CS/Math 240: Supplemental Handout on Divisibility and Primes

Dalibor Zelený

2/19/2011

1 Division Algorithm

Think back to the time you were dividing one number by another at school. At some point, you learned a procedure for dividing n by some number k. This method gave you a quotient q and a remainder r.

Combining n, k, q and r into one equation gives us

$$n = qk + r \quad \text{where} \quad 0 \leq r < k. \tag{1}$$

For example, $70 \div 15 = 4$ with remainder 10 (notice that the remainder is indeed between 0 inclusive and 15 exclusive), and we can write $70 = 4 \cdot 15 + 10$.

In fact, there is exactly one pair of q and r that satisfies (1) for any given n and k.

Theorem 1. *For any integers n and k, there exist unique integers q and r that satisfy* (1).

Proof. Let n and k be given. We first show that there exists a pair of integers q and r that satisfy (1). Afterwards, we show that if two such pairs exist, say q_1 and q_2, and r_1 and r_2, then $q_1 = q_2$ and $r_1 = r_2$.

Let's start by sketching a proof that there are integers q and r that satisfy (1). We claim that there is an integer l such that $kl < n < k(l+1)$. Indeed, take $l = \lfloor n/k \rfloor$. Then pick $q = l$ and $r = n - kl$ as our integers that satisfy (1). One could use induction to prove this more formally.

Now we show rigorously that if $n = q_1 k + r_1$ and $n = q_2 k + r_2$ with $0 \leq r_1 < k$ and $0 \leq r_2 < k$, then $q_1 = q_2$ and $r_1 = r_2$.

Since $n = q_1 k + r_1$ and $n = q_2 k + r_2$, we have $q_1 k + r_1 = q_2 k + r_2$, which we rewrite as

$$(q_1 - q_2)k + r_1 = r_2. \tag{2}$$

We know that $0 \leq r_2 < k$, so

$$0 \leq (q_1 - q_2)k + r_1 < k \tag{3}$$

We argue by cases that (3) implies $q_1 = q_2$.

Case 1: $q_1 < q_2$. Since q_1 and q_2 are integers, $q_1 - q_2 \leq -1$, so $(q_1 - q_2)k \leq k$. But then the first inequality in (3) implies that $0 \leq -k + r_1$, so $k \leq r_1$. This contradicts the fact that $r_1 < k$, so we cannot have $q_1 < q_2$.

Case 2: $q_1 > q_2$. Since q_1 and q_2 are integers, $q_1 - q_2 > 1$, so $(q_1 - q_2)k \geq k$. Then the second inequality in (3) implies that $k + r_1 < k$, so $r_1 < 0$. This contradicts the fact that $r_1 \geq 0$, so we cannot have $q_1 > q_2$.

Case 3: Since Case 1 or Case 2 cannot happen, it follows that $q_1 = q_2$. Then (2) simplifies to $r_1 = r_2$. This completes the proof because we showed that both $q_1 = q_2$ and $r_1 = r_2$. □

2 Primes

We start our discussion of primes by introducing the notion of divisibility.

Definition 1 (Divisibility)**.** *Let $n = qk + r$ with $0 \leq r < k$. When $r = 0$, we say that k* divides *n, and write $k \mid d$ to denote this fact. We also say that k is a* divisor *of n. If $r \neq 0$, we say that k* does not divide *n, and write $k \nmid n$.*

And now we can state what a prime number is.

Definition 2. *An integer $n \geq 2$ is called* prime *if its only divisors are 1 and n itself. Otherwise n is called* composite*, and it has a divisor that is strictly between 1 and n.*

Recall that every integer can be written as a product of primes. We write the *prime factorization* of n as $p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, where $p_1, p_2, \ldots, p_r$ are distinct primes, and the exponents $e_1, e_2, \ldots, e_r$ are positive integers.

We proved in lecture that every integer has a prime factorization, but include the proof on this handout for the sake of completeness. As we shall see later, the prime factorization is, in fact, unique.

Theorem 2. *Every integer $n \geq 2$ can be written as a product of primes.*

Proof. We give a proof by strong induction on n.

Consider the statement $P(n)$: n can be written as a product of primes. We prove $P(2)$ as the base case, and show for all $n \geq 2$ that $P(n)$ implies $P(n+1)$.

The base case is $P(2)$, and we can indeed write 2 as a product of primes because 2 is a prime.

Now we prove the induction step, i.e., $(\forall n \geq 2) P(n) \Rightarrow P(n+1)$.

Assume that n can be written as a product of primes. We argue by cases.

Case 1: $n+1$ is prime. In this case, there is nothing to prove.

Case 2: $n+1$ is not prime. This means that $n+1$ has a divisor k such that $1 < k < n+1$. Hence, we can write $n+1$ as $n+1 = k \cdot l$ where $k, l \in \mathbb{N}$ and $1 < k < n+1$. (This is what it means for a number to have a divisor; also note that this means $1 < l < n+1$.) So now we have $n+1$ written as a product of two smaller numbers.

