INTEGERS MODULO n

PAUL L. BAILEY

ABSTRACT. We define and explore the ring of integers modulo n.

1. Well-Ordering Principle

First we establish a few properties of the integers which we need in order to understand the ring of integers modulo n. One tool which can be used to establish these properties is the Well-Ordering Principle.

Proposition 1. Well-Ordering Principle
Let $X \subset \mathbb{N}$ be a nonempty set of natural numbers. Then X contains a smallest, element; that is, there exists $x_0 \in X$ such that for every $x \in X$, $x \leq x_0$.

Proof. Since X is nonempty, it contains an element, say x_1. If x_1 is the smallest member of X, we are done, so assume that the set

$$Y = \{x \in X \mid y < x_1\}$$

is nonempty. Since there are only finitely many natural numbers less than a given natural number, Y is finite.

Proceed by induction on $\pmod{Y}$. If $\pmod{Y} = 1$, then Y contains exactly one element, which is vacuously the smallest member of Y.

Now assume that $\pmod{Y} = n$. By induction, we assume that any nonempty set with less than n elements contains a smallest member. Since Y is nonempty, let $x_2 \in Y$. If x_2 is the smallest member of Y, we are done, so assume that the set

$$Z = \{x \in Y \mid x < x_2\}$$

is nonempty. Since $x_2 \notin Z$, $\pmod{Z} < n$, so Z contains a smallest member (by our inductive hypothesis), say x_0. Then x_0 is also smaller than any element in Y. This completes the proof by induction.

Thus every finite set of natural numbers has a smallest element, and since Y is finite, is has a smallest element. This element is the smallest member of X. $\square$

Date: May 29, 1996.

2. Division Algorithm

Definition 1. Let $m, n \in \mathbb{Z}$. We say that m *divides* n, and write $m \mid n$, if there exists an integer k such that $n = km$.

Exercise 1. Show that the relation $\mid$ is a partial order on the set of positive integers.

Proposition 2. Division Algorithm for Integers
Let $m, n \in \mathbb{Z}$. There exist unique integers $q, r \in \mathbb{Z}$ such that

$$n = qm + r \qquad \text{and} \qquad 0 \leq r < \pmod{m}.$$

Proof. Let $X = \{z \in \mathbb{Z} \mid z = n - km \text{ for some } k \in \mathbb{Z}\}$. The subset of X consisting of nonnegative integers is a subset of $\mathbb{N}$, and by the Well-Ordering Principle, contains a smallest member, say r. That is, $r = n - qm$ for some $q \in \mathbb{Z}$, so $n = qm + r$. We know $0 \leq r$. Also, $r < \pmod{m}$, for otherwise, $r - \pmod{m}$ is positive, less than r, and in X.

For uniqueness, assume $n = q_1 m + r_1$ and $n = q_2 m + r_2$, where $q_1, r_1, q_2, r_2 \in \mathbb{Z}$, $0 \leq r_1 < m$, and $0 \leq r_2 < m$. Then $m(q_1 - q_2) = r_1 - r_2$; also $-m < r_1 - r_2 < m$. Since $m \mid (r_1 - r_2)$, we must have $r_1 - r_2 = 0$. Thus $r_1 = r_2$, which forces $q_1 = q_2$. $\square$

Definition 2. Let $m, n \in \mathbb{Z}$. A *greatest common divisor* of m and n, denoted $\gcd(m, n)$, is a positive integer d such that

(1) $d \mid m$ and $d \mid n$;
(2) If $e \mid m$ and $e \mid n$, then $e \mid d$.

Proposition 3. *Let $m, n \in \mathbb{Z}$. Then there exists a unique $d \in \mathbb{Z}$ such that $d = \gcd(m, n)$, and there exist integers $x, y \in \mathbb{Z}$ such that*

$$d = xm + yn.$$

Proof. Let $X = \{z \in \mathbb{Z} \mid z = xm + yn \text{ for some } x, y \in \mathbb{Z}\}$. Then the subset of X consisting of positive integers contains a smallest member, say d, where $d = xm + yn$ for some $x, y \in \mathbb{Z}$.

Now $m = qd + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < d$. Then $m = q(xm + yn) + r$, so $r = (1 - qxm)m + (qy)n \in X$. Since $r < d$ and d is the smallest positive integer in X, we have $r = 0$. Thus $d \mid m$. Similarly, $d \mid n$.

