UMA205: Introduction to Algebraic Structures

Naman Mishra

January 2024

Contents

Lecture 25: Wed 13 Mar '24
Lecture 26: Wed 13 Mar '24

Proposition .0.1. *There are exactly $\phi(m)$ units in $\mathbb{Z}/m\mathbb{Z}$.*

Proof. $a \in \mathbb{Z}/m\mathbb{Z}$ is a unit iff $ax \equiv 1 \pmod m$ for some $x \in \mathbb{Z}/m\mathbb{Z}$. This is equivalent to $(a, m) = 1$, and there are $\phi(m)$ such a in $\{0, 1, \ldots, m-1\}$. □

Corollary .0.2. *$\mathbb{Z}/p\mathbb{Z}$ is a field iff p is prime.*

Proof. If p is prime, then every element is a unit.

Conversely, if $p = p_1p_2$, then $\overline{p_1}, \overline{p_2} \neq \bar{0}$, but $\overline{p_1p_2} = \bar{0}$. So $\mathbb{Z}/p\mathbb{Z}$ is not a field. □

Notation. We will denote by $U(\mathbb{Z}/m\mathbb{Z})$ the set of units in $\mathbb{Z}/m\mathbb{Z}$.

Lemma .0.3. *$U(\mathbb{Z}/m\mathbb{Z})$ forms a group under multiplication.*

Proof. If a and b are units, then so is ab.

1 is a unit and an identity.

If a is a unit, there exists a unique x such that $ax \equiv 1 \pmod m$. Then x is a unit and the unique inverse of a. □

Theorem .0.4 (Euler)**.** *If $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod m$.*

Proof. By the previous lemma, $a \in G = U(\mathbb{Z}/m\mathbb{Z})$ and $|G| = \phi(m)$. Consider the map $\psi \colon G \to G$ given by $\psi(x) = ax$.

Claim: ψ is a bijection.

Proof of claim: Since G is a group, the inverse of a exists. Suffices to show that ψ is injective (finite set). $\psi(x) = \psi(y) \iff ax = ay \iff x = y$.

Using this claim, we can write

$$\begin{aligned}
\prod_{x \in G} ax &= \prod_{x \in G} x \\
a^{\phi(m)} \prod_{x \in G} x &= \prod_{x \in G} x \\
a^{\phi(m)} &= 1
\end{aligned}$$

□

Corollary .0.5 (Fermat's little theorem)**.** *If p is prime and $p \nmid a$, then* $a^{p-1} \equiv 1 \pmod{p}$.

Proof. $\phi(p) = p - 1$. □

Lemma .0.6. *If a_1, a_2, …, a_j are coprime to m, then so is $a_1 a_2 \dots a_j$.*

Proof. They are all units, so their product is a unit. □

Lemma .0.7. *If a_1, a_2, …, a_j divide m and $(a_i, a_j) = 1$ for all $i \neq j$, then $a_1 a_2 \dots a_j$ divides m.*

Proof. Induction. The base case $j = 1$ is obvious.

Suppose the statement is true for a_1, a_2, …, a_{j-1}. Then by the previous lemma, $a_1 a_2 \dots a_{j-1}$ is coprime to a_j. So we can write $r \cdot a_1 \dots a_{j-1} + s \cdot a_j = 1$. Multiplying by m, we get

$$r \cdot a_1 \dots a_{j-1} m + s \cdot a_j m = m.$$

But a_j divides the m in the first term, and by the induction hypothesis, $a_1 \dots a_{j-1}$ divides the m in the second term. So $a_1 \dots a_j$ divides m. □

Theorem .0.8 (Chinese remainder theorem)**.** *Write $m = m_1 \dots m_k$ with $(m_i, m_j) = 1$ for all $i \neq j$. Let $b_1, \dots, b_j \in \mathbb{Z}$ and consider the system of congruences*

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_k \pmod{m_k}. \end{aligned}$$

Then the system always has solutions and any two solutions differ by a multiple of m.

Proof. Let $n_i = \frac{m}{m_i} = m_1 \dots m_{i-1} m_{i+1} \dots m_k$. Each m_j, $j \neq i$, is coprime to m_i, so by lemma .0.6, $(m_i, n_i) = 1$. Thus we have r_i and s_i such that $r_i m_i + s_i n_i = 1$. Let $e_i = s_i n_i$. Then $e_i \equiv 1 \pmod{m_i}$. Since each $m_j \neq n_j$ divides m, $e_i \equiv 0 \pmod{m_j}$ for all $j \neq i$.

