HISTORY OF MATHEMATICS MATHEMATICAL TOPIC IV THE EUCLIDEAN ALGORITHM

PAUL L. BAILEY

1. Induction and the Well-Ordering Principle

First we establish a few properties of the integers which we need in order to develop the Euclidean algorithm. We start with the natural numbers $\mathbb{N} = \{1, 2, 3, ...\}$, and accept the Peano Axioms as a characterization of \mathbb{N} . The primary axiom is stated below.

Proposition 1. Peano's Axiom

Let $S \subset \mathbb{N}$. If (a) $1 \in S$, and (b) $n \in S \Rightarrow n+1 \in S$, then $S = \mathbb{N}$.

From this, the Well-Ordering Principle follows.

Proposition 2. Well-Ordering Principle

Let $X \subset \mathbb{N}$ be a nonempty set of positive integers. Then X contains a smallest, element; that is, there exists $a \in X$ such that for every $x \in X$, $a \leq x$.

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

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

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

Since 1 is less than every natural number, 1 is less than every natural number in X. Thus $1 \in X$.

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, $S = \mathbb{N}$.

Date: October 24, 2008.

2. DIVISION ALGORITHM

Proposition 3. Division Algorithm for Integers

Let $m, n \in \mathbb{Z}$. There exist unique integers $q, r \in \mathbb{Z}$ such that

n = qm + r and $0 \le r < m$.

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 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 $n = q_1m + r_1$ and $n = q_2m + r_2$, where $q_1, r_1, q_2, r_2 \in \mathbb{Z}$, $0 \le r_1 < m$, and $0 \le r_2 < m$. 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 $q_1 = q_2$. \Box

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 | 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 4. 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 $0 \le r < d$. 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.

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 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 $0 \le r < m$. Then gcd(n, m) = gcd(m, r).

Proof. Let $d_1 = \text{gcd}(n, m)$ and $d_2 = \text{gcd}(m, r)$. 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 $d_1w = n$, $d_1x = m$, $d_2y = m$, and $d_2z = r$.

Then $d_1w = qd_1x + r$, so $r = d_1(w - qx)$, and $d_1 | r$. Also $d_1 | m$, so $d_1 | d_2$ by definition of gcd.

On the other hand, $n = qd_2y + d_2z = d_2(qy + z)$, 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 $0 \le r < m$. Let $r_0 = n, r_1 = m, r_2 = r$, and $q_1 = q$. Then the equation becomes $r_0 = r_1q_1 + r_2$. Repeat the process by writing $m = rq_2 + r_3$, which is the same as $r_1 = r_2q_2 + r_3$, with $0 \le r_3 < r_2$. Continue in this manner, so in the *i*th stage, we have $r_{i-1} = r_iq_i + r_{i+1}$, with $0 \le r_{i+1} < r_i$. 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, $15 = 210 \cdot 4 + 165 \cdot (-5)$.

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.

4. Fundamental Theorem of Arithmetic

Definition 3. An integer $p \ge 2$, is called *prime* if

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

An integer $n \ge 2$ is called *composite* if it is not prime.

Proposition 6. Let $p \in \mathbb{Z}$, $p \geq 2$. Then p is prime if and only if

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

Proof.

(⇒) 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. \Box

Remark 1 (Euclid's Statement). A composite number is measured by some prime.

Euclid's Proof. Infinite regression, similar to its use in the Euclidean algorithm. \Box

Proposition 7. Let n be a composite number. Then there exists a prime p such that $p \mid n$.

Modern Proof. Since n is composite, there exist $a, b \in \mathbb{N}$ such that 1 < a, b < n and n = ab. By induction, there exists a prime p such that $p \mid b$. Thus $p \mid n$.

Remark 2 (Euclid's Statement). If a number be the least that is measured by prime numbers, it will not be measured by any other prime number except those originally measuring it.

Proposition 8 (Fundamental Theorem of Arithmetic). Let $n \in \mathbb{Z}$, $n \geq 2$. Then there exist unique prime numbers $p_1 < \cdots < p_r$ and positive integers a_1, \ldots, a_r such that

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

Proof. Let

$$X = \{ m \in \mathbb{Z} \mid m \ge 2 \text{ and } m \mid n \}$$

Let $p = \min(X)$. Clearly, p is prime. If n = p, we are done. Otherwise, n = pk for some $k \in \mathbb{Z}$. By strong induction, there exist $q_1 < \cdots < q_s$ 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 $n = u \prod_{i=1}^{r} p_i^{a_i}$.

5. Infinitude of Primes

Remark 3. Let A be a set. We say that A *infinite* if there exists an injective function $\mathbb{N} \to A$. We say that A is *finite* if there exists a surjective function $\{1, \ldots, n\} \to A$, for some $n \in \mathbb{N}$.

Remark 4 (Euclid's Statement). The prime numbers are more than any assigned multitude of prime numbers.

Proposition 9. Let $P = \{n \in \mathbb{Z} \mid n \text{ is prime}\}$. Then P is infinite.

Proof. Suppose that P is finite; then $P = \{p_1, \ldots, p_n\}$ for some primes p_i . Set

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

Since $n > p_i$ for all *i*, *n* cannot be prime; thus *n* is composite. Therefore there exists $p \in P$ such that $p \mid n$. This implies that $p \mid 1$, a contradiction. \Box

Department of Mathematics and CSci, Southern Arkansas University $E\text{-}mail \ address: plbailey@saumag.edu$