If $e \mid m$ and $e \mid n$, then $m = ke$ and $n = le$ for some $k, l \in \mathbb{Z}$. Then $d = xke + yle = (xk + yl)e$. Therefore $e \mid d$. This shows that $d = \gcd(m, n)$.

For uniqueness of a greatest common divisor, suppose that e also satifies the conditions of a gcd. Then $d \mid e$ and $e \mid d$. Thus $d = ie$ and $e = jd$ for some $i, j \in \mathbb{Z}$. Then $d = ijd$, so $ij = 1$. Since i and j are integers, then $i = \pm 1$. Since d and e are both positive, we must have $i = 1$. Thus $d = e$. $\square$

Exercise 2. Let $m, n \in \mathbb{Z}$ and suppose that there exist integers $x, y \in \mathbb{Z}$ such that $xm + yn = 1$. Show that $\gcd(m, n) = 1$.

Exercise 3. Let $m, n \in \mathbb{N}$ and suppose that $m \mid n$. Show that $\gcd(m, n) = m$.

3. Euclidean Algorithm

There is an effective procedure for finding the greatest common divisor of two integers. It is based on the following proposition.

Proposition 4. *Let* $m, n \in \mathbb{Z}$*, and let* $q, r \in \mathbb{Z}$ *be the unique integers such that* $n = qm + r$ *and* $0 \leq r < m$*. Then* $\gcd(n, m) = \gcd(m, r)$*.*

Proof. Let $d_1 = \gcd(n, m)$ and $d_2 = \gcd(m, r)$. Since "divides" is a partial order on the positive integers, it suffices to show that $d_1 \mid d_2$ and $d_2 \mid d_1$.

By definition of common divisor, we have integers $w, x, y, z \in \mathbb{Z}$ such that $d_1 w = n$, $d_1 x = m$, $d_2 y = m$, and $d_2 z = r$.

Then $d_1 w = q d_1 x + r$, so $r = d_1(w - qx)$, and $d_1 \mid r$. Also $d_1 \mid m$, so $d_1 \mid d_2$ by definition of gcd.

On the other hand, $n = q d_2 y + d_2 z = d_2(qy + z)$, so $d_2 \mid n$. Also $d_2 \mid m$, so $d_2 \mid d_1$ by definition of gcd. $\square$

Now let $m, n \in \mathbb{Z}$ be arbitrary integers, and write $n = mq + r$, where $0 \leq r < m$. Let $r_0 = n$, $r_1 = m$, $r_2 = r$, and $q_1 = q$. Then the equation becomes $r_0 = r_1 q_1 + r_2$. Repeat the process by writing $m = r q_2 + r_3$, which is the same as $r_1 = r_2 q_2 + r_3$, with $0 \leq r_3 < r_2$. Continue in this manner, so in the i^{th} stage, we have $r_{i-1} = r_i q_i + r_{i+1}$, with $0 \leq r_{i+1} < r_i$. Since r_i keeps getting smaller, it must eventually reach zero.

Let k be the smallest integer such that $r_{k+1} = 0$. By the above proposition and induction,

$$\gcd(n, m) = \gcd(m, r) = \cdots = \gcd(r_{k-1}, r_k).$$

But $r_{k-1} = r_k q_k + r_{k+1} = r_k q_k$. Thus $r_k \mid r_{k-1}$, so $\gcd(r_{k-1}, r_k) = r_k$. Therefore $\gcd(n, m) = r_k$. This process for finding the gcd is known as the *Euclidean Algorithm*.

In order to find the unique integers x and y such that $xm + yn = \gcd(m, n)$, use the equations derived above and work backward. Start with $r_k = r_{k-2} - r_{k-1} q_{k-1}$. Substitute the previous equation $r_{k-1} = r_{k-3} - r_{k-2} q_{k-2}$ into this one to obtain

$$r_k = r_{k-2} - (r_{k-3} - r_{k-2} q_{k-2}) q_{k-1}) = r_{k-2}(q_{k-2} q_{k-1} + 1) - r_{k-3} q_{k-1}.$$

Continuing in this way until you arrive back at the beginning.

