ABSTRACT ALGEBRA
TOPIC 2: INTEGERS

PAUL L. BAILEY

1. The Well-Ordering Principle

The set of *natural numbers* is $\mathbb{N} = \{0, 1, 2, 3, \dots\}$, as characterized by the five *Peano axioms*. The main axiom with which we are concerned is as follows.

Proposition 1. (Peano's Axiom)
Let $S \subset \mathbb{N}$. If

- **(a)** $0 \in S$, *and*
- **(b)** $n \in S \Rightarrow n + 1 \in S$,

then $S = \mathbb{N}$.

From this, we are able to develop two related tools for proving many properties of the integers. These tools are known as the Well-Ordering Principle, which says that every nonempty set of natural numbers has a smallest element, and the Induction Principle, which says that if we have a sequence of propositions where the first is true and others follow from the previous one, then they are all true.

Proposition 2. (Well-Ordering Principle)
Let $X \subset \mathbb{N}$ be nonempty. Then there exists $a \in X$ such that $a \leq x$ for every $x \in X$.

Proof. Let $X \subset \mathbb{N}$ and assume that X has no smallest element; we show that $X = \varnothing$. Let

$$S = \{n \in \mathbb{N} \mid n < x \text{ for every } x \in X\}.$$

Clearly $S \cap X = \varnothing$; if we show that $S = \mathbb{N}$, then $X = \varnothing$.

Since 0 is less than or equal to every natural number, 0 is less than or equal to every natural number in X. Since X has no smallest element, $x \neq X$, so $0 < x$ for every $x \in X$. Thus $0 \in S$.

Suppose that $n \in S$. Then $n < x$ for every $x \in X$, so $n + 1 \leq x$ for every $x \in X$. If $n + 1$ were in X, it would be the smallest element of X; since X has no smallest element, $n + 1 \notin X$; thus $n + 1 \neq x$ for every $x \in X$, whence $n + 1 < x$ for every $x \in X$. It follows that $n + 1 \in S$, and by Peano's Axiom, $S = \mathbb{N}$. $\square$

Date: February 23, 2007.

2. The Induction Principles

Proposition 3. (Induction Principle)
Let $\{p_i \mid i \in \mathbb{N}\}$ be a set of propositions indexed by $\mathbb{N}$. Suppose that

(I1) *p_0 is true;*
(I2) *p_{n-1} implies p_n, for $n > 0$.*

Then p_i is true for all $i \in \mathbb{N}$.

Proof. Suppose not, and let $n \in \mathbb{N}$ be the smallest natural number such that p_n is false. Then $n \neq 0$, since p_0 is true by **(I1)**, so $n-1$ exists as a natural number. Since $n-1 < n$, p_{n-1} is true. By **(I2)**, $p_{n-1} \Rightarrow p_n$, so p_n is true, contradicting the assumption. Thus p_i is true for all $i \in \mathbb{N}$. □

We call **(I1)** the *base case* and **(I2)** the *inductive step*. We note that by shifting, we can actually start the induction at any integer. Here is an example demonstrating proof by induction.

Example 1. Show that $11^n - 4^n$ is a multiple of 7 for all $n \in \mathbb{N}$.

Proof. A natural number a is a multiple of 7 if and only if $a = 7b$ for some natural number b. We proceed by induction on n. First we verify the base case, when $n = 0$, and then demonstrate the induction step, wherein we show that if the proposition is true for $n-1$, then it is true for n.

(I1) Let $n = 0$. Then $n = 7 \cdot 0$, so n is a multiple of 7 in this case. This verifies the base case.

(I2) Let $n > 0$, and assume that $11^{n-1} - 4^{n-1}$ is a multiple of 7. Then $11^{n-1} - 4^{n-1} = 7k$ for some $k \in \mathbb{N}$. Now compute

$$\begin{aligned} 11^n - 4^n &= 11^n - 11 \cdot 4^{n-1} + 11 \cdot 4^{n-1} - 4^n \\ &= 11(11^{n-1} - 4^{n-1}) + 4^{n-1}(11 - 4) \\ &= 11 \cdot 7k + 4^{n-1} \cdot 7 \\ &= 7(11k + 4^{n-1}), \end{aligned}$$

which is a multiple of seven.

Thus properties **(I1)** and **(I2)** hold, so the proposition is true for all $n \in \mathbb{N}$. □

Proposition 4. (Strong Induction Principle)
Let $\{p_i \mid i \in \mathbb{N}\}$ be a set of propositions indexed by $\mathbb{N}$. Suppose that

(IS) *if p_i is true for all $i < n$, then p_n is true.*

Then p_i is true for all $i \in \mathbb{N}$.

