CRYPTOGRAPHY TOPIC III
INTEGER ARITHMETIC

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. Our primary interest in reviewing this material is to lay the groundwork for the understanding of the modular arithmetic and primality.

The important material for cryptography includes ALL the definitions, (which should be memorized), Proposition 5 and Proposition 7, and a general respect for the subject in general.

1. The Well-Ordering Principle

The *natural numbers* are the set $\mathbb{N} = \{0, 1, 2, 3, \dots\}$, 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, the Well-Ordering Principle follows.

Proposition 2. (Well-Ordering Principle)
Let $X \subset \mathbb{N}$ be a nonempty set of natural numbers. 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 $X = \varnothing$. 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, $S = \mathbb{N}$. □

Date: September 6, 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 $m \in \mathbb{N}$ 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. 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 for Integers)
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 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 $r = n$. 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. □

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 $n = km$.

The next proposition says that the relation "divides" is a partial order on the set of positive integers.

Proposition 6. *Let $a, b, c \in \mathbb{N}$ be positive. Then*

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

Proof. Exercise. □

Definition 2. Let $m, n \in \mathbb{Z}$ be nonzero. 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. $e \mid m$ and $e \mid n$ implies $e \mid d$, for all $e \in \mathbb{Z}$.

Proposition 7. (Euclidean Algorithm for Integers)
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 $d = e$. □

Proposition 8. *Let $m, n \in \mathbb{Z}$ be nonzero and suppose that there exist integers $x, y \in \mathbb{Z}$ such that $xm + yn = 1$. Then $\gcd(m, n) = 1$.*

Proof. Exercise. □

Proposition 9. *Let $m, n \in \mathbb{N}$ be nonzero and suppose that $m \mid n$. Then* $\gcd(m, n) = m$.

Proof. Exercise. □

5. Euclidean Algorithm in Practice

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

Proposition 10. *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 requiring 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, $d = \gcd(m, r)$. □

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.

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

6. Fundamental Theorem of Arithmetic

Definition 3. 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 11. (Euclid's Argument)
Let $p \in \mathbb{Z}$, $p \geq 2$. Then p is prime if and only if

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

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. (The 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 see that we can continue this process until n is completely factored into 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. □

Proposition 14. *Let $P = \{n \in \mathbb{Z} \mid n \text{ is prime}\}$. Then P is infinite.*

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

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

Clearly $n > 1$, so n is divisible by some prime p, and $p = p_i$ for some i. Thus p divides n and $\prod_{i=1}^{r} p_i$, so p divides $1 = n - \prod_{i=1}^{r} p_i$. But 1 cannot be divisible by a prime, so we have a contradiction. □

We will have use for the following property later.

Proposition 15. *Let $a, b, c \in \mathbb{Z}$ be nonzero such that $\gcd(a, b) = 1$. If $a \mid bc$, then $a \mid c$.*

Proof. Suppose that $a \mid bc$. Without loss of generality, we may assume that a, b, c are positive; in this case, we may proceed by induction on a.

If $a = 1$, the proposition is clear, so assume that $a \geq 2$. In this case, there exists such prime p such that $p \mid a$, which implies that $p \mid bc$. By Euclid's argument, either $p \mid b$ or $p \mid c$. But if $p \mid b$, then $p \mid \gcd(a, b) = 1$, which is impossible since $p \geq 2$. Thus $p \mid c$.

Now $a = px$ and $c = py$ for some $x, y \in \mathbb{Z}$, and since $a \mid bc$, we have $bc = az$ for some $z \in \mathbb{Z}$. Thus $bpy = pxz$, whence $by = xz$, and $x \mid by$.

Let $e = \gcd(x, b)$; then $e \mid x$, so $e \mid a$. Also, $e \mid b$, so $e \mid \gcd(a, b) = 1$; this shows that $\gcd(x, b) = 1$.

Now $x < a$, $\gcd(x, b) = 1$, and $x \mid by$. By induction, $x \mid y$, so $y = kx$ for some $k \in \mathbb{Z}$. Thus $a = px$ and $c = pkx = pxk = ak$. Therefore $a \mid c$. □

7. Exercises

Exercise 1. Use induction to prove that, for all $n \in \mathbb{N}$,

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Exercise 2. Use induction to prove that, for all $n \in \mathbb{N}$,

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}.$$

Exercise 3. Use induction to prove that, for all $n \in \mathbb{N}$,

$$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}.$$

Exercise 4. 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 5. Let $m, n \in \mathbb{Z}$ be nonzero and suppose that there exist integers $x, y \in \mathbb{Z}$ such that $mx + ny = 1$. Show that $\gcd(m, n) = 1$.

Exercise 6. Let $m, n \in \mathbb{N}$ be nonzero and suppose that $m \mid n$.
Show that $\gcd(m, n) = m$.

Exercise 7. Let $m, n \in \mathbb{Z}$ be nonzero. Use strong induction to show that there exist $x, y, d \in \mathbb{Z}$ with $d = \gcd(m, n)$ such that

$$mx + ny = d.$$

Exercise 8. 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) $m = 528$, $n = 71$

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