For example, let $n = 210$ and $m = 165$. Work forward to find the gcd:

- $210 = 165 \cdot 1 + 45$;
- $165 = 45 \cdot 3 + 30$;
- $45 = 30 \cdot 1 + 15$;
- $30 = 15 \cdot 2 + 0$.

Therefore, $\gcd(210, 165) = 15$. Now work backwards to find the coefficients:

- $15 = 45 - 30 \cdot 1$;
- $15 = 45 - (165 - 45 \cdot 3) = 45 \cdot 4 - 165$;
- $15 = (210 - 165) \cdot 4 - 165 = 210 \cdot 4 - 165 \cdot 5$.

Therefore, $15 = 210 \cdot 4 + 165 \cdot (-5)$.

4. Prime Integers

Definition 3. An integer $p \in \mathbb{Z}$ is called *prime* if

(1) $p \geq 2$;
(2) $p \mid ab \Rightarrow p \mid a$ or $p \mid b$, where $a, b \in \mathbb{N}$.

Definition 4. An integer $p \in \mathbb{Z}$ is called *irreducible* if

(1) $p \geq 2$;
(2) $p = ab \Rightarrow a = 1$ or $b = 1$, where $a, b \in \mathbb{N}$.

Exercise 4. Let $p \in \mathbb{Z}$. Show that p is prime if and only if p is irreducible.

Exercise 5. Let $a, p \in \mathbb{Z}$ such that p is prime.
Show that $\gcd(a, p) = 1$ or $\gcd(a, p) = p$.

Here is an interesting exercise. The standard proof is by contradiction.

Exercise 6. Show that there are infinitely many prime integers.
(Hint: assume there are only finitely many, multiply them, and add 1.)

The following series of exercises constitutes a proof that every integer greater than one has a unique factorization into prime integers.

Exercise 7. Let $p \in \mathbb{Z}$ be prime and let $m, n \in \mathbb{Z}$.
Show that if $p \mid mn$, then $p \mid m$ or $p \mid n$.

Exercise 8. Let $p \in \mathbb{Z}$ be prime and let $n_1, \dots, n_r \in \mathbb{Z}$.
Show that if $p \mid n_1 \dots n_r$, then $p \mid n_i$ for some $i = 1, \dots, r$.
(Hint: proceed by induction on r.)

Exercise 9. Let $a \in \mathbb{Z}$ such that $a \geq 2$.
Show that $a = p_1 \dots p_2$, where p_i is prime for $i = 1, \dots, r$.
(Hint: proceed by strong induction on n.)

Exercise 10. Let $p_1, \dots, p_r, q_1, \dots, q_s$ be prime integers.
Show that if $p_1 \dots p_r = q_1 \dots q_s$, then $r = s$ and that the q_j's can be relabeled so that $p_i = q_i$ for $i = 1, \dots, r$.
(Hint: assume not, and let m be the smallest integer that has two different prime factorizations.)

5. Congruence Modulo n

Definition 5. Let $n \in \mathbb{N}$, and define a relation $\equiv_n$ on $\mathbb{Z}$ by

$$a \equiv_n b \Leftrightarrow n \mid (a - b).$$

This relation is called *congruence modulo* n; that is, if $a \equiv_n b$, we say that a is *congruent* to b modulo n. Sometimes this is written $a \equiv b \pmod{n}$. If the n is understood, we may drop the " $\pmod{n}$" from the notation.

Proposition 5. *Let $n \in \mathbb{N}$. Then $\equiv_n$ is an equivalence relation on $\mathbb{Z}$.*

Proof. We wish to show that $\equiv_n$ is reflexive, symmetric, and transitive.

(*Reflexivity*) Let $a \in \mathbb{Z}$. Now $0 \cdot n = 0 = a - a$; thus $n \mid (a - a)$, so $a \equiv a$. Therefore $\equiv$ is reflexive.

(*Symmetry*) Let $a, b \in \mathbb{Z}$. Suppose that $a \equiv b$; then $n \mid (a - b)$. Then there exists $k \in \mathbb{Z}$ such that $nk = a - b$. Then $n(-k) = b - a$, so $n \mid (b - a)$. Thus $b \equiv a$. Similarly, $b \equiv a \Rightarrow a \equiv b$. Therefore $\equiv$ is symmetric.