Proof. Suppose not, and let m be the smallest natural number such that p_m is false. Then p_i is true for all $i < m$. By **(IS)**, p_m is true, contradicting the assumption. Thus p_i is true for all $i \in \mathbb{N}$. □

It is common in the statement of the strong induction principle to include the base case **(I1)**, that p_0 is true, as a premise. In practice, we may have to verify **(I1)** as a step in demonstrating **(IS)**. We note that **(I1)** is implied by **(IS)**, but that **(I2)** is not implied by **(IS)** (why?).

3. The Division Algorithm

Proposition 5. (Division Algorithm)
Let $m, n \in \mathbb{Z}$ with $m \neq 0$. There exist unique integers $q, r \in \mathbb{Z}$ such that

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

We offer two proofs of this, one using the well-ordering principle directly, and the other phrased in terms of strong induction.

Proof by Well-Ordering. First assume that m and n are positive.

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, $r < m$, for otherwise, $r - m$ 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 $q_1 = q_2$.

The proposition remains true if one or both of the original numbers are negative because, if $n = mq + r$ with $0 \leq r < m$, then $0 \leq m - r < m$ when $r > 0$, and

- $(-n) = m(-q - 1) + (m - r)$ if $r > 0$ and $(-n) = m(-q)$ if $r = 0$;
- $(-n) = (-m)(q + 1) + (m - r)$ if $r > 0$ and $(-n) = (-m)q$ if $r = 0$;
- $n = (-m)(-q) + r$.

□

Proof by Strong Induction. Assume that m and n are positive.

If $m > n$, set $q = 0$ and $r = n$. If $m = n$, set $q = 1$ and $r = 0$. Otherwise, we have $0 < m < n$. Proceed by strong induction on n. Here we assume that the proposition is true for all natural number less that n, and show that this implies that the proposition is true for n. Then, by the conclusion of the Strong Induction Principle, the proposition will be true for all natural numbers n.

Note that $n = m + (n - m)$ and $n - m < n$, so by induction, $n - m = mq_1 + r$ for some $q_1, r \in \mathbb{Z}$ with $0 \leq r_1 < m$. Therefore $n = m(q_1 + 1) + r_1$; set $q = q_1 + 1$ to see that $n = mq + r$, with r still in the range $0 \leq r < m$.

The proof for uniqueness and the cases where m and/or n are negative are the same as above. □

Notice that the proof by induction reveals division as repeated subtraction. It more closely mimics the algorithm we use to find q and r than does the proof via the Well-Ordering Principle.

4. The Euclidean 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 $n = km$.

Definition 2. Let $m, n \in \mathbb{Z}$ be nonzero. We say that a positive integer $d \in \mathbb{Z}$ is a *greatest common divisor* of m and n, and write $d = \gcd(m, n)$, if

- **(a)** $d \mid m$ and $d \mid n$;
- **(b)** $e \mid m$ and $e \mid n$ implies $e \mid d$, for all $e \in \mathbb{Z}$.

Proposition 6. (Euclidean Algorithm)
Let $m, n \in \mathbb{Z}$ be nonzero. 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 satisfies 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 $d = e$. □

This shows that the $d = \gcd(m, n)$ exists and the formula $xm + yn = d$ holds, but does not give a method of finding x, y, and d. The method we develop is based on the following propositions.

Proposition 7. *Let $m, n \in \mathbb{N}$ and suppose that $m \mid n$. Then* $\gcd(m, n) = m$.

Proof. Clearly $m \mid m$, and we are given $m \mid n$. Now suppose that $e \mid m$ and $e \mid n$. Then $e \mid m$. Thus $m = \gcd(m, n)$. □

Proposition 8. *Let $m, n \in \mathbb{Z}$ be nonzero, and let $q, r \in \mathbb{Z}$ such that $n = qm + r$. Then* $\gcd(n, m) = \gcd(m, r)$.

Proof. Let $d = \gcd(n, m)$. We wish to show that $d = \gcd(m, r)$, which requires showing that d satisfies the two properties of being the greatest common divisor of m and r.

Since $d = \gcd(n, m)$, we know that $d \mid n$ and $d \mid m$. Thus $n = ad$ and $m = bd$ for some $a, b \in \mathbb{Z}$. Now $r = n - mq = ad - bdq = d(a - bq)$, so $d \mid r$. Thus d is a common divisor of m and r.

Let $e \in \mathbb{Z}$ such that $e \mid m$ and $e \mid r$. Then $m = ge$ and $n = he$ for some $g, h \in \mathbb{Z}$, so $n = geq + he = e(gq + h)$; thus $e \mid n$, so e is a common divisor of n and m. Since $d = \gcd(n, m)$, $e \mid d$. Therefore, $d = \gcd(m, r)$. □

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

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 $m = rq_2 + r_3$, 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.

