The group structure of $(\mathbb{Z}/n\mathbb{Z})^*$

Ali Nesin

I. Ring Decomposition.

Ia. Show that if n and m are prime to each other then $\mathbb{Z}/nm\mathbb{Z} \approx \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ (as rings with identity).

Ib. Conclude that if $n = p_1^{n_1} \ldots p_k^{n_k}$ is the prime decomposition of n then

$$\mathbb{Z}/n\mathbb{Z} \approx \mathbb{Z}/\, p_1^{n_1}\, \mathbb{Z} \times \ldots \times \mathbb{Z}/\, p_k^{n_k}\, \mathbb{Z}$$

as rings with identity.

Ic. Conclude that if $n = p_1^{n_1} \ldots p_k^{n_k}$ is the prime decomposition of n then

$$(\mathbb{Z}/n\mathbb{Z})^* \approx (\mathbb{Z}/\, p_1^{n_1}\, \mathbb{Z})^* \times \ldots \times (\mathbb{Z}/\, p_k^{n_k}\, \mathbb{Z})^*.$$

Problem. Therefore to understand the group structure of $(\mathbb{Z}/n\mathbb{Z})^*$, we need to understand the group structures of $(\mathbb{Z}/p^k\mathbb{Z})^*$ for primes p and natural numbers k.

II. Elementary Number Theory.

IIa. Show that if n and m are two integers prime to each other then there are integers a and b such that $an + bm = 1$.

IIb. Conclude that $(\mathbb{Z}/n\mathbb{Z})^* = \{\underline{m} : m$ and n are prime to each other$\}$.

Let $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^*| = |\{m \leq n : m$ and n are prime to each other$\}|$.

IIc. Show that if p is a prime then $\varphi(p^k) = p^k - p^{k-1}$.

IId. Show that if n and m are prime to each other then $\varphi(nm) = \varphi(n)\varphi(m)$.

IIe. Compute $\varphi(500)$.

IIf. Show that $\Sigma_{d|n}\, \varphi(d) = n$. (Hint: Proceed by induction on n and use parts IIc and IId).

III. Elementary Group Theory.

Let G denote a group.

IIIa. Let $H \leq G$. For $a, b \in G$ show that either $aH = bH$ or $aH \cap bH = \varnothing$. Conclude that if G is finite then $|H|$ divides $|G|$.

IIIb. Let $g \in G$ have order d. (By definition d is the smallest positive integer such that $g^d = 1$). Show that $|\langle g\rangle| = d$ and that if $g^n = 1$ then d divides n. Conclude that if $g^n = g^m = 1$ for relatively prime n and m then $g = 1$.

IIIc. Assume G is finite and let $g \in G$ have order d. Conclude from above that d divides $|G|$ and that $g^{|G|} = 1$. Conclude that for any $k \in \mathbb{Z}$ relatively prime to n, we have $k^{\varphi(n)} \equiv 1 \mod n$. Conclude that for any $k \in \mathbb{Z}$ not divisible by the prime p, we have $k^{p-1} \equiv 1 \mod p$. Conclude that for any $k \in \mathbb{Z}$ and prime p, we have $k^p \equiv k \mod p$. (One can show this by induction on $|k|$ also).

IIId. Let $a, b \in G$ be two commuting elements whose orders n and m are relatively prime. Show that ab has order nm.

IIIe. Let $\varphi : G \to H$ be a surjective homomorphism of abelian groups. Let

$$\text{Ker } \varphi = \{g \in G : \varphi(g) = 1\}.$$

Show that Ker $\varphi \leq G$. Show that the map $\underline{\varphi} : G/\text{Ker } \varphi \to H$ defined by $\underline{\varphi}(\underline{g}) = \varphi(g)$ is well-defined and is an isomorphism of groups. (This is also valid for nonabelian groups).

IV. Elementary Ring Theory

Let R be a ring and $f(X) \in R[X]$.

IVa. Show that if $r \in R$ is a root of f then $X - r$ divides f.

IVb. Show that if R is a domain and $r_1, ..., r_k \in R$ are distinct roots of f then

$$(X - r_1)(X - r_2) \dots (X - r_k)$$

divides f.

IVc. Conclude that a polynomial f over a domain can have at most $\deg f$ distinct roots in the domain. Conclude that the polynomial $X^d - 1$ has at most d roots in a field.