(*Transitivity*) Let $a, b, c \in \mathbb{Z}$, and suppose that $a \equiv b$ and $b \equiv c$. Then $nk = a - b$ and $nl = b - c$ for some $k, l \in \mathbb{Z}$. Then $a - c = nk - nl = n(k - l)$, so $n \mid (a - c)$. Thus $a \equiv c$. Therefore $\equiv$ is transitive. $\square$

Proposition 6. *Let $n \in \mathbb{N}$ and let $a_1, a_2 \in \mathbb{Z}$. By the Division Algorithm, there exist unique integers $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ such that*

- *$a_1 = nq_1 + r_1$, where $0 \leq r_1 < n$;*
- *$a_2 = nq_2 + r_2$, where $0 \leq r_2 < n$.*

Then $a_1 \equiv a_2 \pmod{n}$ if and only if $r_1 = r_2$.

Proof.

($\Rightarrow$) Suppose that $a_1 \equiv a_2$. Then $n \mid (a_1 - a_2)$. This means that $nk = a_1 - a_2$ for some $k \in \mathbb{Z}$. But $a_1 - a_2 = n(q_1 - q_2) + (r_1 - r_2)$. Then $n(k + q_1 - q_2) = r_1 - r_2$, so $n \mid r_1 - r_2$.

Multiplying the inequality $0 \leq r_2 < n$ by -1 gives $-n < -r_2 \leq 0$. Adding this inequality to the inequality $0 \leq r_1 < n$ gives $-n < r_1 - r_2 < n$. But $r_1 - r_2$ is an integer multiple of n; the only possibility, then, is that $r_1 - r_2 = 0$. Thus $r_1 = r_2$.

($\Leftarrow$) Suppose that $r_1 = r_2$. Then $a_1 - a_2 = nq_1 - nq_2 = n(q_1 - q_2)$. Thus $n \mid (a_1 - a_2)$, so $a_1 \equiv a_2$. $\square$

6. Integers Modulo n

Definition 6. The partition of $\mathbb{Z}$ induced by the equivalence relation $\equiv_n$ is called the set of *integers modulo* n, and is denoted $\mathbb{Z}_n$. For an integer $a \in \mathbb{Z}$, denote its equivalence class under the equivalence relation by $[a]_n$. If the n is understood, we may write this equivalence class as $[a]$ or $\overline{a}$.

An element $r \in \mathbb{Z}$ is called a *preferred representative* for $[a]_n$ if $r \in [a]_n$ and $0 \leq r < n$.

The division algorithm for the integers assures us that there is a unique preferred representative for each equivalence class. Also, as r ranges over the integers from 0 to $n-1$, the equivalence classes $[r]_n$ are distinct. Thus there are exactly n equivalence classes in the set of integers modulo n; that is, $\pmod{\mathbb{Z}_n} = n$. For example,

$$\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}.$$

Proposition 7. *Let $n \in \mathbb{Z}$. Define the binary operations of addition and multiplication in $\mathbb{Z}_n$ by*

$$\overline{a} + \overline{b} = \overline{a+b} \text{ and } \overline{a} \cdot \overline{b} = \overline{ab}.$$

These operations are well-defined.

Proof. Select $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ such that $a_1 \equiv a_2$ and $b_1 \equiv b_2$; say $a_1 - a_2 = kn$ and $b_1 - b_2 = ln$ for some $k, l \in \mathbb{Z}$.

(*Addition*) We wish to show that $\overline{a_1 + b_1} = \overline{a_2 + b_2}$, i.e., that $a_1 + b_1 \equiv a_2 + b_2$. We simply add the equations above to obtain

$$a_1 - a_2 + b_1 - b_2 = kn + ln;$$

thus

$$(a_1 + b_1) - (a_2 + b_2) = (k + l)n;$$

from this, $n \mid ((a_1 + b_1) - (a_2 + b_2))$, so $a_1 + b_1 \equiv a_2 + b_2$.