Example 2. 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, $15 = 210 \cdot 4 + 165 \cdot (-5)$.

Let's briefly analyze the inductive process of "working backwards".

At each stage, let m denote the smaller number and let n denote the larger number. Always attach x to m and y to n, to get $d = xm + yn$, where $d = \gcd(m, n)$. Now at the very end, the remainder is zero, so $n = mq + 0$. Thus $m = \gcd(n, m)$, that is, $d = m$. Writing d as a linear combination at this stage, we have

$$d = (1)m + (0)nm$$

so $x = 1$ and $y = 0$.

Now we want to lift this to a previous equation of the form $n = mq + r$. Assume, by way of induction, that we have already lifted it to the next equation; that is, we have $n' = m'q' + r'$, where $n' = m$, $m' = r$, and we can express d as a linear combination of m' and n', like this:

$$d = x'm' + y'n'.$$

Then $d = x'r + y'm$. Substitute in $r = n - mq$ to express d as a linear combination of m and n; you get $d = x'(n - mq) + y'm = (y' - x'q)m + x'n$. Set $x = y' - x'q$ and $y = x'$ to obtain $d = xm + yn$.

Definition 3. Let $m, n \in \mathbb{Z}$. We say that m and n are *relatively prime* if

$$\gcd(m, n) = 1.$$

Proposition 9. *Let $m, n \in \mathbb{Z}$. Then*

$$\gcd(m, n) = 1 \quad \Leftrightarrow \quad xm + yn = 1 \text{ for some } x, y \in \mathbb{Z}.$$

Proof. We have already seen that if $\gcd(m, n) = 1$, then $xm + yn = 1$ for some $x, y \in \mathbb{Z}$. Thus we prove the reverse direction; suppose that $xm + yn = 1$ for some $x, y \in \mathbb{Z}$. We wish to show that $\gcd(m, n) = 1$.

Clearly $1 \mid m$ and $1 \mid n$. Suppose that $e \mid m$ and $e \mid n$. Then $m = ke$ and $n = le$ for some $k, l \in e$. So

$$1 = xke + yle = (xk + yl)e.$$

Thus $e \mid 1$, whence $\gcd(m, n) = 1$. □

Proposition 10. *Let $m, n, d \in \mathbb{Z}$ such that $\gcd(m, n) = d$. Then $\gcd(\frac{m}{d}, \frac{n}{d}) = 1$.*

Proof. Since $xm + yn = d$ for some $x, y \in \mathbb{Z}$, we have $x\frac{m}{d} + y\frac{n}{d} = 1$. From Proposition 9, we conclude that $\gcd(\frac{m}{d}, \frac{n}{d}) = 1$. □

Proposition 11. *Let $a, b, c \in \mathbb{Z}$. If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.*

Proof. Since $a \mid bc$, there exists $z \in \mathbb{Z}$ such that $az = bc$. Since $\gcd(a, b) = 1$, there exist $x, y \in \mathbb{Z}$ such that $xa + yb = 1$. Multiplying both sides by c gives

$$xac + ybc = c \Rightarrow xac + yaz = c \Rightarrow a(xc + yz) = c.$$

Thus $a \mid c$. □

Proposition 12. *Let $a, b, c \in \mathbb{Z}$. If $a \mid c$, $b \mid c$, and $\gcd(a, b) = 1$, then $ab \mid c$.*

Proof. There exist $e, f, x, y \in \mathbb{Z}$ such that $ae = c$, $bf = c$, and $xa + yb = 1$. Multiplying the last equation by c gives $xac + ybc = c$. Substitution gives $xabf + ybae = c$, so $ab(xf + ye) = c$. Thus $ab \mid c$. □

Definition 4. Let $m, n \in \mathbb{Z}$. We say that a positive integer $l \in \mathbb{Z}$ is a *least common multiple* of m and n, and write $l = \operatorname{lcm}(m, n)$, if

- **(a)** $m \mid l$ and $n \mid l$;
- **(b)** $m \mid k$ and $n \mid k$ implies $l \mid k$, for all $k \in \mathbb{Z}$.

Proposition 13. *Let $m, n \in \mathbb{Z}$ be nonzero. Then there exists a unique $l \in \mathbb{Z}$ such that $l = \operatorname{lcm}(m, n)$, and if $d = \gcd(m, n)$, then*

$$l = \frac{mn}{d}.$$

Proof. Let $l = \frac{mn}{d}$; we wish to show that l is a least common multiple for m and n. Since $d = \gcd(m, n)$, $\frac{m}{d}$ and $\frac{n}{d}$ are integers, and $l = m\frac{n}{d} = n\frac{m}{d}$. Thus $m \mid l$ and $n \mid l$.