Since $k, l \leq n$, the induction hypothesis implies that both k and l have prime factorizations. Let $p_1, p_2, \ldots, p_r$, $q_1, q_2, \ldots, q_s$ be primes, and let $e_1, e_2, \ldots, e_r$ and $f_1, f_2, \ldots, f_s$ be positive integers. Then we can write the prime factorizations of k and l as

$$k = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \tag{4}$$

$$l = q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r} \tag{5}$$

and combine them in a prime factorization of $n+1$ as

$$n + 1 = kl = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}, \tag{6}$$

which completes the proof. □

We remark that in (6), it may happen that there are pairs $i \in \{1, \ldots, r\}$ and $j \in \{1, \ldots, s\}$ such that $p_i = q_j$. We could then combine the factors $p_i^{e_i}$ and $q_j^{f_j}$ into $p_i^{e_i + f_j}$ so as to get the prime factorization written exactly in the format we described originally. But this is just a minor detail.

Note that every prime in the prime factorization of n divides n. To see this, suppose $n = \prod_{i=1}^{r} p_i^{e^i}$ where all the p_i are primes and $e_i \geq 1$ are integers. Then we can rewrite $n = p_i \left(p_1^{e_1} \cdots p_i^{e_i - 1} \cdots p_r^{e_r} \right)$. We can use this observation and prime factorizations to prove the following theorem.

Theorem 3. *There are infinitely many primes*

Proof. We argue by contradiction.

Suppose there are not infinitely many primes. Then we can enumerate all the primes as $p_1, p_2, \ldots, p_r$ for some integer r.

Consider the integer

$$n = \prod_{i=1}^{r} p_i + 1. \tag{7}$$

By Theorem 2, n has a prime factorization $p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ where p_i is prime and $e_i \geq 1$ is an integer for all $i \in \{1, \ldots, s\}$. Since every prime in n's prime factorization divides n, and the prime factorization of n consists of at least one prime (otherwise n would be 1), n has a prime divisor. But we see from (7) that no prime divides n because we can write $n = (p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_r) p_i + 1$ for any $i \in \{1, \ldots, r\}$. This is a contradiction. The assumption we made was that there were only finitely many primes, which means that this assumption is wrong. It follows that there are infinitely many primes. □

2.1 Greatest Common Divisor and Least Common Multiple

Sometimes it is more convenient to add redundant terms to the prime factorization. This is useful when we use prime factorizations of two numbers to construct another number. Let $p_1, p_2, \ldots, p_r$ be primes and let $e_1, e_2, \ldots, e_r$ be non-negative integers such that $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$. Note that this form of prime factorization is no longer unique because we can multiply by an arbitrary number of primes raised to the zeroth power and not change the product on the right-hand side.

We use this redundant form to describe the greatest common divisor and the least common multiple of two integers.

Definition 3. *The* greatest common divisor *of integers a and b, denoted* $\gcd(a, b)$*, is the largest integer d such that $d \mid a$ and $d \mid b$. Furthermore, if $c \mid a$ and $c \mid b$, then $c \mid d$.*

Definition 4. *The* least common multiple *of integers a and b, denoted* $\operatorname{lcm}(a, b)$*, is the smallest integer m such that $a \mid m$ and $b \mid m$. Furthermore, if $a \mid n$ and $b \mid n$, then $m \mid n$.*

We can express both of these integers using prime factorizations.

As a warmup, let's find $\gcd(60, 72)$ and $\operatorname{lcm}(60, 72)$. We can do this using prime factorizations. Write $60 = 2^2 \cdot 3^1 \cdot 5^1$ and $72 = 2^3 \cdot 3^2$. Let's expand the prime factorization of 72 so that the list of primes in prime factorization of both 60 and 72 is the same. We get $72 = 2^3 \cdot 3^2 \cdot 5^0$. Note that $\gcd(60, 72) = 12 = 2^2 \cdot 3^1$, and $\operatorname{lcm}(60, 72) = 360 = 2^3 \cdot 3^2 \cdot 5^1$. Let's write all four prime factorizations together and observe a pattern.

$$\begin{aligned} 60 &= 2^2 \cdot 3^1 \cdot 5^1 \\ 72 &= 2^3 \cdot 3^2 \cdot 5^0 \\ \gcd(60, 72) &= 2^2 \cdot 3^1 \cdot 5^0 \\ \operatorname{lcm}(60, 72) &= 2^3 \cdot 3^2 \cdot 5^1 \end{aligned}$$

The pattern we see is that to let the greatest common divisor, we take the smaller of the exponents e_i and f_i for each i, and we take the larger of the exponents e_i and f_i for each i to get the least common multiple. More formally, if

$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$
$$b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$$

then

$$\gcd(a, b) = \prod_{i=1}^{r} p_i^{\min(e_i, f_i)}$$
$$\operatorname{lcm}(a, b) = \prod_{i=1}^{r} p_i^{\max(e_i, f_i)}$$