(*Multiplication*) We wish to show that $\overline{a_1} \cdot \overline{b_1} = \overline{a_2} \cdot \overline{b_2}$, i.e., that $a_1 b_1 \equiv a_2 b_2$. To do this, adjust the original equations to obtain

$$a_1 = a_2 + kn \qquad \text{and} \qquad b_1 = b_2 + ln$$

and multiply them to obtain

$$a_1 b_1 = a_2 b_2 + a_2 ln + b_2 kn + kln^2,$$

whence

$$a_1 b_1 - a_2 b_2 = (a_2 l + b_2 k + kln)n;$$

thus $n \mid (a_1 b_1 - a_2 b_2)$, so $a_1 b_1 \equiv a_2 b_2$. $\square$

7. The Group of Integers Modulo n

Proposition 8. *Addition on $\mathbb{Z}_n$ is commutative, associative, and invertible, with identity element $\overline{0}$.*

Proof. Now select $a, b \in \mathbb{Z}$ so that $\overline{a}$, $\overline{b}$, and $\overline{c}$ are arbitrary members of $\mathbb{Z}_n$.

To see that $+$ is commutative, note that

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a+b} \text{ by definition of } + \\ &= \overline{b+a} \text{ by commutativity in } \mathbb{Z} \\ &= \overline{b} + \overline{a} \end{aligned}$$

To see that $+$ is associative, note that

$$\begin{aligned} (\overline{a} + \overline{b}) + \overline{c} &= \overline{a+b} + \overline{c} \\ &= \overline{(a+b)+c} \\ &= \overline{a+(b+c)} \\ &= \overline{a} + \overline{b+c} \\ &= \overline{a} + (\overline{b} + \overline{c}). \end{aligned}$$

To see that $\overline{0}$ is an additive identity, note that $\overline{0} + \overline{a} = \overline{0+a} = \overline{a}$.

The additive inverse of $\overline{a}$ is $\overline{-a}$, since $\overline{a} + \overline{-a} = \overline{a-a} = \overline{0}$. ☐

Remark 1. A *group* $(G, \cdot, e)$ is a set G together with a binary operation

$$\cdot : G \times G \to G$$

which is associative and invertible with identity element e. If the operation is also commutative, the group is called an *abelian group.*

The above proposition tells us that $(\mathbb{Z}_n, +, \overline{0})$ is an abelian group.

8. Order of an Element in $\mathbb{Z}_n$

For any $k \in \mathbb{N}$ and any $\overline{a} \in \mathbb{Z}_n$, define $k\overline{a}$ to be $\overline{a}$ added to itself k times:

$$k\overline{a} = \sum_{i=1}^{k} \overline{a}.$$

Proposition 9. *Let $k \in \mathbb{N}$ and $\overline{a} \in \mathbb{Z}_n$. Then $k\overline{a} = \overline{ka}$.*

Proof. Since addition is associative, we can ignore parentheses. Then

$$k\overline{a} = \sum_{i=1}^{k} \overline{a} = \overline{\sum_{i=1}^{k} a} = \overline{ka}.$$

$\square$

Definition 7. Let $\overline{a} \in \mathbb{Z}_n$. Define the *order* of $\overline{a}$ to be smallest positive integer k such that $k\overline{a} = \overline{0}$. The order of $\overline{a}$ is denoted $\mathrm{ord}(\overline{a})$.

Proposition 10. *Let $\overline{a} \in \mathbb{Z}_n$ and let* $\mathrm{ord}(\overline{a}) = k$. *Then*
(a) $j\overline{a} = \overline{0} \Leftrightarrow k \mid j$;
(b) $n\overline{a} = \overline{0}$;
(c) $k \mid n$.

Proof.
(a) If $k \mid j$, then $j = lk$ for some $l \in \mathbb{Z}$. In this case, $j\overline{a} = l\overline{0} = \overline{0}$.
Conversely, suppose that $j\overline{a} = \overline{0}$. Write $j = qk + r$, where $0 \leq r < k$. Then $j\overline{a} = qk\overline{a} + r\overline{a} = r\overline{a}$ since $k\overline{a} = 0$. But k is the smallest positive integer such that $k\overline{a} = \overline{0}$. Thus $r = 0$, and $j = qk$. Thus $k \mid j$.
(b) Note that $n\overline{a} = \overline{na} = \overline{0}$. Thus $n\overline{a} = \overline{0}$.
(c) By (b), $n\overline{a} = \overline{0}$. Thus $k \mid n$ by part (a). $\square$

Exercise 11. Let $\overline{a} \in \mathbb{Z}_n$ and let $d = \gcd(a, n)$.
Then $\mathrm{ord}(\overline{a}) = \frac{n}{d}$.
(Hint: let $k = \mathrm{ord}(\overline{a})$, and show that $k \mid \frac{n}{d}$ and that $\frac{n}{d} \mid k$.)