Now suppose that k is an integer such that $m \mid k$ and $n \mid k$; we wish to show that $l \mid k$. We have $k = ae$ and $k = bf$ for some $e, f \in \mathbb{Z}$. Thus $ae = bf$, and dividing by d gives $e\frac{a}{d} = f\frac{b}{d}$. Thus $\frac{a}{d} \mid f\frac{b}{d}$, and since $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$, we have $\frac{a}{d} \mid f$. Thus $f = g\frac{a}{d}$ for some $g \in \mathbb{Z}$, so $k = bf = g\frac{ab}{d} = gl$. Thus $l \mid k$, so l is a least common multiple of m and n.

For uniqueness, note that any two least common multiples must divide each other; but they are both positive, so they must be equal. □

5. Fundamental Theorem of Arithmetic

Definition 5. An integer $p \geq 2$, is called *prime* if

$$a \mid p \Rightarrow a = 1 \text{ or } a = p, \quad \text{where } a \in \mathbb{N}.$$

Proposition 14. *Let $a, p \in \mathbb{Z}$, with p prime. Then*

$$\gcd(a, p) = \begin{cases} p & \text{if } p \mid a; \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Let $d = \gcd(a, p)$. Then $d \mid p$, so $d = 1$ or $d = p$. We have $p \mid p$, so if $p \mid a$, we have $p \mid d$. In this case, $d = p$. If p does not divide a, then $d \neq p$, so we must have $d = 1$. □

Proposition 15. (Euclid's Argument)
Let $p \in \mathbb{Z}$, $p \geq 2$. Then p is prime if and only if

$$p \mid ab \Rightarrow p \mid a \text{ or } p \mid b, \quad \text{where } a, b \in \mathbb{N}.$$

Proof.
($\Rightarrow$) Given that $a \mid p \Rightarrow a = 1$ or $a = p$, suppose that $p \mid ab$. Then there exists $k \in \mathbb{N}$ such that $kp = ab$. Suppose that p does not divide a; then $\gcd(a, p) = 1$. Thus there exist $x, y \in \mathbb{Z}$ such that $xa + yp = 1$. Multiply by b to get $xab + ypb = b$. Substitute kp for ab to get $(xk + yb)p = b$. Thus $p \mid b$.
($\Leftarrow$) Given that $p \mid ab \Rightarrow p \mid a$ or $p \mid b$, suppose that $a \mid p$. Then there exists $k \in \mathbb{N}$ such that $ak = p$. So $p \mid ak$, so $p \mid a$ or $p \mid k$. If $p \mid a$, then $pl = a$ for some $l \in \mathbb{N}$, in which case $alk = a$ and $lk = 1$, which implies that $k = 1$ so $a = p$. If $p \mid k$, then $k = pm$ for some $m \in \mathbb{N}$, and $apm = p$, so $am = 1$ which implies that $a = 1$. □

Proposition 16. *Let $n \in \mathbb{Z}$ with $n \geq 2$.*
There exists a prime $p \in \mathbb{Z}$ such that $p \mid n$.

Proof. Proceed by strong induction on n. If n is prime, it divides itself; otherwise, n is not prime, and $n = ab$ for some $a, b \in \mathbb{Z}$ with $a < n$ and $b < n$. By induction, a is divisible by a prime, so $n = ab$ is divisible by that prime. □

Proposition 17. (Fundamental Theorem of Arithmetic)
Let $n \in \mathbb{Z}$, $n \geq 2$. Then there exist unique prime numbers $p_1, \ldots, p_r$, unique up to order, such that

$$n = \prod_{i=1}^{r} p_i.$$

Proof. We know that n is divisible by some prime, say $n = pm$ for some $p, m \in \mathbb{Z}$ with p prime. Since m is smaller than n, we conclude by induction that m factors into a product of primes; thus $n = pm$ factors into a product of primes. To see that this factorization is unique, suppose that there exist prime $p_1, \ldots, p_r$ and $q_1, \ldots, q_s$ such that

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s.$$

By repeatedly applying Euclid's Argument, we see that $p_1 \mid q_i$ for some i, and by renumbering if necessary, we may assume that $p_1 \mid q_1$. Since q_1 is prime, $p_1 = 1$ or $p_1 = q_1$; but p_1 is also prime, so it is greater than 1; thus $p_1 = q_1$. Canceling these, we see that $p_2 \cdots p_r = q_2 \cdots q_s$, and we may repeat this process obtaining $p_2 = q_2$, $p_3 = q_3$, and so forth. We also see that $r = s$, for otherwise, we would obtain an equation in which a product of primes equals one. □

6. Congruence Modulo n

Definition 6. Let $n \in \mathbb{N}$, and define a relation $\equiv_n$ on $\mathbb{Z}$ by

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

This relation is called *congruence modulo* n; that is, if $a \equiv_n b$, we say that a is *congruent* to b modulo n. This relation may also be written $a \equiv b \pmod{n}$, or simply $a \equiv b$ if the n is understood.

