NUMERICAL ANALYSIS TOPIC I
THE EUCLIDEAN ALGORITHM

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. This follows from the principle of induction, which we assume.

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 $x \in X$, $x \leq x_0$.

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 $|Y|$. If $|Y| = 1$, then Y contains exactly one element, which is vacuously the smallest member of Y.

Now assume that $|Y| = n$. 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 $x_2 \notin Z$, $|Z| < n$, 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. □

Date: January 28, 2004.

2. Division Algorithm

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

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

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, $r < m$, 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 $q_1 = q_2$. □

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.

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 $d = e$. □

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. Prime Decomposition Algorithm

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

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

Exercise 4. Let $a, p \in \mathbb{Z}$ such that p is prime.
Show that $\gcd(a, p) = 1$ or $\gcd(a, p) = p$.

Exercise 5. Show that there are infinitely many prime integers.
(Hint: assume there are only finitely many, multiply them, and add 1.)

Proposition 4 (Fundamental Theorem of Arithmetic)**.** *Let $n \in \mathbb{Z}$. Then there exist unique prime numbers $p_1 < \cdots < p_r$, positive integers $a_1, \ldots, a_r$, and unique $u \in \{\pm 1\}$ such that*

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

Proof. If $n < 0$, let $u = -1$; otherwise let $u = 1$. Let

$$X = \{m \in \mathbb{Z} \mid 1 < m \leq un \text{ and } m \mid n\}$$

Let $p = \min(X)$. Clearly, p is prime. If $n = up$, we are done. Otherwise, $n = upk$ for some $k \in \mathbb{Z}$. By strong induction, there exist $q_1 < \ldots, q_s$ and $b_1, \ldots, b_s$ such that $k = \prod_{i=1}^{s} q_i^{b_i}$. If $p = q_1$, set $p_i = q_i$, $a_1 = b_1 + 1$, and $a_i = b_i$ for $i > 1$, and $r = s$; otherwise set $p_1 = p$, $p_{i+1} = q_i$, $a_1 = 1$, and $a_{i+1} = b_i$, and $r = s + 1$. Now $n = u \prod_{i=1}^{r} p_i^{a_i}$. □

Program 1. Write a program to find the first `MAX` prime numbers.

Program 2. Write a program to find the gcd of two integers by finding the common primes, using a table of primes generated by Program 1.

4. Euclidean Algorithm

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

Proposition 5. *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. □

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*.

Program 3. Write a function which takes $m, n \in \mathbb{Z}$ and uses the Euclidean Algorithm to find $d = \gcd(m, n)$.

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

Let's briefly analyse 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 $d = xm + yn$.

Program 4. 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. □

Department of Mathematics & Computer Science, Southern Arkansas University
E-mail address: `plbailey@saumag.edu`