Exercise 12. Find the order of $\overline{6}$, $\overline{11}$, $\overline{18}$, and $\overline{28}$ in $\mathbb{Z}_{36}$.

9. The Ring of Integers Modulo n

Proposition 11. *Multiplication on $\mathbb{Z}_n$ is commutative and associative, with identity element $\overline{1}$. Furthermore, multiplication distributes over addition:*

$$\overline{a} \cdot (\overline{b} + \overline{c}) = (\overline{a} \cdot \overline{b}) + (\overline{a} \cdot \overline{c})$$

for all $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}$.

Proof. Select $a, b, c \in \mathbb{Z}$ so that $\overline{a}$, $\overline{b}$, and $\overline{c}$ are arbitrary members of $\mathbb{Z}_n$.

(*Commutativity*) $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \cdot \overline{a}$.

(*Associativity*) $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{ab} \cdot \overline{c} = \overline{abc} = \overline{a} \cdot \overline{bc} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$.

(*Identity*) $\overline{a} \cdot \overline{1} = \overline{a \cdot 1} = \overline{a} = \overline{1 \cdot a} = \overline{1} \cdot \overline{a}$.

(*Distributivity*)

$\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b+c} = \overline{a(b+c)} = \overline{ab+ac} = \overline{ab} + \overline{ac} = (\overline{a} \cdot \overline{b}) + (\overline{a} \cdot \overline{c})$. □

Remark 2. A *ring* $(R, +, 0, \cdot, 1)$ is a set R together with a pair of binary operations $+$ and $\cdot$ such that $+$ is commutative, associative, and invertible with identity element 0, and $\cdot$ is associative with identity element 1, such that $\cdot$ distributes over $+$. If additionally $\cdot$ is commutative, the ring is called a *commutative ring*.

The above proposition, together with the fact that addition is commutative, associative, and invertible, say that $(\mathbb{Z}_n, +, \overline{0}, \cdot, \overline{1})$ is a *commutative ring*.

Proposition 12. *Let $\overline{a} \in \mathbb{Z}_n$. Then $\overline{a} \cdot \overline{0} = \overline{0} \cdot \overline{a} = \overline{0}$.*

Proof. By definition of multiplication in $\mathbb{Z}_n$, $\overline{a} \cdot \overline{0} = \overline{a \cdot 0} = \overline{0} = \overline{0 \cdot a} = \overline{0} \cdot \overline{a}$. □

An element $\overline{a} \in \mathbb{Z}_n$ is called *invertible* if there exists an element $\overline{b} \in \mathbb{Z}_n$ such that $\overline{a} \cdot \overline{b} = \overline{1}$.

Proposition 13. *Let $n \in \mathbb{N}$ and let $\overline{a} \in \mathbb{Z}_n$.*
Then $\overline{a}$ is invertible if and only if $\gcd(a, n) = 1$.

Proof.

($\Rightarrow$) Suppose that $\overline{a}$ is invertible, and let $\overline{b}$ be its inverse. Then $\overline{ab} = \overline{1}$, so $ab \equiv 1 \pmod{n}$. That is, $kn = ab - 1$ for some $k \in \mathbb{Z}$. Thus $ab + (-k)n = 1$. Therefore $\gcd(a, n) = 1$.

($\Leftarrow$) Suppose that $\gcd(a, n) = 1$. Then there exist $x, y \in \mathbb{Z}$ such that $xa + yn = 1$. Then $\overline{x} \cdot \overline{a} + \overline{y} \cdot \overline{n} = \overline{1}$. But $\overline{n} = \overline{0}$, so $\overline{y} \cdot \overline{n} = \overline{0}$. Thus $\overline{x} \cdot \overline{a} = \overline{1}$, and $\overline{x}$ is the inverse of $\overline{a}$, so $\overline{a}$ is invertible. □

Exercise 13. Let $p \in \mathbb{N}$ be a prime number.
Show that every nonzero element of $\mathbb{Z}_p$ is invertible.

An element $\overline{a} \in \mathbb{Z}_n$ is called a *zero divisor* if it is not zero and if there exists a nonzero element $\overline{b} \in \mathbb{Z}_n$ such that $\overline{a} \cdot \overline{b} = \overline{0}$.