Proposition 18. *Let $n \in \mathbb{N}$. Then $\equiv$ modulo n is an equivalence relation on $\mathbb{Z}$.*

Proof. We wish to show that $\equiv$ 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. □

Proposition 19. *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 $a_1 \equiv a_2$. □

7. Chinese Remainder Theorem

The Chinese Remainder Theorem indicates a condition under which we can solve a system of congruences.

Proposition 20. (Chinese Remainder Theorem)
Let $a, b, m, n \in \mathbb{Z}$ *such that* $\gcd(m, n) = 1$*. Then there exists* $c \in \mathbb{Z}$ *with* $0 \leq c < mn$ *such that*

- $c \equiv a \pmod{m}$*;*
- $c \equiv b \pmod{n}$*.*

Proof. There exist $x, y \in \mathbb{Z}$ such that $mx + ny = 1$. Let $c = mxb + nya$. Then

$$c - a = mxb + nya - a = mxb + (ny - 1)a = mxb - mxa,$$

so m divides $c - a$; thus $c \equiv a \pmod{m}$. Also

$$c - b = mxb + nya - b = (mx - 1)b + nya = -nyb + nya,$$

so n divides $c - b$; thus $c \equiv b \pmod{n}$. □

Example 3. Let $m = 104$, $n = 231$, $a = 11$, and $b = 23$. Find $c \in \mathbb{Z}$ with $0 \leq c < mn$ such that $c \equiv a \pmod{m}$ and $c \equiv b \pmod{n}$.

Solution. First we use the Euclidean algorithm to write $mx + yn = d$. We have

$$\begin{aligned}
231 &= 104 \cdot 2 + 23 \\
104 &= 23 \cdot 4 + 12 \\
23 &= 12 \cdot 1 + 11 \\
12 &= 11 \cdot 1 + 1 \\
11 &= 1 \cdot 11 + 0
\end{aligned}$$

Thus

$$\begin{aligned}
1 &= (-1)11 + 12 \\
&= (2)12 + (-1)23 \\
&= (-9)23 + (2)104 \\
&= (20)104 + (-9)231
\end{aligned}$$

That is, $x = 20$, $y = -9$, and $d = 1$,

Now set

$$c = mxb + nya \pmod{24024} = 24971 \pmod{24024} = 947.$$

□

8. Integers Modulo n

Let $n \in \mathbb{Z}$, $n \geq 2$. The equivalence relation $\equiv_n$ partitions the set $\mathbb{Z}$ into blocks, known as *congruence classes modulo* n. For an integer $a \in \mathbb{Z}$, denote its congruence class by $[a]_n$. If the n is understood, we may write this congruence class as $[a]$, or more commonly, as $\overline{a}$.

An element $r \in \mathbb{Z}$ is called a *preferred representative* for $[a]_n$ if $r \in [a]_n$ and $0 \leq r < n$. This is the remainder when any element in $[a]_n$ is divided by n

The division algorithm for the integers tells us that there is a preferred representative for each congruence class. Also, Proposition 19 guarantees that as r ranges over the integers from 0 to $n-1$, the congruence classes $[r]_n$ are distinct. Thus there are exactly n equivalence classes, modulo n. Henceforth, whenever we refer to $\mathbb{Z}_n$, assume that $n \in \mathbb{Z}$ with $n \geq 2$.

Definition 7. The *ring of integers modulo* n is

$$\mathbb{Z}_n = \{[a]_n \mid a \in \mathbb{Z}\}.$$

That is, $\mathbb{Z}_n$ is the set of equivalence classes modulo n, and $|\mathbb{Z}_n| = n$. For example,

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

Proposition 21. *Define the binary operations on* $\mathbb{Z}_n$*,*

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n \quad \text{and} \quad \cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n,$$

known as addition and multiplication, by

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

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 $a_1 = a_2 + kn$ and $b_1 = b_2 + ln$, 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 $a_1 b_1 \equiv a_2 b_2$. □

Definition 8. The *residue map modulo* n is the function

$$\xi_n : \mathbb{Z} \to \mathbb{Z}_n \quad \text{given by} \quad \xi_n(a) = \overline{a}.$$

Proposition 22. *Let* $n \in \mathbb{Z}$*,* $n \geq 2$*, and consider the residue map* $\xi_n : \mathbb{Z} \to \mathbb{Z}_n$*. Then*

- **(a)** $\xi_n(0) = \overline{0}$ *and* $\xi_n(1) = \overline{1}$*;*
- **(b)** $\xi_n(a + b) = \xi_n(a) + \xi_n(b)$*;*
- **(c)** $\xi_n(ab) = \xi_n(a)\xi_n(b)$*.*

