LECTURE 9

Divisibility, Cont'd

We ended last time with the following lemma:

Lemma 9.1. *If $a, b, q, r \in \mathbb{Z}$ and $a = bq + r$, then*

$$GCD(a, b) = GCD(b, r) \quad .$$

The lemma above is used in proving the following algorithm for finding the greatest common divisor of two integers.

Theorem 9.2. *THE EUCLIDEAN ALGORITHM Let a and b be positive integers with $a \geq b$. If $b \mid a$, then $GCD(a, b) = b$. If $b \nmid a$, then the following algorithm*

$$\begin{array}{rcl} a & = & bq_0 + r_0 \quad ; \quad 0 < r_0 < b \\ b & = & r_0 q_1 + r_1 \quad ; \quad 0 \leq r_1 < r_o \\ r_0 & = & r_1 q_2 + r_2 \quad ; \quad 0 \leq r_2 < r_1 \\ r_1 & = & r_2 q_3 + r_3 \quad ; \quad 0 \leq r_3 < r_2 \\ r_2 & = & r_3 q_4 + r_4 \quad ; \quad 0 \leq r_4 < r_3 \\ & & \vdots \end{array}$$

terminates after a finite number of steps; that is for some integer t:

$$\begin{array}{rcl} r_{t-2} & = & r_{t-1} q_t + r_t \quad ; \quad 0 \leq r_t < r_{t-1} \\ r_{t-1} & = & r_t q_{t+1} + 0 \quad . \end{array}$$

Then r_t, the last non-zero remainder, is the greatest common divisor of a and b.

Proof.

If $b \mid a$ then $a = bq + 0$, so $GCD(a, b) = GCD(b, 0) = b$ by Lemma 1.7. If $b \nmid a$, then by the division algorithm there exists $q \in \mathbb{Z}$ such that

$$a = bq_0 + r_0$$

and moreover, $0 < r_0 < b$. Applying Lemma 1.7, we have

$$GCD(a, b) = GCD(b, r_0) \quad . \tag{9.1}$$

If $r_0 \mid b$, then we have $GCD(b, r) = r_0$; and so

$$GCD(a, b) = GCD(b, r_0) = r_0 \quad .$$

If $r_0 \nmid b$, then by the division algorithm

$$b = q_1 r_0 + r_1$$

with $0 < r_1 < r_0$. Applying Lemma 1.7 again, we have

$$GCD(b, r_0) = GCD(r_0, r_1) \tag{9.2}$$

which together with (9.1) yields

$$GCD(a, b) = GCD(r_0, r_1) \quad . \tag{9.3}$$

If $r_1 \mid r_0$, then $GCD(r_0, r_1) = r_1$ and we have

$$GCD(a,b) = GCD(r_0, r_1) = r_1 \quad .$$

Otherwise, if $r_1 \nmid r_0$, then we have by the division algorithm

$$r_0 = r_1 q_2 + r_2 \quad .$$

Then by Lemma 1.7

$$GCD(r_1, r_0) = GCD(r_1, r_2) \quad . \tag{9.4}$$

So, (9.3) and (9.4) imply

$$GCD(a,b) = GCD(r_1, r_2) \tag{9.5}$$

One continues in this manner until one reaches a step t where $r_{t+1} = 0$. The last non-zero remainder r_t will then be the greatest common divisor of a and b. (This process terminates because the numbers r_i satisfy

$$b > r_o > r_1 > \cdots > r_{t-1} > r_t$$

and are bounded from below by zero.) □

Example. Find the greatest common divisor of 4236 and 2592.

$$\begin{aligned}
4236 &= (1)(2592) + 1704 \\
2592 &= (1)(1704) + 888 \\
1704 &= (1)(888) + 816 \\
888 &= (1)(816) + 72 \\
816 &= (11)(72) + 24 \\
72 &= (3)(24) + 0
\end{aligned}$$

Therefore

$$GCD(4236, 2592) = 24 \quad .$$

1. Primes and Unique Factorization

Every non-zero integer n has at least four distinct factors; 1, -1, n and -n. Integers that have **only** these divisors play a crucial role in number theory.

DEFINITION 9.3. *An integer p is said to be* ***prime*** *if $p \neq 0, \pm 1$ and the only divisors of p are ± 1 and $\pm p$. If an integer z other than $0, \pm 1$ that is not prime, is said to be* ***composite.*** *h*

Note that if $z > 0$ is composite, then we can write z as

$$z = pq \qquad \text{with } 1 < p, q < z$$

PROPOSITION 9.4. *The set of prime numbers is infinite.*

Proof.