For example, in $\mathbb{Z}_6$, the invertible elements are 1 and 5. The zero divisors are $\overline{2}$, $\overline{3}$, and $\overline{4}$. For example, $\overline{3} \cdot \overline{4} = \overline{12} = \overline{0}$.

Exercise 14. Let $n \in \mathbb{N}$ and let $\overline{a} \in \mathbb{Z}_n$ be a nonzero element.
Show that $\overline{a}$ is invertible if and only if $\overline{a}$ is not a zero divisor.

Exercise 15. Show that if $n \in \mathbb{N}$ is not a prime number, then $\mathbb{Z}_n$ contains zero divisors.

10. Algebraic Equations in $\mathbb{Z}_n$

It is convenient to drop the BAR notation. That is, all numbers are to be interpreted as members of $\mathbb{Z}_n$ for some fixed n, and if we say 0, 1, or a, we mean $\overline{0}$, $\overline{1}$, or $\overline{a}$.

Having dropped the BAR notation, we use the preferred representatives for equivalence classes. Note that $-\overline{a} = \overline{-a} = \overline{n-a}$. For example, in $\mathbb{Z}_8$, we have $-2 = 6$ and $-4 = 4$ (modulo 8).

We now turn our attention to the question of when an equation, such as $14x = 1$ or $x^2 + 1 = 0$, has a solution in $\mathbb{Z}_n$, and how many solutions it has. For example, $14x = 1$ has a solution if and only if 14 is invertible in $\mathbb{Z}_n$, and this is the case if and only if n and 14 are relatively prime. In fact, we have an expicit technique for finding the inverse 14. This technique makes repeated use of the division algorithm.

Suppose $n = 33$. Then 14 and 33 are relatively prime, so there exist integers x and y such that $14x + 33y = 1$. To find them, we divide:

- $33 = 14 \cdot 2 + 5$;
- $14 = 5 \cdot 2 + 4$
- $5 = 4 \cdot 1 + 1$;
- $2 = 1 \cdot 2 + 0$.

The second to last remainder is 1, so $\gcd(14, 33) = 1$. Now work backwards to find x and y:

- $1 = 5 - 4$;
- $1 = 5 - (14 - 5 \cdot 2) = 5 \cdot 3 - 14 \cdot 1$;
- $1 = (33 - 14 \cdot 2) \cdot 3 - 14 \cdot 1 = 33 \cdot 3 - 14 \cdot 7$.

Thus the inverse of 14 in $\mathbb{Z}_{33}$ is $-7 = 26$.

Exercise 16. Find the inverse of 15 in $\mathbb{Z}_{49}$.

The equation $x^2 + 1 = 0$ is more interesting. To understand it, note that -1 exists in $\mathbb{Z}_n$ as $\overline{n-1}$. So a solution to the equation $x^2 + 1 = 0$ would be a square root of negative 1 in $\mathbb{Z}_n$. For example, in $\mathbb{Z}_5$, we have $2^2 = 4 = -1 \pmod 5$.

It is also possible that a quadratic equation, such as $x^2 - 1 = 0$, can have more than two solutions in $\mathbb{Z}_n$. Note that $x^2 - 1 = (x+1)(x-1)$, even in $\mathbb{Z}_n$. Suppose that $n = 15$. Then $x = 1$ and $x = -1 = 14$ are solutions, but so is 4, since $(4+1)(4-1) = 5 \cdot 3 = 0$ (modulo 15).

However, suppose that $n = p$ is a prime number. Then in $\mathbb{Z}_p$, a quadratic equation can have at most 2 roots. This is because $\mathbb{Z}_p$ has no zero divisors. If the quadratic has a root, it factors; then if the product of the factors is zero, one of them must be zero.

For example, let us find the roots of $x^2 + 8x + 1 = 0$ in $\mathbb{Z}_{11}$. Now $8 \equiv -3 \pmod{11}$ and $1 \equiv -10 \pmod{11}$, so our equation becomes $x^2 - 3x - 10 = 0$. This factors as $(x-5)(x+2) = 0$. Since 11 is prime, the only roots are 5 and $-2 = 8$.

Exercise 17. Find all square roots of -1 in $\mathbb{Z}_{101}$.

Department of Mathematics, University of California, Irvine
E-mail address: `pbailey@@math.uci.edu`