Proof. This is immediate from the definitions of addition and multiplication in $\mathbb{Z}_n$, and the fact that the are well-defined. □

9. Properties of Addition

Proposition 23. *Addition on $\mathbb{Z}_n$ is commutative, associative, admits an identity $\overline{0}$, and admits additive inverses.*

Proof. 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

$$\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a}.$$

To see that $+$ is associative, compute

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

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 $\overline{a} + \overline{-a} = \overline{a-a} = \overline{0}$. □

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

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

In $\mathbb{Z}_n$, we have $n\overline{a} = \overline{na} = \overline{0}$. So, some multiple of $\overline{a}$ is zero; thus there is a smallest positive integer k such that $k\overline{a} = 0$.

Definition 9. Let $\overline{a} \in \mathbb{Z}_n$. Define the *additive order* of $\overline{a}$ to be smallest positive integer k such that $k\overline{a} = \overline{0}$. The additive order of $\overline{a}$ is denoted $\text{ord}_+(\overline{a})$.

Proposition 25. *Let $\overline{a} \in \mathbb{Z}_n$ and let $\text{ord}_+(\overline{a}) = k$. 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). □

Proposition 26. *Let $\overline{a} \in \mathbb{Z}_n$ and let $d = \gcd(a, n)$. Then $\text{ord}_+(\overline{a}) = \frac{n}{d}$.*

Proof. Let $k = \text{ord}(\overline{a})$. Now $\frac{n}{d}\overline{a} = \overline{\frac{na}{d}} = n\overline{\frac{a}{d}} = \overline{0}$; thus $k \mid \frac{n}{d}$.

On the other hand, $k\overline{a} = \overline{0}$, so $ka = nl$ for some $l \in \mathbb{Z}$. Dividing by d gives $k\frac{a}{d} = \frac{n}{d}l$. Thus $\frac{n}{d} \mid k\frac{a}{d}$, and since $\gcd(\frac{a}{d}, \frac{n}{d}) = 1$, we have $\frac{n}{d} \mid k$.

Thus $k \mid \frac{n}{d}$ and $\frac{n}{d} \mid k$, and since both are positive they must be equal. □

Example 4. Let $n = 24$ and $a = 20$. Now $\gcd(a, n) = 4$, so $\text{ord}_+(a) = \frac{24}{4} = 6$. Indeed, $6 \cdot 20 = 120$ is the smallest multiple of 20 which is divisible by 24.

Example 5. Let $p = 7$ and consider $\mathbb{Z}_p$. The order of every nonzero element is 7.

10. Properties of Multiplication

Proposition 27. *Multiplication on $\mathbb{Z}_n$ is commutative and associative, with identity element $\overline{1}$. Furthermore, multiplication distributes over addition.*

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

To see that multiplication is commutative, compute

$$\overline{a} \cdot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \cdot \overline{a}.$$

To see that multiplication is associative, compute

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

To see that $\overline{1}$ is a multiplicative identity, compute $\overline{a} \cdot \overline{1} = \overline{a \cdot 1} = \overline{a} = \overline{1 \cdot a} = \overline{1} \cdot \overline{a}$.

To see the multiplication distributes over addition, compute

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

□

Proposition 28. *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 $\mathbb{Z}_n$, $\overline{a} \cdot \overline{0} = \overline{a \cdot 0} = \overline{0} = \overline{0 \cdot a} = \overline{0} \cdot \overline{a}$. □

Definition 10. Let $n \in \mathbb{Z}$, $n \geq 2$, and let $\overline{a} \in \mathbb{Z}_n$. We say that $\overline{a}$ is *invertible* in $\mathbb{Z}_n$ if there exists an element $\overline{b} \in \mathbb{Z}_n$ such that $\overline{a} \cdot \overline{b} = \overline{1}$.

Proposition 29. *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 $ab + (-k)n = 1$. By Proposition 9, $\gcd(a, n) = 1$.

($\Leftarrow$) 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. □

Example 6. Let $p \in \mathbb{N}$ be a prime number.
Then every nonzero element of $\mathbb{Z}_p$ is invertible, because each nonzero positive integer less than p is relatively prime to p.

Definition 11. Let $n \in \mathbb{Z}$ with $n \geq 2$, and let $\overline{a} \in \mathbb{Z}_n$ be nonzero. We say that $\overline{a}$ is a *zero divisor* if there exists $\overline{b} \in \mathbb{Z}_n$ which is nonzero such that $\overline{a}\overline{b} = \overline{0}$.

