Chapter 4

Date: Mar 27 Made by Eric

In this note, $\mathbb{Z}_n$ is always a ring, containing congruence classes of $\equiv_n$, or the cosets of $\mathbb{Z}/n\mathbb{Z}$ if you wish
In this note, p and for each $i \in \mathbb{Z}$, p_i is always a prime

Definitions and Theorems

Definition 1. *Let $[a] \in \mathbb{Z}_n$ be a congruence class*

$$[b] \text{ is the } \textbf{inverse} \text{ of } [a], \text{ if } [a][b] = [1]$$

Definition 2. *A class $[a] \in \mathbb{Z}_n$ is a **unit** if $[a]$ have an inverse*

Definition 3. *Euler's function $\varphi : \mathbb{N} \to \mathbb{N}$ is defined by $\varphi(x) = |\{y : y \leq x | gcd(x, y) = 1\}|$*

Definition 4. *Let $R \subseteq \mathbb{Z}$. Let $\psi_n : R \to U_n$ defined by $\psi_n(x) = [x]$*

$$R \text{ is a } \textbf{reduced set of residues mod (n)} \text{ if } \psi_n \text{ is bijective}$$

Definition 5. *Let $A \subseteq \mathbb{Z}$. Let $\psi_n : A \to \mathbb{Z}_n$ defined by $\psi_n(x) = [x]$*

$$A \text{ is a } \textbf{completed set of residues mod (n)} \text{ if } \psi_n \text{ is bijective}$$

Lemma 1. *$[a]$ is a unit in $\mathbb{Z}_n$, if and only if $gcd(a, n) = 1$*

Proof. $[a]$ is a unit in $\mathbb{Z}_n \iff \exists [b] \in \mathbb{Z}_n, [a][b] = [1] \iff \exists [b] \in \mathbb{Z}_n, [ab] = 1 \iff \exists b \in \mathbb{Z}, ab \equiv_n 1 \iff gcd(a, n) = 1$ ■

Theorem 2. *Let U_n be the set of units $U_n = \{[x] \in \mathbb{Z}_n | \exists y \in \mathbb{Z}_n, xy = 1\}$*

$$U_n \text{ form a group under multiplication}$$

Proof. Let $x, z \in U_n$ and $xy = 1 = zr$

Because $\mathbb{Z}_n$ is commutative, so $(xz)(yr) = (xy)(zr)$, which give us $xy \in U_n$

$1 \in \mathbb{Z}_n$

Let $x \in U_n$ and $xy = 1$

$x^{-1}y^{-1} = (yx)^{-1} = 1$ ■

Corollary 2.1. $\forall a : gcd(a, n) = 1, a^{\varphi(n)} \equiv_n 1$

Proof. We now prove $|U_n| = \varphi(n)$

Let $f : S = \{y : y < n | gcd(y, n) = 1\} \to U_n$ defined by $f(y) = [y]$

$\forall y \in S, gcd(y, n) = 1 \implies [y] \in U_n$

$f(y) = f(x) \implies [y] = [x] \implies n|y - x \implies y = x$ **Because ($y, x < n$)**

For each $[x] \in U_n$, we do division algorithm on x with n to have a remainder $r < n$, such that $[r] = [x]$, so $f(r) = n$ (done)

$gcd(a, n) = 1 \implies [a] \in U_n \implies [a]^{|U_n|} = [1] \implies [a]^{\varphi(n)} = [1] \implies a^{\varphi(n)} \equiv_n 1$

■

Lemma 3. *Let* $n = p^e, \exists e \in \mathbb{N}$

$$\varphi(n) = p^e - p^{e-1}$$

Proof. There are exactly $p^{e-1} - 1$ natural numbers $p, 2p, \dots, (p^{e-1} - 1)p$ smaller than n and is divided by p

So there are exactly $p^e - 1 - (p^{e-1} - 1) = p^e - p^{e-1}$ natural numbers samller than n is not divided by p

$a < n$ and p do not divide $a \iff a < n, gca(a, n) = 1$

■

Lemma 4. *If A is a complete set of residues mod (n), and if m and c are integers with m co-prime to n,then the set $Am + c = \{am + c|a \in A\}$ is also a completed set of residues mod (n)*

Proof. $gcd(m, n) = 1 \implies m \in U_n \implies [m^{-1}] \in \mathbb{Z}_n$

Because A is a complete set of residues mod (n), $\forall [x] \in \mathbb{Z}_n, \exists a \in A, [a] = [m^{-1}(x - c)]$

$[am] = [a][m] = [m^{-1}(x - c)][m] = [x - c]$

$[am + c] = [am] + [c] = [x - c] + [c] = [x]$

So $\forall [x] \in \mathbb{Z}_n, \exists a \in A, [am + c] = [x]$

Let $\psi_n : Am + c \to \mathbb{Z}_n$ be defined by $\psi_n(am + c) = [am + c]$

ψ_n is onto for we know

$|Am + c| = |A| = |\mathbb{Z}_n|$

■

Theorem 5. *Let n, m be coprime*

$$\varphi(nm) = \varphi(n)\varphi(m)$$

Proof. For all natural numbers q smaller than mn, we write $q = xm + y$

$gcd(q,nm)=1 \iff gcd(q,n)=1=gcd(q,m)$

$gcd(q,m)=1 \iff gcd(xm+y,m)=1 \iff gcd(y,m)=1$

There are $\varphi(m)$ number amount of y we can choose so that $gcd(y,m)=1$, we let these y form a set $\{y_1,\dots,y_{\varphi(m)}\}$

