Plan

- Review of Last Lecture
- Section 19. Integral Domains (continued)
- Section 20. Fermat's and Euler's Theorems

Review of Last Lecture

Recall that a ring $(R, +, \cdot)$ is called a **ring with unity** if there is an identity element for $\cdot$, which is unique if exists. This multiplicative identity element is called the **unity**. We often denote it by 1.

Definition 18.16. Let R be a ring with unity $1 \neq 0$. An element $u \in R$ is called a **unit** if it has a multiplicative inverse, that is, there exists $u' \in R$ such that

$$uu' = u'u = 1.$$

If every non-zero element in R is a unit, then R is called a **division ring.**

Definition 18.16 (continued) A commutative division ring is called a **field**.

Example. $\mathbb{R}$, $\mathbb{Q}$ and $\mathbb{C}$ are fields.

Example. $\mathbb{Z}$ is NOT a field, because only two elements $1, -1$ are units. Other elements are not units.

Let R be any of the commutative rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, it is well-known that for $a, b \in R$, $a \neq 0, b \neq 0$, then $ab \neq 0$.

This property doesn't hold for other rings.

Example. In $\mathbb{Z}_{10}$, $4 \neq 0, 5 \neq 0$, but $4 \cdot 5 = 0$. 4 and 5 are called 0 divisors.

Definition. Let R be a commutative ring, a is called a 0 **divisor** if
(1) $a \neq 0$,
(2) there exists $b \in R$, $b \neq 0$ such that $ab = 0$.

The rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ have NO 0-divisor.

Definition 19.6. A ring D is called an **integral domain** if it satisfies the following three conditions
(1) D is a commutative ring.
(2) D has a unity 1, $1 \neq 0$.
(3) D has no 0-divisors.

Example. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are integral domains.

Example. $\mathbb{Z}_{10}$ and $C[0,7]$ are NOT integral domains, because they have 0-divisors.

Theorem 19.9. Every field is an integral domain.

Theorem 19.3. In the ring $\mathbb{Z}_n$, the 0 divisors are precisely those non-zero elements that are not relatively prime to n.

Examples. In $\mathbb{Z}_{12}$, $2, 3, 4, 6, 8, 9, 10$ are 0 divisors. The other five elements are not 0 divisors.

Corollary 19.3. If p is a prime, then $\mathbb{Z}_p$ has no 0 divisors. So $\mathbb{Z}_p$ is an integral domain.

Theorem 19.11. Every finite integral domain is a field.

Sketch of proof. Recall that a ring R is a field iff the following three conditions are satisfied:
(1) R is commutative.
(2) R has unity 1, and $1 \neq 0$.
(3) Every nonzero element $a \in R$, there exists $a^{-1} \in R$ such that $aa^{-1} = 1$.
If R is an integral domain, then (1) (2) are satisfied for R. It remains to prove (3) holds. Let $a \in R$, $a \neq 0$, consider the infinite list $a, a^2, a^3, \ldots$.

Corollary 19.12. If p is a prime, then $\mathbb{Z}_p$ is a field.

Theorem 20.1 (Little Theorem of Fermat) If $a \in \mathbb{Z}$ and a is not a multiple of prime p, then p divides $a^{p-1} - 1$, that is,

$$a^{p-1} \equiv 1 \pmod{p}$$

Example. $p = 7$, $5^6 - 1$ and $(-3)^6 - 1$ are both multiples of 7.

Corollary 20.2. If $a \in \mathbb{Z}$, p is a prime, then $a^p - a$ is a multiple of p.

Theorem 20.1 and Corollary 20.2 are equivalent. We give an elementary proof of Corollary 20.2.

Proof of Corollary of 20.2. It is enough to prove the case $a > 0$. We use the induction on a. If $a = 1$,

$$a^p - a = 1^p - 1 = 0 = 0 \cdot p$$

is a multiple of p. Assume $a = n$, $n^p - n$ is a multiple of p. Then for $a = n + 1$,

$$a^p - a = (n+1)^p - (n+1) = \sum_{i=1}^{p-1} \binom{p}{i} n^i + n^p - n$$

For each $1 \leq i \leq p-1$, $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ is a multiple of p, and $n^p - n$ is a multiple of p, $(n+1)^p - (n+1)$ is a multiple of p.

We now give a group theoretic proof of Fermat's theorem. The same method can be used to prove Euler's generalization. First we need

Theorem 20.6. The set G_n of non-zero elements of $\mathbb{Z}_n$ that not 0 divisors forms a group under the multiplication modulo n.

Example. In $\mathbb{Z}_{10}$, $2, 4, 5, 6, 8$ are 0-divisors. So

$$G_{10} = \{1, 3, 7, 9\}$$

is a group under modulo 10 multiplication.

Example. In $\mathbb{Z}_7$, there is no 0-divisors, so

$$G_7 = \{1, 2, 3, 4, 5, 6\}$$

which is a group under modulo 7 multiplication.

Let $\phi(n)$ be the number of non-zeros elements of $\mathbb{Z}_n$ that are not divisors of 0, that is, $\phi(n)$ is the numbers of elements in $\{1, 2, \ldots, n-1\}$ are relatively prime to n. Then

$$|G_n| = \phi(n)$$

$\phi(n)$, as a function of n, is called the **Euler phi-function.**

Theorem 20.8. If a is an integer relatively prime to n, then $a^{\phi(n)} - 1$ is divisible by n.

How to computer Euler's phi-function $\phi(n)$?

We use the following two rules:

(1) $\phi(mn) = \phi(m)\phi(n)$ for m, n relatively primes.

(2) $\phi(p^k) = p^k - p^{k-1}$, where p is a prime.

Example. Prove that for any positive integer a relatively prime to 10, then the last three digits in the decimal expression for $a^{400} - 1$ are 0.

$$\phi(1000) = \phi(2^3 5^3) = \phi(2^3)\phi(5^3) = (2^3 - 2^2)(5^3 - 5^2) = 400$$

By Euler's theorem, $a^{400} - 1$ is divisible by 1000. So then the last three digits in the decimal expression for $a^{400} - 1$ are 0.

Euler's Theorem implies the Fermat's Little Theorem. Because for a prime p, $\phi(p) = p - 1$, so for every a relatively prime to p, so $a^{p-1} - 1$ is a multiple of p.

The end