Suppose on the contrary, that there is only a finite number of primes. Then there is a maximal prime number $p_{\max}$ and every every number z greater than p must be divisible by some r with

$$2 \leq r < z \quad .$$

For the if $z > p_{\max}$, then z must be composite and so capable of being written

$$z = z_1 z_2 \qquad \text{with } 1 < z_1, z_2 < z$$

On the other hand, if either of the factor z_1 or z_2 is greater than $p_{\max}$, then it too must be composite and so capable of being written as a product of two smaller integers. In fact, whenever a factorization of z has a factor $q > p_{\max}$, the factor q can be replaced by two smaller factors. Since z is finite, by a finite process we will be able to write z as a product of integers between 2 and $p_{\max}$.

Now consider the integer

$$z = p_{\max}! \ + \ 1 \quad .$$

If n is any integer such that $2 \leq n \leq p_{\max}$, then

$$\begin{aligned} z &= (2)(3)\cdots(n)\cdots(p_{\max}-1)(p_{\max})+1 \\ &= [(2)(3)\cdots(n-1)(n+1)\cdots(p_{\max}-1)(p_{\max})]\,(n)+1 \end{aligned}$$

and so the Division Algorithm applied to n and z has remainder 1. Thus, z is not divisible by any integer between 2 and $p_{\max}$. But this contracdicts the conclusion of the preceding paragraph. Hence, there can be no maximal prime. Hence, there cannot be a finite number of primes. □

One immediate consequence of the definition of a prime number is that if p and q are prime and p divides q then $p = \pm q$. This is because the definition excludes the possibility that $p = \pm 1$.

Here is a deeper result.

THEOREM 9.5. *Let p be an integer with $p \neq 0, \pm 1$. Then p is prime if and only if p has this property:*

$$p \mid bc \quad \Rightarrow \quad p \mid b \quad \textit{or} \quad p \mid c \quad .$$

Proof.

$\Rightarrow$

Suppose p is prime and $p \mid bc$. Consider the greatest common divisor $GCD(p,b)$ of p and b. Now $GCD(p,b)$ must be a positive integer greater than or equal to 1 that divides both p and b. The only positive divisors of p are 1 and $|p|$. Therefore,

$$GCD(p,b) \in \{1, |p|\}$$

If $GCD(p,b) = |p|$, then certainly $p \mid b$. If $GCD(p,b) = 1$, then $p \mid c$ by Theorem 8.5. Thus, in every case, $p \mid b$ or $p \mid c$.

$\Leftarrow$

Let p be an integer $\neq 0, \pm 1$ with the property that

$$p \mid bc \qquad \Rightarrow \qquad p \mid b \quad \text{or} \quad p \mid c \qquad . \tag{9.6}$$

Suppose $p = st$. Then certainly $p \mid st$ and so by hypothesis (9.6), either $p \mid s$ or $p \mid t$. But then either

$$p \mid s \quad \Rightarrow \quad |s| \geq |p| \tag{9.7}$$

or

$$p \mid t \quad \Rightarrow \quad |t| \geq |p| \tag{9.8}$$

But since s and t are to be factors of p we must have

$$|s| \leq p \qquad \text{and} \qquad |t| \leq p \tag{9.9}$$

Thus, comparing (9.7), (9.8) and (9.9) we conclude that either

$$|s| = |p|$$

or

$$|t| = |p| \quad .$$

Thus, either

$$s = \pm p \qquad \Rightarrow \qquad q = \pm 1$$

or

$$t = \pm p \qquad \Rightarrow \qquad p = \pm 1 \quad .$$

Hence the only divisors of p are ± 1 and $\pm p$; and so p is prime. $\square$

Below is an easy corollary to this theorem.

COROLLARY 9.6. *If p is prime and $p \mid a_1 a_2 \cdots a_n$, then p divides at least one of the a_i.*

Proof.

By the previous theorem, if p is prime and p divides $a_1 a_2 \cdots a_n = a_1(a_2 \cdots a_n)$, then p divides a_1 or p divides $a_2 \cdots a_n$. If $p \mid a_1$ we are finished. Otherwise, $p \mid a_2(a_3 \cdots a_n)$. Applying Theorem 1.8 again, we conclude either p divides a_2 or p divides $a_3 \cdots a_n$. If p divides a_2 we are done, if not then we apply Theorem 1.8 to $a_3 \cdots a_n = a_3(a_4 \cdots a_n)$. After at most n steps, there must be an integer k, $1 \leq k \leq n$, such that $p \mid a_k$. $\square$

THEOREM 9.7. *Every integer n except $0, \pm 1$ is the product of primes*

Proof. First note that if $n = p_1 \cdots p_k$ is a product of primes, then $-n = (-p_1)p_2 \cdots p_k$ is also a product of primes. Hence it suffices to consider only the case when $n > 1$. Let S denote the set of positive integers greater than 1 that are *not* expressible as a product of primes. We shall show that S is empty. Assume on the contrary that S is non-empty. Then by the Well-Ordering Axiom, S has a least element m. Since $m \in S$, m is not itself prime. m must therefore have positive divisors other than 1 or m. Say $m = ab$, with $1 < a < m$ and $1 < b < m$. Now since a and b are less than m, and since m is the smallest element of S, $a \notin S$ and $b \notin S$. Hence, both a and b are expressible as products of primes

$$\begin{aligned} a &= p_1 \cdots p_r \\ b &= q_1 \cdots q_s \quad . \end{aligned}$$