This gives a solution

$$x_0 = b_1 e_1 + b_2 e_2 + \dots + b_k e_k.$$

Suppose x_1 is another solution. Then $x_1 - x_0 \equiv 0 \pmod{m_i}$ for all i. So each of m_1, m_2, …, m_k divides $x_1 - x_0$. By lemma .0.7, m divides $x_1 - x_0$. □

Example (Original example of Sunzi). A certain number leaves a remainder of 2 when divided by 3, a remainder of 3 when divided by 5, and a remainder of 2 when divided by 7. What is the number?

We have

$$\begin{aligned} m_1 &= 3 & m_2 &= 5 & m_3 &= 7 \\ b_1 &= 2 & b_2 &= 3 & b_3 &= 2 \end{aligned}$$

and compute

$$n_1 = 35 \qquad n_2 = 21 \qquad n_3 = 15.$$

We want

$$3r_1 + 35s_1 = 1 \qquad 5r_2 + 21s_2 = 1 \qquad 7r_3 + 15s_3 = 1.$$

One solution is

$$r_1, s_1 = 12, -1 \qquad r_2, s_2 = -4, 1 \qquad r_3, s_3 = -2, 1.$$

This gives

$$e_1 = -35 \qquad e_2 = 21 \qquad e_3 = 15,$$

and finally the solution

$$\begin{aligned} x &= 2(-35) + 3(21) + 2(15) \\ &= -70 + 63 + 30 \\ &= 23. \end{aligned}$$

Lecture 27: Fri 15 Mar '24

Proposition .0.9. *If $R_1, \ldots, R_n$ are rings, then $S = R_1 \times \cdots \times R_n$ is also a ring under componentwise addition and multiplication.*

Proof. Zero is $(0, \ldots, 0)$ and one is $(1, \ldots, 1)$. Inverses are also componentwise. Everything else works componentwise. □

Exercise .0.10. *$u = (u_1, \ldots, u_n)$ is a unit in S iff each u_i is a unit in R_i.*

Theorem .0.11. *If $m = m_1 \ldots m_k$ and $(m_i, m_j) = 1$ for all $i < j$, then*

$$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}.$$

That is, they are isomorphic as rings.

Proof. Define $\psi_i \colon \mathbb{Z} \to \mathbb{Z}/m_i\mathbb{Z}$ as $\psi_i(a) = a \bmod m_i$. Define $\psi = (\psi_1, \ldots, \psi_k)$.

By the Chinese Remainder Theorem, $\psi(n) = (b_1, \ldots, b_k)$ always has a solution, so ψ is surjective.

If $\psi(n) = 0$, then $n \equiv 0 \pmod{m_i}$ for all i, so $n \equiv 0 \pmod{m}$. Thus ψ can be restricted to $\mathbb{Z}/m\mathbb{Z}$ in a natural way, and is then a bijection since its domain and codomain have the same size.

It is easy to check that ψ respects addition and multiplication. $\square$

Corollary .0.12.

$$U(\mathbb{Z}/m\mathbb{Z}) \cong U(\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times U(\mathbb{Z}/m_k\mathbb{Z}).$$

Thus we can restrict our attention to the study of $U(\mathbb{Z}/p^n\mathbb{Z})$ for p prime.

Lemma .0.13. *Let k be a field and $f \in k[x]$ with $\deg f = n$. Then f has at most n distinct roots in k.*

Proof. Induction. Trivial for $n = 1$.

If f has no roots in k, we are done. Otherwise, let α be a root of f. Divide f by $(x-\alpha)$ to get $f(x) = (x-\alpha)q(x) + r$. r has degree less than $(x-a)$, so r is a constant and hence 0.

Thus $f(x) = (x-\alpha)q(x)$ where q has degree $n-1$. Suppose $\beta \neq \alpha$ is a root of f. Then $0 = f(\beta) = (\beta - \alpha)q(\beta)$, so β is a root of q.

But by the induction hypothesis, q has at most $n-1$ roots, so f has at most n roots. Winduction. $\square$

Remark. If k is not a field, this need not hold. For example, let $k = \mathbb{Z}/4\mathbb{Z}$ and let $f(x) = 2x(x+1)$. Then $0, 1, 2, 3$ are all roots of f.

What's wrong? $\mathbb{Z}/4\mathbb{Z}$ has zero divisors. In fact, the above lemma can be generalized to any integral domain.

