MATH 324 Summer 2006
Elementary Number Theory

Notes on Fundamental Theorem of Arithmetic

Department of Mathematical and Statistical Sciences
University of Alberta

The Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic states that if $n > 1$ is a positive integer, then n can be written as a product of primes in only one way, apart from the order of the factors.

Recall that an integer n is said to be a *prime* if and only if $n > 1$ and the only positive divisors of n are 1 and n.

In order to prove the fundamental theorem of arithmetic, we need the following lemmas.

Lemma 1. Every integer $n > 1$ is either a prime number or a product of prime numbers.

proof. We will prove this by induction on n. The lemma is clearly true for $n = 2$. Assume now that it is true for every positive integer k with $2 \leq k < n$. If n is not a prime, then it has a positive divisor d with $d \neq 1$ and $d \neq n$. Therefore, $n = m \cdot d$, where $m \neq n$. However, both m and d are less than n and greater than 1, so by the induction hypothesis each of m and d is a product of primes, therefore n is also a product of primes. This completes the induction.

$\square$

Lemma 2. If a prime p does not divide a, then $\gcd(p, a) = 1$.

proof. Let $d = \gcd(p, a)$, then $d \mid p$ and p is prime, so that $d = 1$ or $d = p$. However, $d \mid a$, so we must have $d \neq p$, since $p \nmid a$. Therefore, $d = 1$.

$\square$

Lemma 3. If a prime p divides ab, then $p \mid a$ or $p \mid b$. More generally, if a prime p divides a product $a_1 a_2 \cdots a_n$, the p divides at least one of the integers a_i, for $1 \leq i \leq n$.

proof. Suppose that $p \mid ab$ and that $p \nmid a$. We will prove that $p \mid b$. From Lemma 2 we have $\gcd(p, a) = 1$, and by the Euclidean algorithm there exist integers x and y such that $1 = xa + yp$, and therefore,

$$b = x \cdot ab + yb \cdot p,$$

so that $p \mid b$. For the more general statement, use induction on n.

$\square$

Theorem. *Fundamental Theorem of Arithmetic* Every integer $n > 1$ can be represented as a product of prime factors in only one way, apart from the order of the factors.

proof. The proof is by induction on n. The theorem is true for $n = 2$. Assume, then, that the theorem is true for all integers k with $1 < k < n$. We will show that this implies that it is also true for n. If n is prime, then there is nothing more to prove. Assume, then, that n is composite and that n has two factorizations, say

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t. \tag{$*$}$$

We want to show that $s = t$ and that each p_i equals some q_j.

Since $p_1 \,\big|\, q_1 q_2 \cdots q_t$ and p_1 is prime, then by Lemma 3, p_1 must divide some q_j. We may assume then (relabel) that $p_1 \,\big|\, q_1$, and therefore $p_1 = q_1$ since they are both primes. In $(*)$ we can cancel p_1 on both sides to get

$$\frac{n}{p_1} = p_2 \cdots p_s = q_2 \dots q_t.$$

If $s > 1$ or $t > 1$, then $1 < \dfrac{n}{p_1} < n$, and by the induction hypothesis the two factorizations of $\dfrac{n}{p_1}$ must be identical, apart from the order of the factors. Therefore $s = t$ and the factorizations in $(*)$ are also identical, apart from the order of the factors. The induction is complete.

$\square$

Note: In the factorization of an integer n, a particular prime p may occur more than once. If the *distinct* prime factors of n are $p_1, p_2, \dots, p_k$, and if p_i occurs as a prime factor α_i times, for $1 \le i \le k$ then we can write

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

that is,

$$n = \prod_{i=1}^{k} p_i^{\alpha_i},$$

and this is called the factorization of n into prime powers. We can also express 1 in this form by taking each exponent $\alpha_i = 0$.

Corollary. If

$$n = \prod_{i=1}^{k} p_i^{\alpha_i},$$

then the set of positive divisors of n is the set of all numbers d of the form

$$d = \prod_{i=1}^{k} p_i^{\beta_i},$$

where $0 \le \beta_i \le \alpha_i$ for $i = 1, 2, \dots, k$, and the number of positive divisors of n, denoted by $\tau(n)$, is given by

$$\tau(n) = (1 + \alpha_1)(1 + \alpha_2) \cdots (1 + \alpha_k).$$

As an example of the use of the prime factorization of an integer, we have the following result.

Theorem. If $n > 1$ is a positive integer, then n is a perfect square if and only if n has an odd number of divisiors.

Proof. Let the prime factorization of n be given by

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where $p_1 < p_2 < \cdots < p_k$ are distinct primes and for $1 \leq i \leq k$, each of the integers $\alpha_i \geq 1$.

Now note that n is a perfect square if and only if each α_i is an even integer, that is, if and only if there exist positive integers β_i such that

$$\alpha_i = 2\beta_i$$

for $1 \leq i \leq k$.

From the previous corollary, n is a perfect square if and only if the number of divisors of n is

$$\tau(n) = (2\beta_1 + 1)(2\beta_2 + 1) \cdots (2\beta_k + 1),$$

that is, if and only if $\tau(n)$ is an odd integer.

$\square$

Example. *The Locker Problem*

A certain locker room contains n lockers numbered $1, 2, \ldots, n$ and they are all originally locked. An attendant performs a sequence of operations $T_1, T_2, \ldots, T_n$ whereby with the operation T_k, $1 \leq k \leq n$, the condition of being locked or unlocked is changed for all those lockers and only those lockers whose numbers are multiples of k. Show that after all the n operations have been performed, all those lockers whose numbers are perfect squares (and only those lockers) are now open or unlocked.

proof. Locker number m, for $1 \leq m \leq n$, will be unlocked after the n operations have been performed if and only if it has changed state an odd number of times, that is, if and only if the integer m has an odd number of positive divisors. Therefore, locker number m is unlocked after all n operations are performed if and only if m is a perfect square.