Proposition 30. *Let $n \in \mathbb{Z}$ with $n \geq 2$, and let $\overline{a} \in \mathbb{Z}_n$. If $\overline{a}$ is invertible, then $\overline{a}$ is not a zero divisor.*

Proof. Suppose a is invertible, and let $b \in \mathbb{Z}$ such that $ab = 0$. Multiply on the left by a^{-1} to get $a^{-1}ab = a^{-1} \cdot 0$, whence $b = 0$. This shows that a is not a zero divisor, because the only element in $\mathbb{Z}_n$ which can be multiplied with a to produce 0 is 0 itself. □

Example 7. Let $n = 6$; in $\mathbb{Z}_6$, the invertible elements are $\overline{1}$ and $\overline{5}$. The zero divisors are $\overline{2}$, $\overline{3}$, and $\overline{4}$. To see this, consider $\overline{2} \cdot \overline{3} = \overline{6} = 0$, and $\overline{3} \cdot \overline{4} = \overline{12} = 0$.

Proposition 31. *Let $n \in \mathbb{Z}$ with $n \geq 2$, and let $\overline{a} \in \mathbb{Z}_n$ be nonzero. Then $\overline{a}$ is a zero divisor if and only if* $\gcd(a, n) \geq 2$.

Proof. Let $d = \gcd(a, n)$.

Suppose that $d = 1$. Then $\overline{a}$ is invertible by Proposition 29, so $\overline{a}$ is not a zero divisor by Proposition 30.

Suppose that $d \geq 2$. Using arithmetic in $\mathbb{Z}$, the Euclidean algorithm dictates that there exist $x, y \in \mathbb{Z}$ such that $ax + ny = d$. We also have $d \mid n$. Then there exists $b \in \mathbb{Z}$ such that $bd = n$, and since $d \geq 2$, we have $0 < b < n$. Applying the residue map to $ax + ny = d$ gives $\overline{ax} + \overline{ny} = \overline{d}$, and since $\overline{n} = \overline{0}$, we have $\overline{ax} = \overline{d}$. Multiply this equation by $\overline{b}$ to get

$$\overline{ax}\overline{b} = \overline{db} = \overline{n} = \overline{0}.$$

Thus $\overline{a}$ is a zero divisor. □

Definition 12. The *group of units* of $\mathbb{Z}_n$ is

$$\mathbb{Z}_n^* = \{\overline{a} \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}.$$

The *Euler phi function* is defined by $\phi(n) = |\mathbb{Z}_n^*|$.

Thus $\overline{a} \in \mathbb{Z}_n^*$ if and only if $\overline{a}$ is invertible in $\mathbb{Z}_n$. The next proposition says that $\mathbb{Z}_n^*$ is closed under multiplication.

Proposition 32. *Let $n \in \mathbb{Z}$, $n \geq 2$, and let $\overline{a}, \overline{b} \in \mathbb{Z}$ be invertible. Then $\overline{a}\overline{b}$ is invertible.*

Proof. Clearly, $(\overline{a}\overline{b}) = \overline{b}^{-1}\overline{a}^{-1}$, since $(\overline{a}\overline{b})(\overline{b}^{-1}\overline{a}^{-1}) = \overline{a}(\overline{b}\overline{b}^{-1})\overline{a}^{-1} = \overline{a}\overline{a}^{-1} = \overline{1}$. □

For example,

- $\mathbb{Z}_p^* = \{1, \dots, p-1\}$, if p is prime;
- $\mathbb{Z}_6^* = \{1, 5\}$;
- $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$;
- $\mathbb{Z}_{15}^* = \{1, 2, 4, 6, 7, 8, 11, 13, 14\}$.

Definition 13. Let $n \in \mathbb{Z}$, $n \geq 2$, and let $\overline{a} \in \mathbb{Z}_n^*$. The *multiplicative order* of $\overline{a}$, denoted $\text{ord}_*(\overline{a})$ is the smallest positive integer k such that $\overline{a}^k = \overline{1}$.

Example 8. Find $\text{ord}_*(\overline{7})$ in $\mathbb{Z}_{15}^*$.

Solution. We have

$$\overline{7}^2 = \overline{49} = \overline{4};$$
$$\overline{7}^3 = \overline{4} \cdot \overline{7} = \overline{28} = \overline{13};$$
$$\overline{7}^4 = \overline{13} \cdot \overline{7} = \overline{91} = \overline{1}.$$

Thus $\text{ord}_*(\overline{7}) = 4$. □

11. Casting Out n's

The process of *casting out n's* involves subtracting n from a number until one arrives at a number less than n. Clearly, this number is the remainder upon division by n, so it is related to modular arithmetic.

The method of casting out n's, together with decimal notation, led Arabs of 1500 years ago to discover certain divisibility criteria. We demonstrate this in modern notation.

