2. Integers and Algorithms

2.1. Euclidean Algorithm. Euclidean Algorithm. Suppose a and b are integers with $a \geq b > 0$.

(1) Apply the division algorithm: $a = bq + r$, $0 \leq r < b$.
(2) Rename b as a and r as b and repeat until $r = 0$.

The last nonzero remainder is the greatest common divisor of a and b.

The Euclidean Algorithm depends upon the following lemma.

LEMMA 2.1.1. *If* $a = bq + r$, *then* $\mathrm{GCD}(a, b) = \mathrm{GCD}(b, r)$.

PROOF. We will show that if $a = bq + r$, then an integer d is a common divisor of a and b if, and only if, d is a common divisor of b and r.

Let d be a common divisor of a and b. Then $d|a$ and $d|b$. Thus $d|(a - bq)$, which means $d|r$, since $r = a - bq$. Thus d is a common divisor of b and r.

Now suppose d is a common divisor of b and r. Then $d|b$ and $d|r$. Thus $d|(bq + r)$, so $d|a$. Therefore, d must be a common divisor of a and b.

Thus, the set of common divisors of a and b are the same as the set of common divisors of b and r. It follows that d is the *greatest* common divisor of a and b if and only if d is the greatest common divisor of b and r. □

Discussion

The fact that the Euclidean algorithm actually gives the greatest common divisor of two integers follows from the division algorithm and the equality in Lemma 2.1.1. Applying the division algorithm repeatedly as indicated yields a sequence of remainders $r_1 > r_2 > \cdots > r_n > 0 = r_{n+1}$, where $r_1 < b$. Lemma 2.1.1 says that

$$\mathrm{GCD}(a, b) = \mathrm{GCD}(b, r_1) = \mathrm{GCD}(r_1, r_2) = \cdots = \mathrm{GCD}(r_{n-1}, r_n).$$

But, since $r_{n+1} = 0$, r_n divides r_{n-1}, so that

$$\mathrm{GCD}(r_{n-1}, r_n) = r_n.$$

Thus, the last nonzero remainder is the greatest common divisor of a and b.

EXAMPLE 2.1.1. *Find* GCD *(1317, 56).*

$$\begin{aligned} 1317 &= 56(23) + 29 \\ 56 &= 29(1) + 27 \\ 29 &= 27(1) + 2 \\ 27 &= 2(13) + 1 \\ 2 &= 1(2) + 0 \end{aligned}$$

GCD *(1317,56)=1*

Example 2.1.1 shows how to apply the Euclidean algorithm. Notice that when you proceed from one step to the next you make the new dividend the old divisor (replace a with b) and the new divisor becomes the old remainder (replace b with r). Recall that you can find the quotient q by dividing b into a on your calculator and rounding *down* to the nearest integer. (That is, $q = \lfloor a/b \rfloor$.) You can then solve for r. Alternatively, if your calculator has a **mod** operation, then $r = \mathbf{mod}(a, b)$ and $q = (a - r)/b$. Since you only need to know the remainders to find the greatest common divisor, you can proceed to find them recursively as follows:

Basis. $r_1 = a \,\mathbf{mod}\, b$, $r_2 = b \,\mathbf{mod}\, r_1$.

Recursion. $r_{k+1} = r_{k-1} \,\mathbf{mod}\, r_k$, for $k \geq 2$. (Continue until $r_{n+1} = 0$ for some n.)

2.2. GCD's and Linear Combinations.

THEOREM 2.2.1. *If $d = \mathrm{GCD}(a, b)$, then there are integers s and t such that*

$$d = as + bt.$$

Moreover, d is the smallest positive integer that can be expressed this way.

Discussion

Theorem 2.2.1 gives one of the most useful characterizations of the greatest common divisor of two integers. Given integers a and b, the expression $as + bt$, where s and t are also integers, is called a **linear combination** of a and b.

EXERCISE 2.2.1. *Prove that if a, b, s, t, and d are integers such that $d|a$ and $d|b$, then $d|(as + bt)$.*

The Euclidean Algorithm can, in fact, be used to provide the representation of the greatest common divisor of a and b as a linear combination of a and b. Here is how it would work for the example in Example 2.1.1.