Corollary .0.14. *Let $f, g \in k[x]$ with $\deg f = \deg g = n$. If f and g agree at $n+1$ points, then $f = g$.*

Proof. Take the difference. This has degree at most n but has $n+1$ roots, so it is the zero polynomial. $\square$

Proposition .0.15. *For any prime p,*

$$x^{p-1} - 1 \equiv (x-1)(x-2)\dots(x-(p-1)) \pmod{p}$$

for all x.

Proof. View this polynomial over the field $\mathbb{Z}/p\mathbb{Z}$. Let f be the difference of the two sides,

$$f(x) = x^{p-1} - 1 - (x-1)(x-2)\dots(x-(p-1)).$$

Note that the x^{p-1} term cancels out, so $\deg f \leq p-2$.

By Fermat's little theorem, $x^{p-1} = 1$ for all $x \neq 0$. Thus $f(x) = 0$ for all $x \neq 0$. Thus f has at least $p-1$ roots, so it must be the zero polynomial. $\square$

Corollary .0.16 (Wilson's theorem)**.** *If p is prime, then*

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof. Set $x = 0$ in the above proposition. $p = 2$ is verified by hand. Every other prime is odd, so the powers of -1 on the RHS cancel out. $\square$

Proposition .0.17. *If p is prime and $d \mid p-1$, then $x^d \equiv 1 \pmod{p}$ has d solutions.*

Proof. Let $d' = (p-1)/d$. Then

$$\begin{aligned} \frac{x^{p-1}-1}{x^d-1} &= \frac{(x^d)^{d'}-1}{x^d-1} \\ &= 1 + x^d + \cdots + (x^d)^{d'-1} \\ \implies x^{p-1} - 1 &= (x^d-1)g(x) \end{aligned}$$

where $g(x)$ has degree $dd' - d = p - 1 - d$. By the previous proposition, $x^{p-1} - 1$ has $p-1$ roots, so $x^d - 1$ has at least d roots. Since $x^d - 1$ has degree d, it has exactly d roots. $\square$

Definition .0.18 (Cyclic group)**.** A group H is said to be *cyclic* if it is generated by a single element x, *i.e.*,

$$H = \{x^n \mid n \in \mathbb{Z}\}.$$

Examples.

- $(\mathbb{Z}, +)$ is cyclic, generated by 1.
- $(\mathbb{Z}/n\mathbb{Z}, +)$ is cyclic, generated by $\bar{1}$.
- $(\mathbb{Z}/4\mathbb{Z}, +)$ is generated by $\bar{1}$ and $\bar{3}$, but not by $\bar{2}$, which only generates a subgroup.

Definition .0.19 (Order of an element)**.** The *order* of an element $x \in H$ is the smallest positive integer n such that $x^n = 1$. If no such n exists, we say that x has *infinite order*.

Examples.

- In $(\mathbb{Z}, +)$, 1 has infinite order.
- In $(\mathbb{Z}/4\mathbb{Z}, +)$, $\bar{1}$ has order 4 but $\bar{2}$ has order 2.

Theorem .0.20 (Gauss). *If p is prime, then $G = U(\mathbb{Z}/p\mathbb{Z})$ is cyclic.*

Proof. For a divisor $d \mid p-1$, define $\psi(d)$ to be the number of elements of orger d in G.

By proposition .0.17, $x^d - 1$ has d solutions in $\mathbb{Z}/p\mathbb{Z}[x]$. Thus there are d elements whose dth power is 1. Thus

$$\sum_{c \mid d} \psi(c) = d.$$

By Möbius inversion,

$$\sum_{c \mid d} \mu(c) \frac{d}{c} = \psi(d).$$

By **??**,

$$\psi(d) = \phi(d).$$

In particular, $\psi(p-1) = \phi(p-1)$.

If $p = 2$, then $|G| = 1$ makes the result trivial. If $p > 2$, then $\phi(p-1) > 1$, so there exists an element with order $p-1$. That element generates G. $\square$

Example. For $p = 5$, $U(\mathbb{Z}/p\mathbb{Z}) = \{1, 2, 3, 4\}$. Then

$$\begin{array}{llll} 2^1 \equiv 2 & 2^2 \equiv 4 & 2^3 \equiv 3 & 2^4 \equiv 1 \\ 3^1 \equiv 3 & 3^2 \equiv 4 & 3^3 \equiv 2 & 3^4 \equiv 1 \\ 4^1 \equiv 4 & 4^2 \equiv 1. & & \end{array}$$

So the group is cyclic, with $\phi(5) = 2$ choices for the generator.