Fix $n \in \mathbb{Z}$ with $n \geq 0$. For $a \in \mathbb{Z}$, let $\overline{a}$ denote the remainder when a is divide by n. The last proposition states that $\overline{a+b} \equiv \overline{a} + \overline{b}$ and $\overline{ab} \equiv \overline{a}\overline{b}$, modulo n.

If $d_0, d_1, \ldots, d_r$ are the digits of $a \in \mathbb{N}$ (where $0 \leq d_i \leq 9$), then

$$a = \sum_{i=0}^{r} d_i \cdot 10^i.$$

The idea of casting out n's revolves around the fact that

$$a \equiv \sum_{i=0}^{r} \overline{d_i} \cdot \overline{10}^i \pmod{n}.$$

Proposition 33. (Casting Out 3's and 9's)
Let $n = 3$ or $n = 9$. Let $a, s \in \mathbb{Z}$ be given by

$$a = \sum_{i=0}^{k} d_i \cdot 10^i \quad \text{and} \quad s = \sum_{i=0}^{k} d_i.$$

Then a is divisible by n if and only if s is divisible by n.

Proof. In $\mathbb{Z}_3$ or $\mathbb{Z}_9$, we have $\overline{10} = \overline{1}$. Thus

$$\overline{a} = \overline{\sum_{i=0}^{k} d_i \cdot 10^i} = \sum_{i=0}^{k} \overline{d_i} \cdot \overline{10}^i = \sum_{i=0}^{k} \overline{d_i} = \overline{s}.$$

So a and s have the same remainder upon division by n, and in particular a is divisible by n if and only if s is divisible by n. □

Proposition 34. (Casting Out 11's)
Let $n = 11$. Let $a, s \in \mathbb{Z}$ be given by

$$a = \sum_{i=0}^{k} d_i \cdot 10^i \quad \text{and} \quad s = \sum_{i=0}^{k} (-1)^i d_i.$$

Then a is divisible by n if and only if s is divisible by n.

Proof. In $\mathbb{Z}_{11}$, we have $10 \equiv -1 \pmod{n}$. Thus

$$\overline{a} = \overline{\sum_{i=0}^{k} d_i \cdot 10^i} = \sum_{i=0}^{k} \overline{d_i} \cdot \overline{10}^i = \sum_{i=0}^{k} \overline{d_i}(\overline{-1})^i = \overline{s}.$$

Thus a is divisible by n if and only if s is divisible by n. □

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

We now turn our attention to the question of when an equation, such as $\overline{14}x = \overline{1}$ or $x^2 + \overline{1} = \overline{0}$, has a solution in $\mathbb{Z}_n$, and how many solutions it has. For example, $\overline{14}x = \overline{1}$ has a solution if and only if $\overline{14}$ 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 explicit technique for finding the inverse $\overline{14}$. 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 $\overline{14}$ in $\mathbb{Z}_{33}$ is $\overline{-7} = \overline{26}$.

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

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

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

13. Exercises

Exercise 1. Let $a, b, c \in \mathbb{N}$ be positive. Show that

(a) $a \mid a$;
(b) $a \mid b$ and $b \mid a$ implies $a = b$;
(c) $a \mid b$ and $b \mid c$ implies $a \mid c$.

Exercise 2. Let $m, n, d \in \mathbb{Z}$ with $d = \gcd(m, n)$. Show that

$$\text{lcm}(m, n) = \frac{mn}{d}.$$

Exercise 3. Construct a proof of the Euclidean Algorithm using Proposition 8 and induction.

Exercise 4. Let $n \in \mathbb{Z}$ with $n \geq 2$. Show that if n is not a prime number, then $\mathbb{Z}_n$ contains zero divisors.

Exercise 5. Let $n \in \mathbb{Z}$ with $n \geq 2$, 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 6. Find the additive order of $\overline{6}$, $\overline{11}$, $\overline{18}$, and $\overline{28}$ in $\mathbb{Z}_{36}$.

Exercise 7. Find $\mathbb{Z}_{48}^*$.

Exercise 8. Find $\phi(100)$.

Exercise 9. Find the multiplicative order of $\overline{10}$ in $\mathbb{Z}_{21}^*$.

Exercise 10. Find the inverse of $\overline{15}$ in $\mathbb{Z}_{49}$.

Exercise 11. Solve the equation $\overline{17}x = \overline{23}$ in $\mathbb{Z}_{71}$.

Exercise 12. Solve the equation $x^2 - \overline{5}x - \overline{2} = \overline{0}$ in $\mathbb{Z}_{11}$.

Exercise 13. Solve the equation $x^2 - \overline{5}x + \overline{4} = 0$ in $\mathbb{Z}_6$.

Exercise 14. Find all square roots of $-\overline{1}$ in $\mathbb{Z}_{101}$.

Department of Mathematics and CSci, Southern Arkansas University
E-mail address: plbailey@saumag.edu