The structure of the integers mod n, with application to square roots.

Burton Rosenberg

November 14, 2003

A representation of $\mathbb{Z}_n$. In $\mathbb{Z}_n$ what is meant by 0 is any integer which is a multiple of n; what is meant by 1 is any integer which is one more than a multiple of n; and so forth,

$$a \mapsto \{\, a + \kappa n \,|\, \kappa \in \mathbb{Z} \,\}$$

To perform addition we take any element from each set, sum them, and form the set of multiples,

$$\{\, a + \kappa n \,\} + \{\, b + \kappa n \,\} = \{\, (a+b) + \kappa n \,\}$$

Multiplication is defined similarly.

Notation: We have abbreviated the notation, consider the κ as ranging over all integers. But this isn't a big deal. What is a big deal is that $\{\, a + \kappa n \,\}$ is a set, and the a appearing in the set's definition is generic. Let $A = \{\, a + \kappa n \,\}$. The notation means that $\forall a \in A$, $A = \{\, a + \kappa n \,\}$. Any definition or proof, such as the one above, to be well defined must make use of this more precise definition of A. More properly, the definition of addition is,

$$\text{Given } A, B \in \mathbb{Z}_n, a \in A, b \in B, \text{ define } A + B = \{\, a + b + \kappa n \,\}$$

and we show that the resulting set is the same regardless of the a and b chosen. Briefly, another $a' \in A$ differs from a as a multiple of n, which can be absorbed into the κ.

Lemma 1 *Let n and m be integers greater than one, and m divides n. The map $\phi : \mathbb{Z}_n \rightarrow \mathbb{Z}_m$ is a ring homomorphism.*

Proof: The map is well-defined. Actually, we haven't even defined the map. Here it is,

$$\phi\{\, a + \kappa n \,\} = \{\, a + \kappa m \,\},$$

meaning that for any $a \in A, \phi(A) = \{\, a + \kappa m \,\}$ and that the resulting set is the same regardless of the a chosen. To verify this, let $a, a' \in A$. Since $n|(a - a')$ so $m|(a - a')$. Therefore $\{\, a + \kappa m \,\} = \{\, a' + \kappa m \,\}$.

We need to show $\phi(A+B) = \phi(A) + \phi(B)$ and $\phi(A\,B) = \phi(A)\,\phi(B)$. We just show addition.

$$\begin{aligned}\phi(\{\,a+\kappa n\,\}+\{\,b+\kappa n\,\}) &= \phi(\{\,a+b+\kappa n\,\}) = \{\,a+b+\kappa m\,\} \\ &= \{\,a+\kappa m\,\}+\{\,b+\kappa m\,\} = \phi(\{\,a+\kappa n\,\})+\phi(\{\,b+\kappa n\,\})\end{aligned}$$

Since it doesn't matter which $a \in A$ we take, we take the one which is most convenient for the proof.

Definition 1 (Direct Products) *The direct product* $\mathbb{Z}_n \times \mathbb{Z}_m$ *of* $\mathbb{Z}_n$ *and* $\mathbb{Z}_m$ *is the set of all pairs* (a, b)*, with* $a \in \mathbb{Z}_n$ *and* $b \in \mathbb{Z}_m$*; addition and multiplication is component-wise:* $(a, b)+(c, d) = (e, f)$ *where* $e = a + c \bmod m$ *and* $f = b + d \bmod n$*;* $(a, b)(c, d) = (e, f)$ *where* $e = ac \bmod m$ *and* $f = bd \bmod n$*.*

Theorem 1 *Let* n *and* m *be two relatively prime integers, both greater than one. The map* $\phi : \mathbb{Z}_{nm} \to \mathbb{Z}_n \times \mathbb{Z}_m$ *is a ring isomorphism.*

We have yet to define ϕ: it is the map $\phi(a) = (\phi(a), \phi(a))$. *Caution:* It is a different ϕ for each component — take $a \bmod n$ for the first component and $a \bmod m$ for the second component.

Lemma 2 *Hypothesis as above, the map* ϕ *is bijective.*

Proof: Let $A, B \in \mathbb{Z}_{mn}$. If $\phi(A) = \phi(B)$ then for any $a \in A$ and $b \in B$, $\{\,a + \kappa n\,\} = \{\,b + \kappa n\,\}$ and$\{\,a + \kappa m\,\} = \{\,b + \kappa m\,\}$. So $n|(a - b)$ and $m|(a - b)$. Because n and m are relatively prime $nm|(a - b)$ so $A = B$. So the map is injective. Both groups have nm elements. So the map is bijective.

