REAL ANALYSIS WITH TOPOLOGY
TOPIC III: INTEGERS

PAUL L. BAILEY

ABSTRACT. The document reviews the main properties of the integers, including the division algorithm, the Euclidean algorithm, and the Fundamental Theorem of Arithmetic, as well as giving several examples of proof by induction. We then move into modular arithmetic.

Modular arithmetic involves computing remainders upon addition and multiplication, and has wide ranging applications.

This is a stripped down version of this documents; we will not use much of number theory in this course, so the theory of modular integers is rephrased without equivalence classes.

1. INTEGERS

The *set of integers*, denoted by $\mathbb{Z}$, consists of the natural numbers, their negatives, and zero. That is,

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

The primary aspects of the integers which illuminate their structure as a set include:

- Integers are closed under addition; if we add two integers, we get another integer.
- Integers are closed under subtraction.
- Integers are closed under multiplication.
- Integers are *not* closed under division; if we divide one integer into another, we get *either* a rational number (which we discuss in the next topic), or we get *two* integers (as we discuss in the next section.
- Integers are *totally ordered* by the relation $\leq$; given two integers, either one is less than the other, or they are equal.
- Integers are *partially ordered* by divisibility. It is this aspect of the integers we wish to explore in this document. We define this now

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 $e \in \mathbb{Z}$.

Date: August 11, 2018.

2. The Division Algorithm

Proposition 1. (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.

3. The Euclidean Algorithm

Proposition 2. (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 3. *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 4. *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 $r = he$ 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, $d = \gcd(m, r)$. □

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

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

Proposition 5. *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 6. *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 5, we conclude that $\gcd(\frac{m}{d}, \frac{n}{d}) = 1$. □

Proposition 7. *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 8. *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 9. *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. □

4. Fundamental Theorem of Arithmetic

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

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

Proposition 10. *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 11. (Euclid's Argument)
Let $p \in \mathbb{Z}$, $p \geq 2$. Then p is prime if and only if

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

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 12. *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 13. (Fundamental Theorem of Arithmetic)
Let $n \in \mathbb{Z}$, $n \geq 2$. Then there exist unique prime numbers $p_1, \dots, p_r$, 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 $p_1, \dots, p_r$ and $q_1, \dots, q_s$ 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. □

5. Integers Modulo n

Definition 6. Let $n \in \mathbb{Z}$ with $n \geq 2$. Let $a, b \in \mathbb{Z}$. We say that *a is congruent to b modulo n*, and write $a \equiv b \pmod{n}$, if the difference $a - b$ is a multiple of n:

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad n \mid (a - b).$$

Definition 7. Let $n \in \mathbb{Z}$ with $n \geq 2$, and let $a \in \mathbb{Z}$. The *congruence class of a modulo n*, denoted $\overline{a}$, is the set of all integers which are congruent to a modulo n:

$$\overline{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\}.$$

Proposition 14. *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 $a_1 \equiv a_2$. $\square$

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

The division algorithm for the integers tells us that there is a preferred representative for each congruence class. Also, Proposition 14 guarantees that as r ranges over the integers from 0 to $n - 1$, the congruence classes $\overline{r}$ are distinct. Thus there are exactly n equivalence classes, modulo n.

Definition 8. The *ring of integers modulo n* is

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

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

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

Henceforth, whenever we refer to $\mathbb{Z}_n$, assume that $n \in \mathbb{Z}$ with $n \geq 2$.

Define the binary operations of addition and multiplication on $\mathbb{Z}_n$ by

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

Definition 9. Let $a, n \in \mathbb{Z}$, $n \geq 2$, and $a \in \mathbb{Z}$. We say that $\overline{a} \in \mathbb{Z}_n$ is *invertible* if there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{n}$.

Proposition 15. *Let $\overline{a} \in \mathbb{Z}_n$. Then $\overline{a}$ is invertible if and only if* $\gcd(a, n) = 1$.

Proof. Apply the Euclidean Algorithm to find the inverse of $\overline{a}$. $\square$

Department of Mathematics - BASIS Scottsdale
Email address: paul.bailey@basised.com