Notes

September 12, 2014

assignment

1.4 #16

$[a] \in \mathbb{Z}_n$. $[a]$ is nilpotent if $[a]^k = 0$ for some $k \geq 1$. zero is always nilpotent. show that $\mathbb{Z}_n$ has no nonzero nilpotents iff n has no factor that is a square. if n has no square factors then the prime factorization consists of distinct primes to the power of one only.

proof

$\Rightarrow$

Assume that $\mathbb{Z}_n$ has no nonzero nilpotents. by contradiction assume that there exists some prime p such that $p^2|n$. write $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$ at least one $\alpha_i \geq 1$. choose $a = p_1 p_2 \dots p_t$. then $[a]^{\max \alpha} = [0]$. and $[a] \neq 0$, contradiction because $n|a$ so n is square free.

$\Leftarrow$ assume $n = p_1 p_2 \dots p_t$ $\forall p_i$ are distinct. take $[a] \in \mathbb{Z}_n$ andd assume $[a]^k = [0]$. then $n|a^k$ and $p_1 p_2 \dots p_t | a^k$. $\forall p_i, p_i | a^k$. For every i $p_i|a$ therefore $p_1 p_2 \dots p_t | a$ and $n|a$ so $[a] = [0]$.

last time

$[a]_n$ is invertible iff $(a, n) = 1$ a non-zero element of $\mathbb{Z}_n$ is either invertible or a zero-divisor

proof

let $[a]_n \in \mathbb{Z}_n, n \not| a$. if $(n, a) = 1$ thne $[a]_n$ is invertible. if $(n, a) = d > 1$ then $[a]_n [\frac{n}{d}] = [0]_n$ because $a\frac{n}{d} = \frac{a}{d} n$ so $a\frac{n}{d}$ is a multiple of n. $d > 1 \to d \neq 0$.

consequence

the following are equivalent:

1. n is prime
2. $[0]$ is the only zero divisor of $\mathbb{Z}_n$.
3. every nonzero element of $\mathbb{Z}_n$ is invertible.

proof

if n prime, $(n, a) = 1$ for $0 < a < n$

euler function

if $n \in \mathbb{Z}^+$ $\mathcal{P}(n) =$ the number of positive integers in $\{1, 2, \ldots, n\}$ that are relatively prime to n.

example

$\mathcal{P}(6) = 2$ (because 1 and 5).

observe $\mathcal{P}(n)$ is the number of invertible elements in $\mathbb{Z}_n$.

notation

$\mathbb{Z}_n^* = \{[a]_n : [a]_n \text{ is invertible}\}$. so $\mathcal{P}(n) = |\mathbb{Z}_n^*|$

proposition

$\mathbb{Z}_n^*$ is closed under multiplication.

proof

let $[a]_n, [b]_n \in \mathbb{Z}_n^*$ then $[a]_n[a']_n = [1]$ and similarly $[b]_n[b']_n = [1]$

then $[a]_n[b]_n[a']_n[b']_n = [1]_n$ $\square$

exercise

if $n = p_1^{\alpha 1} \ldots p_t^{\alpha t}, \alpha i \geq 1$ distinct primes

eulers thm

if $(a, n) = 1$ then $a^{\mathcal{P}(n)} \equiv 1 \mod n$.

proof

$\mathbb{Z}_n^* = \{[a_1], [a_2], \ldots, [a_{\mathcal{P}(n)}\}$. now consider $\{[aa_1], [aa_2], \ldots, [aa_{\mathcal{P}(n)}\} \in \mathbb{Z}_n^*$. These are distinct elements.

$$\begin{aligned}
[aa_i] &= [aa_j] \text{ multiply by the inverse of a} \\
[a]^{-1}[aa_i] &= [a]^{-1}[aa_j] \\
[a_i] &= [a_j]
\end{aligned}$$

so $\{[aa_1], [aa_2], \ldots, [aa_{\mathcal{P}(n)}\} = \mathbb{Z}_n^*$

note that the two lists are permutations of eachother.

then $[a_1][a_2] \ldots [a_n] = [aa_1][aa_2] \ldots [aa_{\mathcal{P}(n)}]$