IVd. Find a counterexample to IVb and IVc if R is not a domain.

V. Case $k = 1$.

Va. Show that $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime.

From now on we let K denote a field and G, a finite multiplicative subgroup of K^*. We will show that G is cyclic. By setting $K = \mathbb{Z}/p\mathbb{Z}$, this will show that $(\mathbb{Z}/p\mathbb{Z})^* \approx \mathbb{Z}/(p-1)\mathbb{Z}$, settling the case $k = 1$.

Let $|G| = n$. It is enough to show that G has an element of order n.

Vb. Let $g \in G$ have order d. Show that $\{x \in G : x^d = 1\} = \langle g \rangle \approx \mathbb{Z}/d\mathbb{Z}$. (Hint: Everything takes place in a field!)

Vc. Let d be a divisor of n. Conclude from above that G has either 0 or $\varphi(d)$ elements of order d.

Vd. Using IIf and Vc show that G has (exactly $\varphi(n)$) elements of order n.

Ve. Conclude that G is cyclic. Conclude that $(\mathbb{Z}/p\mathbb{Z})^* \approx \mathbb{Z}/(p-1)\mathbb{Z}$.

VI. Case $p > 2$ and $k > 1$.

We let $R = \mathbb{Z}/p^k\mathbb{Z}$. We will show that R^* is cyclic. Since

$$|R^*| = p^k - p^{k-1} = p^{k-1}(p-1)$$

and since p^{k-1} and $p - 1$ are prime to each other, by IIId, it is enough to find elements of order p^{k-1} and $p - 1$ of R^*. We will show that $1 + p$ is an element of R^* of order p^{k-1}. It is more difficult to find explicitly an element of order $p - 1$.

VIa. Show that any $a \in R$ can be written as

$$a = a_0 + a_1 p + \dots + a_{k-1}p^{k-1}$$

for some unique $a_0, ..., a_{k-1} \in \{0, 1, ..., p-1\}$. From now on, given $a \in R$, a_0 will denote the above "first coordinate" of a.

VIb. Show that $a \in R^*$ iff $a_0 \neq 0$.

VIc. Show that for all i, $1 + p^iR \leq R^*$.

VId. Show that $|1 + pR| = p^{k-1}$ and that $|R^*/(1+pR)| = p - 1$.

VIe. Show that if $p > 2$ and $a \in 1 + p^iR^*$ then $a^p \in 1 + p^{i+1}R^*$. Show that this is false if $p = 2$. Conclude that the order of $1 + p$ is p^{k-1}.

Now we will find an element of order $p - 1$.

VIf. Let $\varphi : R^* \to R^*$ be the group homomorphism defined by $\varphi(r) = r^{p-1}$. Show that $\varphi(R^*) \leq 1 + pR$. (Hint: IIIc.)

VIg. Show that φ restricted to $1 + pR$ is one-to-one. (Hint: VId). Conclude that $\varphi(R^*) = 1 + pR$.

VIi. Conclude that $R^* \approx (1 + pR) \times \{r \in R^* : r^{p-1} = 1\}$. (Hint : VIg, IIIe, IIIb).

VIj. Let $\psi : R^* \to (\mathbb{Z}/p\mathbb{Z})^*$ be defined by $\psi(a) = [a_0]$. Show that ψ is a surjective homomorphism of groups. Conclude that $R^*/(1+pR) \approx (\mathbb{Z}/p\mathbb{Z})^* \approx \mathbb{Z}/(p-1)\mathbb{Z}$. (Hint IIIe).

VIk. Conclude from VIi and VIj that $\{r \in R^* : r^{p-1} = 1\} \approx \mathbb{Z}/(p-1)\mathbb{Z}$. Conclude that R^* has an element of order $p - 1$. Conclude that R^* is cyclic.

VII. Case *p* = 2 and *k* > 1.

Show that $(\mathbb{Z}/2^k\mathbb{Z})^* \approx \mathbb{Z}/2^{k-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. (Details will be given later).

VIII. General Teorem.

Conclude from all the above that

1) if 4 does not divide n, $(\mathbb{Z}/n\mathbb{Z})^* \approx \mathbb{Z}/\varphi(n)\mathbb{Z}$,

2) if 4 divides n, $(\mathbb{Z}/n\mathbb{Z})^* \approx \mathbb{Z}/\varphi(n/2)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.