Remark: The inverse of this map is the Chinese Remainder Theorem. There exists integers s and t such that $sn + tm = 1$, because n and m are relatively prime. Select $b \in B$ and $a \in A$. So bsn is an integer which is $0 \bmod n$ and $b \bmod m$ (that is, $\{\,bsn + \kappa m\,\} = \{\,b + \kappa m\,\}$). Likewise atm is $0 \bmod m$ and $a \bmod n$ (that is, $\{\,atm + \kappa n\,\} = \{\,a + \kappa n\,\}$). The inverse map is then $\phi^{-1}(a, b) = \{\,atm + bsn + \kappa mn\,\}$.

Lemma 3 *Hypothesis as above,* $\phi(a + b) = \phi(a) + \phi(b)$ *and* $\phi(ab) = \phi(a)\phi(b)$*.*

Proof: A previous result shows $\phi(a + b) = \phi(a) + \phi(b)$ for each component individually. Then,

$$\begin{aligned}\phi(a+b) &= (\phi(a+b), \phi(a+b)) = (\phi(a)+\phi(b), \phi(a)+\phi(b)) \\ &= (\phi(a), \phi(a)) + (\phi(b), \phi(b)) = \phi(a) + \phi(b)\end{aligned}$$

The last step requires that ϕ be a bijection. Multiplication is shown similarly.

Proof (of theorem): By the above lemmas, ϕ is a bijection preserving ring operations, hence a ring isomorphism.

Corollary 2 *For $n > 1$ an integer, write $n = \prod_{i=1}^k p_i^{e_i}$, where the p_i are distinct primes. Then there is a ring isomorphism $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \ldots \times \mathbb{Z}_{p_k^{e_k}}$.*

Proof: Show that ring isomorphisms $F \cong G \times H$ and $H \cong J \times K$ imply a ring isomorphism $F \cong G \times J \times K$. Then use induction.

Application to square roots: Let $a \in \mathbb{Z}_n$ such that $a^2 = 1$. Then,

$$\phi(a)^2 = \phi(a^2) = \phi(1) = 1$$

for each ϕ in the isomorphism of $\mathbb{Z}_n \cong \prod_i \mathbb{Z}_{p_i^{e_i}}$. Conversely, if $a_i \in \mathbb{Z}_{p_i^{e_i}}$ such that $a_i^2 = 1$, then,

$$\phi^{-1}((a_i))^2 = \phi^{-1}((a_i)^2) = \phi^{-1}((a_i^2)) = \phi^{-1}((1, 1, \ldots, 1)) = 1.$$

If p is an odd prime, and e a positive integer greater than 1, then 1 has exactly two square roots in $\mathbb{Z}_{p^e}$. Hence:

Theorem 3 *Let n be a positive, odd integer greater than 1 with k distinct prime factors. There are 2^k numbers $a \in \mathbb{Z}_n$ such that $a^2 = 1 \bmod n$.*

An example: Let $n = 3 \cdot 5 \cdot 7 = 105$. The theorem says there are eight roots of unity in $\mathbb{Z}_{105}$. We use the chinese remainder theorem to find them.

In $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7$ the roots of unity are simply (a, b, c) where $a, b, c \in \{1, -1\}$, each 1 and -1 interpreted in the proper ring: $\mathbb{Z}_3$, $\mathbb{Z}_5$ and $\mathbb{Z}_7$.

Invoking chinese remainder once,

$$2 \cdot 3 + (-1) \cdot 5 = 1 \;\Rightarrow\; b \cdot 6 - a \cdot 5 = e.$$

Substituting $a, b \in \{1, -1\}$ gives $e \in \{1, -1, 11, -11\}$. These are the four roots of unity in $\mathbb{Z}_{15}$. Invoking chinese remainder again,

$$1 \cdot 15 + (-2) \cdot 7 = 1 \;\Rightarrow\; c \cdot 15 - e \cdot 14 = f.$$

Substituting values for e and $c \in \{1, -1\}$ and reducing mod 105,

$$f \in \{\, 1, 29, 71, 64, 76, 104, 41, 34 \,\} \pmod{105}.$$

These are the eight roots of unity in $\mathbb{Z}_{105}$.