EXAMPLE 2.2.1. *Express* $1 = \text{GCD}(1317, 56)$ *as a linear combination of 1317 and 56.*

Solution: We work backwards using the equations derived by applying the Euclidean algorithm in example 2.1.1, expressing each remainder as a linear combination of the associated divisor and dividend:

$$\begin{aligned}
1 &= \underline{27} - 13 \cdot \underline{2} && \textit{linear combination of 2 and 27}\\
1 &= \underline{27} - 13(\underline{29} - \underline{27} \cdot 1) && \textit{substitute } \underline{2} = \underline{29} - \underline{27}(1)\\
1 &= 14 \cdot \underline{27} - 13 \cdot \underline{29} && \textit{linear combination of 27 and 29}\\
1 &= 14(\underline{56} - 1 \cdot \underline{29}) - 13 \cdot \underline{29} && \textit{substitute } \underline{27} = \underline{56} - 1 \cdot \underline{29}\\
1 &= 14 \cdot \underline{56} - 27 \cdot \underline{29} && \textit{linear combination of 29 and 56}\\
1 &= 14 \cdot \underline{56} - 27(\underline{1317} - 23 \cdot \underline{56}) && \textit{substitute } \underline{29} = \underline{1317} - 23 \cdot \underline{56}\\
1 &= 635 \cdot \underline{56} - 27 \cdot \underline{1317} && \textit{linear combination of 56 and 1317}
\end{aligned}$$

(The dividends, divisors, and remainders have been underlined.)

So $\text{GCD}(1317, 56) = 1 = 1317(-27) + 56(635)$.

Theorem 2.2.1 can be proved by mathematical induction following the idea in the preceding example.

Proof of Theorem 2.2.1. Suppose a and b are integers. We may assume a and b are positive, since $\text{GCD}(a, b) = \text{GCD}(\pm a, \pm b)$. The Euclidean algorithm uses the division algorithm to produce a sequence of quotients and remainders as follows:

$$\begin{aligned}
a &= bq_1 + r_1\\
b &= r_1q_2 + r_2\\
r_1 &= r_2q_3 + r_3\\
&\vdots\\
r_{n-2} &= r_{n-1}q_n + r_n\\
r_{n-1} &= r_nq_{n+1} + 0
\end{aligned}$$

where r_n is the last nonzero remainder. We will use the second principle of mathematical induction to prove that r_k is a linear combination of a and b for $1 \leq k \leq n$.

1. Basis Step ($k = 1$). $r_1 = a - bq_1 = a(1) + b(-q_1)$.
2. Induction Step. Suppose r_i is a linear combination of a and b for $1 \leq i \leq k$. For $1 \leq k \leq n$ we have

$$r_{k+1} = r_{k-1} - r_kq_{k+1}$$

(where $r_0 = b$ when $k = 1$). By the inductive hypothesis r_{k-1} and r_k are linear combinations of a and b. (This works for $k = 1$, since $r_0 = b$ is trivially a linear combination of a and b.) Write

$$r_{k-1} = as_1 + bt_1$$

and

$$r_k = as_2 + bt_2$$

for integers s_1, t_1, s_2, t_2, and substitute into the equation above:

$$r_{k+1} = (as_1 + bt_1) - (as_2 + bt_2)q_{k+1} = a(s_1 - s_2q_{k+1}) + b(t_1 - t_2q_{k+1}).$$

Thus, r_{k+1} is a linear combination of a and b. By the second principle of mathematical induction, r_n is a linear combination of a and b. But r_n is the greatest common divisor of a and b. This proves the first part of the theorem.

Next, we show that d is the smallest positive integer expressible as a linear combination of a and b. Suppose a positive integer c can be expressed as a linear combination of a and b:

$$c = ax + by$$

for integers x and y. Since $d|a$ and $d|b$, then $d|c$, which implies $d \leq c$. □

Here is an alternative proof of Theorem 2.2.1 that does not use the Euclidean algorithm.