But then

$$m = ab = p_1 \cdots p_r q_1 \cdots q_s$$

is a product of primes, so $m \notin S$. Hence we have a contradiction. Therefore, the set S must be empty. $\square$

Any integer other than $0, \pm 1$ that is not prime is called **composite**; since it can always be represented as a product of primes. This representation is not unique however. For example,

$$\begin{aligned} 45 &= 3 \cdot 3 \cdot 5 \\ &= -3 \cdot 5 \cdot -3 \\ &= -5 \cdot 3 \cdot -3 \end{aligned}$$

etc.. But notice that these different factorizations are essentially the same; the only difference being the ordering and the sign of the pairs of factors.

THEOREM 9.8. *THE FUNDAMENTAL THEOREM OF ARITHMETIC Every integer n except $0, \pm 1$ is a product of primes. This prime factorization is unique in the following sense: If*

$$n = p_1 p_2 \cdots p_r \qquad \text{and} \qquad n = q_1 q_2 \cdots q_s$$

with each p_i,q_j prime, then $r = s$ (that is the number of factors is the same) and after reordering and relabeling the q_j's

$$\begin{aligned} p_1 &= \pm q_1 \\ p_2 &= \pm q_2 \\ &\vdots \\ p_r &= \pm q_r \quad . \end{aligned}$$

Proof.

By Theorem 1.10 every integer n other than $0, \pm 1$ has a prime factorization. Suppose n has two factorizations, as listed in the statement of the theorem. Then

$$p_1(p_2 p_3 \cdots p_r) = q_1 q_2 q_3 \cdots q_s \quad ,$$

so that $p_1 \mid (q_1 q_2 \cdots q_n)$. By Corollary 1.9 (if p is prime and $p \mid (a_1 a_2 \cdots a_n)$ then p divides at least one of the factors a_1), p_1 must divide at least one of the q_i. By reordering an relabeling the q_i's if necessary, we may assume that $p_1 \mid q_1$. Since q_1 and p_1 are prime, we must have $p_1 = \pm q_1$. Consequently,

$$(\pm q_1)(p_2 p_3 \cdots p_r) = q_1 q_2 q_3 \cdots q_s \quad .$$

Dividing both sides by q_1 yields

$$(\pm 1) p_2 (p_3 p_4 \cdots p_r) = q_2 q_3 \cdots q_s \quad ,$$

which shows that p_2 divides $q_2 q_3 \cdots q_s$. As above, by Corollary 1.9, p_2 must divide one of the factors $q_2, q_3, \ldots, q_s$, which by a suitable reordering and relabeling we may take to be q_2. Hence $p_2 = \pm q_2$, and

$$(\pm 1)(\pm q_2)(p_3 p_4 \cdots p_r) = q_2 q_3 \cdots q_s \quad .$$

Dividing both sides by q_2 yields

$$(\pm 1)(\pm 1) p_3 p_4 \cdots p_r = q_3 q_4 \cdots q_s \quad .$$

We can continue in this manner until we run out of prime factors p_i on the left or until we run out of the prime factors q_j on the right. If $r < s$, then at the last step we have

$$\underbrace{(\pm 1)(\pm 1) \cdots (\pm 1)}_{r \text{ factors}} \quad = \quad q_{r+1} q_{r+2} \cdots q_s$$

.

Thus,

$$q_{r+1} q_{r+2} \cdots q_s = \pm 1 \quad .$$

But the q_i are all prime and so they cannot be divisors of 1. Hence we have a contradiction. If $s < r$ we end up with the statement

$$\underbrace{(\pm 1)(\pm 1) \cdots (\pm 1)}_{s\text{-factors}} \quad (p_{s+1} p_{s+2} \cdots p_r) = 1$$

which also leads to a contradiction. Hence $s = r$ and after the elimination process described above we are left with

$$\begin{aligned} p_1 &= \pm q_1 \\ p_2 &= \pm q_2 \\ &\vdots \\ p_r &= \pm q_r \quad . \end{aligned}$$

□

If we restrict attention to positive integers n, then we have an even stronger version of the unique factorization theorem.

Corollary 9.9. *Every integer $n > 1$ can be written in one and only one way as*

$$n = (p_1)^{s_1} (p_2)^{s_2} \cdots (p_r)^{s_r}$$

where the s_i are positive integers and the p_i are positive prime integers such that

$$p_1 < p_2 < \cdots < p_r \quad .$$