3/2/18

Let $m_1 = n_2 n_3 \dots n_k$

$(n_1, n_j) = 1 \ \forall j \neq 1$

so,

$(n_1, (n_2 \cdot n_3 \cdot \dots \cdot n_k)) = 1$

can find $u_1 \equiv 1 \pmod{n_1}$

$u_1 \equiv 0 \pmod{(n_2 \cdots n_k)}$

$u_1 \equiv 0 \pmod{n_j}, \ (j = 2, \dots, k)$

Sec 1.4

Let $n \in \mathbb{N}'$

$\equiv \pmod{n}$ is an equivalence relation

Congruence classes $[a]_n = \{b \mid a \equiv b \pmod{n}\}$

$\mathbb{Z}_n = \{[0]_n, [1]_n, [\dots]_n, \dots [n-1]_n\}$ ← n of these

$[a]_n + [b]_n = [a+b]_n$

$[a]_n \cdot [b]_n = [ab]_n$

Ch 1.4

$n > 1, n \in \mathbb{Z}$

$[a]_n = \{b : b \equiv a \bmod n\}$

$\mathbb{Z}_n = \{[0]_n, [1]_n \dots [n-1]_n\}$

Define addition and multiplication

$[a]_n + [b]_n = [a+b]_n$

$[a]_n \cdot [b]_n = [a \cdot b]_n$

$c \in [a]_n, d \in [b]_n$, is $[a+b]_n = [c+d]_n$? yes.

$a \equiv c \bmod n$

$b \equiv d \bmod n$

$\Rightarrow a + b \equiv c + d \pmod{n}$

$a \cdot b \equiv c \cdot d \pmod{n}$

$(\mathbb{Z}, +, \cdot)$

Commute $[a]_n + [b]_n = [b]_n + [a]_n$, $[a]_n[b]_n = [b]_n[a]_n$

associate $([a]_n + [b]_n) + [c]_n = [a]_n + ([b]_n + [c]_n)$

identities $[a]_n + [b]_n = [0]_n$, $[a]_n[1]_n = [a]_n$

$\Rightarrow [b]_n = [-a]_n$

distributivity $[a]_n([b]_n + [c]_n) = [a]_n[b]_n + [a]_n[c]_n$

Proof of distrib

$[a]_n([b]_n + [c]_n)$

$= [a]_n([b+c]_n)$

$= [a(b+c)]_n$ since integers are distributive

$= [ab+ac]_n$

$= [ab]_n + [ac]_n$

$= [a]_n[b]_n + [a]_n[c]_n$

There is b s.t.

$[a]_n[b]_n = [1]_n$

iff

$[ab]_n = [1]_n$

iff

$[ab-1]_n \equiv [0]$

iff

$ab-1 \equiv 0 \pmod{n}$

$ab \equiv 1 \pmod{n}$

iff $(a,n) = 1$

if $(a,n) = d > 1$

$a'd = a$

$n'd = n$

$a \cdot n' \equiv 0 \pmod{n}$

$[a]_n[n']_n \equiv [0] \pmod{n}$

Zero divisor

If $n = p$, p prime.
Then $\mathbb{Z}_p$ is a field, e.g., all elements have an additive inverse.

Notation

$\mathbb{Z}_n^\times = \{[a] : [a] \text{ invertible}\}$

Euler φ function
$\varphi(n) = |\mathbb{Z}_n^\times| = |\{0 < a < n : (a,n) = 1\}|$

If p is prime, then
$\varphi(p) = p - 1$
since $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$

Thm Euler:
$n = p_1^{r_1} \cdots p_k^{r_k}$
$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$
$= (p_1^{r_1} - p_1^{r_1 - 1}) \cdots (p_k^{r_k} - p_k^{r_k - 1})$

for a prime power $\boxed{\text{Pf}}$ $n = p^r$
$|\mathbb{Z}_{p^r}^\times| = |\{a \mid 0 < a < p^r, (a, p^r) = 1\}|$
$\Rightarrow (a, p) = 1$

$\{0, 1, 2, \ldots, p^r - 1\} = \mathbb{Z}_{p^r}$
$\setminus p\mathbb{N}$
$\{0p, 1p, 2p, \ldots (p^{r-1} - 1)p\}$

$p^r - p^{r-1}$ elements!

Theorem Suppose $n>1$ in $\mathbb{Z}$ and a in $\mathbb{N}$
$(a,n)=1$.
Then, $a^{\varphi(n)} \equiv 1 = a^0 \pmod n$

Corollary : period of $\{a^k : k \in \mathbb{Z}\}$
(mod n) is a divisor of $\varphi(n)$

$\boxed{\text{Pf}}$ $n=p^r$, $\varphi(n)=p^r-p^{r-1}$

Fermat Corr
If p prime, $a^p = a \pmod p$
and $a^{p-1} \equiv 1$, $a \neq 0$

$\boxed{\text{Proof}}$

$\mathbb{Z}_n^\times = \{[a_1]_n, \dots, [a_{\varphi(n)}]_n\}$ an enumeration of relative primes to n.

Let $a \in \mathbb{Z}$, $(a,n)=1$
$a \cdot a_i$ relatively prime to n
$(a_i,n)=1$ and $(a,n)=1$
$\Rightarrow (a_i a, n)=1$

unit is an element of $\mathbb{Z}_n^\times$

units are closed under mult!

If $i \neq j$, then
$[aa_i] \neq [aa_j]$
Else,
$aa_i \equiv aa_j \pmod n$
or, $a(a_i - a_j) \equiv 0 \pmod n$
That is $n \mid a(a_i - a_j)$
$\Rightarrow n \mid (a_i - a_j)$
$\Rightarrow a_i - a_j = 0$ ↯

7/3/18

$[a_i]_n \to [aa_i]_n$ is 1-1, thus is a bijection

$\mathbb{Z}_n^\times = \{[a_1]_n, \dots, [a_{\varphi(n)}]\} = \{[aa_1]_n \dots [aa_{\varphi(n)}]\}$

$\prod_{i=1}^{\varphi(n)} [a_i]_n = \prod_{i=1}^{\varphi(n)} [aa_i]_n = \prod_{i=1}^{\varphi(n)} [a]_n \prod_{i=1}^{\varphi(n)} [a_i]_n$

$\Rightarrow 1 = \prod_{i=1}^{\varphi(n)} [a]$

$[a^{\varphi(n)}]_n = [1]_n$

$\Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$