Second proof of Theorem 2.2.1. Let S be the set of all positive integers that can be expressed as a linear combination of the positive integers a and b. Clearly $S \neq \emptyset$, since $a, b \in S$. By the well-ordering principle S has a least element d. We will prove by contradiction that $d|a$ and $d|b$.

If $d \nmid a$, then use the division algorithm to get integers q and r such that

$$a = dq + r,$$

where $0 < r < d$. Since both a and d are linear combinations of a and b, then $r = a - dq$ is also. But this means that $r \in S$, contradicting the fact that d is the smallest member of S.

Similarly, one shows that $d|b$.

If c is a divisor of a and b, then c divides any linear combination of a and b; hence, $c|d$. Thus, $d = \text{GCD}(a, b)$. □

EXERCISE 2.2.2. *Prove that if p is a prime number and n is an integer that is not divisible by p, then there are integers s and t such that $ps + nt = 1$. [First show that* $\text{GCD}(p, n) = 1$.*]*

EXERCISE 2.2.3. *Prove that if 1 is a linear combination of a and b, then* $\mathrm{GCD}(a, b) = 1$.

2.3. Uniqueness of Prime Factorization.

LEMMA 2.3.1. *If* $\mathrm{GCD}(a, b) = 1$ *and* $a|bc$, *then* $a|c$.

PROOF. Assume $\mathrm{GCD}(a, b) = 1$ and $a|bc$. Write $1 = as + bt$ for integers s and t. Multiply both sides by c:

$$c = acs + bct.$$

Since $a|bc$, a divides this linear combination

$$a(cs) + (bc)t = c$$

of a and bc.

□

THEOREM 2.3.1. *Suppose a and b are integers and p is a prime number. If $p|ab$, then $p|a$ or $p|b$.*

PROOF. We will prove the equivalent statement: if $p|ab$ and $p \nmid a$, then $p|b$. (You should convince yourself that the two propositional forms $P \to (Q \vee R)$ and $(P \wedge \neg Q) \to R$ are equivalent.)

Suppose $p|ab$ and $p \nmid a$. Then $\mathrm{GCD}(p, a) = 1$. By the Lemma 1, $p|b$. □

Discussion

Theorem 2.3.1 is very useful in deciding how prime factors are distributed in a product of two integers. For example, we gave an indirect proof in Module 3.2 that if the product of two integers x and y is even, then either x is even or y is even. As we hinted there, a direct proof is possible, and Theorem 2.3.1 provides just the right information to make it work.

EXERCISE 2.3.1. *Use Theorem 2.3.1 to give a direct proof that if the product of two integers x and y is even, then either x is even or y is even.*

EXERCISE 2.3.2. *Use mathematical induction to prove the following generalization of Theorem 2.3.1. Suppose $a_1, a_2, ..., a_n$ are integers and p is a prime number. If $p|a_1a_2 \cdots a_n$, then $p|a_i$ for some $i = 1, 2, ..., n$. [Hint: The induction step has two cases.]*

EXERCISE 2.3.3. *Use Lemma 2.3.1 to prove that if k, ℓ, and m are positive integers such that $k|m$, $\ell|m$, and k and ℓ are relatively prime, then the product $k\ell|m$.*

EXERCISE 2.3.4. *Suppose a and b are positive integers, $d = \mathrm{GCD}(a, b)$, $a = dk$, and $b = d\ell$. Prove that k and ℓ are relatively prime. [Hint: Show that 1 can be expressed as a linear combination of k and ℓ.]*

We can now give a proof of Theorem 6 of *Module 5.1 Integers and Division*: If a and b are positive integers, then $ab = \mathrm{GCD}(a, b) \cdot \mathrm{LCM}(a, b)$.

Proof of Theorem 6, Module 5.1. Let $d = \mathrm{GCD}(a, b)$. Write $a = dk$, $b = d\ell$, where k and ℓ are positive integers, which, by Exercise 2.3.4, are relatively prime. Then

$$ab = (dk)(d\ell) = d \cdot (k\ell d) = \mathrm{GCD}(a, b) \cdot (k\ell d).$$

We will succeed once we show that $k\ell d = \mathrm{LCM}(a, b)$. We will prove this by contradiction.

