COMPUTATIONAL MATHEMATICS
TOPIC II: INTEGERS

PAUL L. BAILEY

1. Well-Ordering Principle

First we establish a few properties of the integers which we need in order to develop the Euclidean algorithm. 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 nonnegative integers. Then X contains a smallest element; that is, there exists $x_0 \in X$ such that for every $x \in X$, $x \leq x_0$.

Discussion. For the purposes of this class, we accept the Well-Ordering Principle as an axiom of the natural numbers. In a more formal treatment, it is equivalent to the Principle of Mathematical Induction, in the sense that either can be proven from the other, given some reasonable definition of the natural numbers. □

2. The Division Algorithm

Proposition 2 (**Division Algorithm**)**.**
Let $m, n \in \mathbb{Z}$ with $m \neq 0$. There exist unique integers $q, r \in \mathbb{Z}$ such that

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

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

Proof. 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 $r = 0$;
- $n = (-m)(-q) + r$.

□

Date: August 16, 2018.

3. 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 3 (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 4. *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 5. *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 1. Let $n = 210$ and $m = 165$.

(a) Find $d \in \mathbb{Z}$ such that $d = \gcd(n, m)$.

(b) Find $x, y \in \mathbb{Z}$ such that $xm + yn = d$.

Solution. 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", to see how the lifted coefficients are functions of the previous coefficients.

At each stage we have an equation of the form $d = x'm' + y'n'$, which we wish to lift to a previous equation of the form $n = mq + r$, where $m = n'$ and $r = m'$. Thus we have $d = x'r + y'm$, and $r = n - mq$. Plug the second into the first to get

$$\begin{aligned} d &= x'r + y'm \\ &= x'(n - mq) + y'm \\ &= x'n - x'mq + y'm \\ &= (y' - x'q)m + (x')n \\ &= xm + yn \end{aligned}$$

Thus we see that, to obtain our new $d = xm + ym$, we need to set

$$x = y' - x'q \qquad \text{and} \qquad y = x'.$$

4. Relative Primality

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

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

Proposition 6. *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 7. *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 6, we conclude that $\gcd(\frac{m}{d}, \frac{n}{d}) = 1$. □

Proposition 8. *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 9. *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 10. *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 11. *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 12 (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 13. *Let $n \in \mathbb{Z}$ with $n \geq 2$. There exists a prime p such that $p \mid n$.*

Proof. Assume the proposition is false; then there exists a smallest positive integer n which is not divisible by a prime. But then $n = ab$ for some $a, b \in \mathbb{Z}$ where $1 < a < n$, so a is divisible by a prime, which in turns must divide n. □

Proposition 14. (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. Mathematical Exercises

Exercise 1. In each case, find $d = \gcd(m, n)$, and find $x, y \in \mathbb{Z}$ such that

$$mx + ny = d.$$

(a) $m = 75$, $n = 300$
(b) $m = 123$, $n = 248$
(c) $m = 528$, $n = 71$

Exercise 2. 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 $a \mid c$.

7. Programming Exercises

Write all programs using the C programming language and the standard library.

Program 1. Write a function which takes $m, n \in \mathbb{Z}$ and uses the Euclidean Algorithm to find $d = \gcd(m, n)$.

Program 2. Write a function which takes $m, n \in \mathbb{Z}$ and uses the Euclidean Algorithm to find $d = \gcd(m, n)$ and $x, y \in \mathbb{Z}$ such that $xm + yn = d$.

Hint. The computation of $\gcd(m, n)$ does not require the remembrance of the previous equations; however, the computation of the x and y does. You can either use an array to store the remainders, or you can use recursion. □

Program 3. Write a function which takes $m, n \in \mathbb{Z}$ and finds $l = \operatorname{lcm}(m, n)$.

Program 4. Write a program to find the first `MAX` prime numbers.

Program 5. Write a program which prints the prime factors of a given integer.

Department of Mathematics and CSci, BASIS Scottsdale
Email address: `plbailey@saumag.edu`