid mn$, then $d = (p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r})(q_1^{r_1} q_2^{r_2} \cdots q_s^{r_s}) = d_1 d_2$, such that $(d, m) = d_1$ and $(d, n) = d_2$. Now,

$$\begin{aligned} f(mn) &= \sum_{d|mn} \phi(d) = \sum_{d_1|m,\; d_2|n} \phi(d_1 d_2) = \sum_{d_1|m,\; d_2|n} \phi(d_1)\phi(d_2) \\ &= \sum_{d_1|m} \phi(d_1) \sum_{d_2|n} \phi(d_2) = f(m)f(n) \end{aligned}$$

Let n be a non-zero, such that $n > 1$. Let $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, where p_i's are distinct primes.

$$\begin{aligned} f(p_1^{e_1}) &= \sum_{d|p_1^{e_1}} \phi(d) = \phi(1) + \phi(p_1) + \phi(p_1^2) + \cdots + \phi(p_1^{e_1}) \\ &= 1 + p_1 + \cdots + p_1^{e_1 - 1}(p_1 - 1) = p_1^{e_1} \\ \text{Then, } f(n) &= f(p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}) = f(p_1^{e_1}) f(p_2^{e_2} \cdots p_r^{e_r}) \\ &= p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} = n = \sum_{d|n} \phi(d). \end{aligned}$$

□

Theorem 19. *Let $(\mathbb{F}, +, \cdot)$ be a field and G a finite subgroup of $(\mathbb{F} - \{0\}, \cdot)$, then G is a cyclic group.*

Proof. Given that $G \subseteq (\mathbb{F} - \{0\}, \cdot)$ is finite, i.e, $|G| < \infty$. Let $|G| = n$. If $d \mid n$ define G_d as the set containing all the elements in G of order d. We have $G = \coprod_{d|n} G_d$, then $|G| = \sum_{d|n} |G_d|$. If $G_d = \phi$, then $|G_d| = 0$. Suppose $|G_d| \neq 0$, let $a \in G_d$, then $o(a) = d$.
Consider $H = \{1, a, a^2, \cdots, a^{d-1}\},\ a^d = 1$. Then $X^d - 1$ is a polynomial in $\mathbb{F}[X]$. Notice that all the elements of H are the roots of the polynomial and these are the only roots of $X^d - 1\ in\ \mathbb{F}$. Therefore, $G_d \subseteq H$. Notice that the number of elements in H of order d are $\phi(d)$, since $o(a^i) = o(a) = d$ iff $(i, d) = 1$, then $|G_d| = \phi(d)$. Hence, $G_d = \phi(d)$ or 0.
We know, $\sum_{d|n} \phi(d) = n$ and $n = \sum_{d|n} |G_d|$, hence $|G_d|$ is never 0, i.e, G_d is never empty $\forall\ d \mid n$. In particular, $G_n \neq \phi$, therefore there exists an element of order n. Hence, G is cyclic. ☐

Corollary 19.1. *$(\mathbb{Z}_p - \{0\}, \cdot_p)$ is cyclic group in $F = (\mathbb{Z}_p - \{0\}, +, \cdot_p)$.*

Definition 14 (Legendre Symbol)**.** *Let $c \in \mathbb{Z}$, p is an odd prime. Then we define:*

$$(\frac{c}{p}) = \begin{cases} 0, & if\ p \mid c \\ 1, & if\ \exists\ x \in Z,\ x^2 \equiv c (mod\ p) \\ -1, & otherwise \end{cases}$$

Theorem 20. *The properties of Legendre Symbol are listed below:*

i) *If $a \equiv b (mod\ p)$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

ii) $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$.

iii) $\left(\frac{a}{p}\right) = \bar{a}^{(\frac{p-1}{2})}$, *where $\bar{a} = a (mod\ p)$.*

iv)