Suppose $m = \mathrm{LCM}(a, b)$ and $m < k\ell d$. Observe that $k\ell d = (dk)\ell = a\ell$ and $k\ell d = (d\ell)k = bk$. That is, both a and b divide $k\ell d$; hence, their least common multiple m does also.

Since $k|a$ and $\ell|b$, k and ℓ both divide m; hence, by Exercise 2.3.3, the product $k\ell|m$.

> [Aside: We also know that d divides m, so it is tempting to assert that $k\ell d$ also divides m. But we can't use Exercise 2.3.3 to conclude this, since d may not be relatively prime to either k or ℓ. Can you give an example where d divides both k and ℓ?]

Thus $m = k\ell x$ for some positive integer x, and $x < d$, by hypothesis. Since $m|k\ell d$, $x|d$. Write $d = xy$, where y is an integer > 1. Now:

$a = dk = xyk|m = k\ell x$, so $y|\ell$.

$b = d\ell = xy\ell|m = k\ell x$, so $y|k$.

This implies that k and ℓ are not relatively prime, since $y > 1$. Thus, the assumption $m < k\ell d$ is false, and so $m = k\ell d$. □

This generalization of Theorem 2.3.1 can be used to prove the uniqueness of prime factorizations asserted in the Fundamental Theorem of Arithmetic (Module 5.1): If n is a positive integer greater than 1, then n can be written uniquely as a product of prime numbers where the factors appear in nondecreasing order.

Proof of uniqueness of prime factorization. We have already shown that we can write any integer $n > 1$ as a product

$$n = p_1 p_2 \cdots p_k,$$

where each p_i is prime. By reordering the factors, if necessary, we can always assume that

$$p_1 \leq p_2 \leq \cdots \leq p_k.$$

We will prove by induction on k that if an integer $n > 1$ has a factorization into k primes, $k \geq 1$, then the factorization is unique.

1. Basis Step ($k = 1$). In this case $n = p_1$ is prime, and so it has no other factorization into primes.
2. Induction Step. Assume that every integer that can be factored into k primes has a unique factorization. Suppose

   $$n = p_1 p_2 \cdots p_k p_{k+1},$$

   where each p_i is prime and

   $$p_1 \leq p_2 \leq \cdots \leq p_k \leq p_{k+1}.$$

   Suppose n has another prime factorization

   $$n = q_1 q_2 \cdots q_\ell,$$

   where each q_j is prime (possibly, $\ell \neq k+1$) and

   $$q_1 \leq q_2 \leq \cdots \leq q_\ell.$$

   By the generalization of Theorem 2.3.1 in Exercise 2.3.2, since $p_1 | n = q_1 q_2 \cdots q_\ell$, then $p_1 | q_j$ for some j. But q_j is also prime, so

   $$p_1 = q_j \geq q_1.$$

   On the other hand, since $q_1 | p_1 p_2 \cdots p_k p_{k+1}$, then $q_1 | p_i$ for some i, and since p_i is prime,

   $$q_1 = p_i \geq p_1.$$

   But if $p_1 \geq q_1$ and $q_1 \geq p_1$, then $p_1 = q_1$. Thus we can cancel the first factor from both sides of the equation

   $$p_1 p_2 \cdots p_k p_{k+1} = q_1 q_2 \cdots q_\ell$$

   to get

   $$p_2 \cdots p_k p_{k+1} = q_2 \cdots q_\ell.$$

   The integer on the left-hand side of this equation has a prime factorization using k primes. By the induction hypothesis, this factorization is unique. This means that $\ell = k+1$ and

   $$p_2 = q_2,\ p_3 = q_3,\ \ldots,\ p_{k+1} = q_{k+1}.$$

   Thus, $p_i = q_i$ for $1 \leq i \leq k+1$, and the factorization of n is unique.

By the first principle of mathematical induction, every integer greater than one has a unique prime factorization. □