Let $X=\{x\in\mathbb{Z}|0\leq x<n\}$

For each fixed y, $Xm+y$ is a completed set of residues mod (n)

$gcd(q,n)=1 \iff gcd(xm+y,n)=1$

For each fixed y, $gcd(xm+y,n)=1$ have $\varphi(n)$ solution

Notice $xm+y=x'm+y' \iff x=x'$ and $y=y'$

Let $R\subseteq X$ and R be a reduced set of residues mod (n)

So there are $|\{y_1,\dots,y_{\varphi(m)}\}|\times|R|=\varphi(m)\varphi(n)$ solutions ■

Theorem 6. *Let $n=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$, where p_i are distinct*

$$\varphi(n)=(p_1^{e_1}-p_1^{e_1-1})\cdots(p_k^{e_k}-p_k^{e_k-1})$$

Proof. We prove by induction

$$\text{Base step: }\varphi(p_1^{e_1}p_2^{e_2})=(p_1^{e_1}-p_1^{e_1-1})(p_2-p_2^{e_2-1})$$

$\varphi(p_1^{e_1}p_2^{e_2})=\varphi(p_1^{e_1})\varphi(p_2^{e_2})=(p_1^{e_1}-p_1^{e_1-1})(p_2-p_2^{e_2-1})$

$$\text{Induction step: }\varphi(p_1^{e_1}\cdots p_n^{e_n})=(p_1^{e_1}-p_1^{e_1-1})\cdots(p_n^{e_n}-p_n^{e_n-1})\implies \varphi(p_1^{e_1}\cdots p_{n+1}^{e_{n+1}})=(p_1^{e_1}-p_1^{e_1-1})\cdots(p_{n+1}^{e_{n+1}}-p_{n+1}^{e_{n+1}-1})$$

$\varphi(p_1^{e_1}\cdots p_{n+1}^{e_{n+1}})=\varphi(p_1^{e_1}\cdots p_n^{e_n})\varphi(p_{n+1}^{e_{n+1}})=(p_1^{e_1}-p_1^{e_1-1})\cdots(p_n^{e_n}-p_n^{e_n-1})(p_{n+1}^{e_{n+1}}-p_{n+1}^{e_{n+1}-1})=(p_1^{e_1}-p_1^{e_1-1})\cdots(p_{n+1}^{e_{n+1}}-p_{n+1}^{e_{n+1}-1})$ ■

Exercises

5.3

Show that if R is a reduced set of residues mod (n), and if an integer a is a unit mod (n), then the set $aR=\{ar|r\in R\}$ is also a reduced set of residues mod (n)

Proof. We now prove $\psi_n[aR]\subseteq U_n$

$\psi_n[aR]\subseteq U_n \iff \forall ar\in aR,[ar]\in U_n$
Because a is a unit mod (n) and R is a reduced set of residues mod (n), so we have $gcd(a,n)=1$ and $gcd(r,n)=1$, which give us $gcd(ar,n)=1$

$gcd(ar, n) = 1 \implies [ar] \in U_n$(done)

We now prove $|aR| = |U_n|$

Let $f : R \to aR$ be defined by $f(r) = ar$

$f(r) = f(r') \implies ar = ar' \implies a(r - r') = 0 \implies r = r'$ **Notice f is from subset of $\mathbb{Z}$ to $\mathbb{Z}$**
$\forall ar \in aR, f(r) = ar$

f is a one-to-one and onto function from R to aR, so $|aR| = |R| = |U_n|$ (done) ■

5.6

Compute $\varphi(42)$

Proof. $\varphi(42) = \varphi(2)\varphi(3)\varphi(7) = 1 * 2 * 6 = 12$ ■

5.8

Prove that for each integer m, there are only finitely many integer n satisfy $\varphi(n) = m$

Proof. We prove $\exists N \in \mathbb{N}, \forall n > N, \varphi(n) > m$

Let $p_1, \ldots, p_{k-1}$ be all primes smaller than m, p_k be the smallest prime bigger than m

We pick $N = p_1^{e_1} \cdots p_k^{e_k}$, such that for all $1 \leq i \leq k$, $p_i^{e_i} - p_i^{e_i - 1} > m$

Let $n > N$

If the prime factorization of n contains only $p_1, \ldots, p_k$, then there exists $1 \leq i \leq k$, such that $e_i' > e_i$ and $p_i^{e_i'}$ is in the prime factorization, then $\varphi(p_i^{e_i'})|\varphi(n)$, where $\varphi(p_i^{e_i'}) = p_i^{e_i'} - p_i^{e_i'-1} > p_i^{e_i} - p_i^{e_i-1} > m$

If the prime factorization of n contains $p_l^{e_l}$, where $p_l > p_i, \forall 1 \leq i \leq k$, which give us $\varphi(n) > m$

$\varphi(p_l^{e_l})|\varphi(n)$, where the smallest $\varphi(p_l^{e_l}) = p_l - 1 > m$, which give us $\varphi(n) > m$ ■