$\square$

We will show that the prime factorization of an integer leads to a method to find the greatest common divisor and the least common multiple of two positive integers. First the definition.

Definition. If a and b are positive integers, then the **least common multiple** of a and b is the smallest positive integer m such that $a \,\big|\, m$ and $b \,\big|\, m$.

Note: The least common multiple of a and b is denoted by $[a, b]$ or $\text{lcm}(a, b)$, and its existence is guaranteed by the well ordering property of the positive integers.

Once the prime power decomposition of the positive integers a and b are known, it is trivial to find both $\gcd(a,b)$ and $\text{lcm}(a,b)$, in fact, if

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \qquad \text{and} \qquad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

where $p_1 < p_2 < \cdots < p_k$ are distinct primes, $0 \le \alpha_i$ and $0 \le \beta_i$, for $1 \le i \le k$, (zero exponents are allowed so that we may use the same primes in the factorization of both a and b), then

$$\gcd(a,b) = p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_2,\beta_2\}} \cdots p_k^{\min\{\alpha_k,\beta_k\}}$$

and

$$\text{lcm}(a,b) = p_1^{\max\{\alpha_1,\beta_1\}} p_2^{\max\{\alpha_2,\beta_2\}} \cdots p_k^{\max\{\alpha_k,\beta_k\}}.$$

The hard part (how hard is an open question) is *finding* the prime power decomosition of a positive integer.

From the above, we have an easy proof of the following theorem.

Theorem. If a and b are positive integers, then

$$\gcd(a,b) \cdot \text{lcm}(a,b) = a \cdot b.$$

Proof. Note that for any two real numbers x and y we have

$$\max\{x,y\} + \min\{x,y\} = x + y$$

since on the left, one is x and the other is y. Now multiply the prime power decompositions of a and b together to get

$$\gcd(a,b) \cdot \text{lcm}(a,b) = a \cdot b.$$

$\square$

As application of the fundamental arithmetic, we give another proof that there are infinitely primes. The proof below shows that the sum of the reciprocals of the primes diverges.

Theorem. Consider the sum

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \frac{1}{19} + \frac{1}{23} + \cdots + \frac{1}{p}$$

in which the denominators run through the prime numbers from 2 to some prime number p.

This sum can be made greater than any preassigned real number $M > 0$, no matter how large, provided the prime p is sufficiently large, that is, the infinite series

$$\sum_{p \text{ prime}} \frac{1}{p}$$

diverges. Thus, if there were only finitely many primes, then the series above would converge, which is a contradiction.

Proof. Let $\{p_1, p_2, p_3, \ldots, p_m, \ldots\}$, be the sequence of primes, where p_m is the m^{th} prime (the sequence could be finite or it could be infinite), and suppose that the series

$$\sum_{m\geq 1} \frac{1}{p_m}$$

converges, then there exists a positive integer k such that

$$\sum_{m\geq k+1} \frac{1}{p_m} < \frac{1}{2}.$$

Let $Q = p_1 \cdot p_2 \cdots p_k$, and consider the numbers $1+nQ$ for $n = 1, 2, 3, \ldots$. None of these is divisible by any of the primes $p_1, p_2, \ldots, p_k$. Therefore, all of the prime factors of $1+nQ$ occur among the primes $p_{k+1}, p_{k+2}, \ldots$. Thus, for each integer $r \geq 1$, we have

$$\sum_{n=1}^{r} \frac{1}{1+nQ} \leq \sum_{t=1}^{\infty} \left(\sum_{m\geq k+1} \frac{1}{p_m} \right)^t,$$

since the sum on the right includes among its terms all the terms on the left.

However, the sum on the right is dominated by a convergent geometric series, so we have

$$\sum_{n=1}^{r} \frac{1}{1+nQ} \leq \sum_{t=1}^{\infty} \left(\sum_{m\geq k+1} \frac{1}{p_m} \right)^t \leq \sum_{t=1}^{\infty} \left(\frac{1}{2}\right)^t = 1$$

for all $r \geq 1$.

Now note that for each $n \geq 1$ we have $1 + nQ < 2nQ$, so that

$$\sum_{n=1}^{r} \frac{1}{1+nQ} > \frac{1}{2Q} \sum_{n=1}^{r} \frac{1}{n}$$

which can be made arbitrarily large, since the harmonic series diverges. This condradiction shows that our original assumption must have been incorrect, therefore the series $\displaystyle\sum_{p \text{ prime}} \frac{1}{p}$ diverges.

$\square$

We give a second proof, which gives an estimate on how fast the sum grows. First we prove the following lemmas:

Lemma 1. If x is a real number with $x \geq 2$, then $\displaystyle\prod_{\substack{p\leq x\\ p \text{ prime}}} \left(1 - \frac{1}{p}\right) < \frac{1}{\log x}$.

proof. For each prime $p \leq x$, we have $p > 1$, and the geometric series

$$\frac{1}{1-1/p} = 1 + \frac{1}{p} + \frac{1}{p^2} + \cdots$$

converges, and therefore

$$\prod_{\substack{p \leq x \\ p \text{ prime}}} \frac{1}{1-1/p} = \prod_{\substack{p \leq x \\ p \text{ prime}}} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right),$$

and by the unique factorization theorem, when the product on the right is multiplied out it gives the sums of the reciprocals of all integers having only primes not exceeding x as prime divisors. In particular, all positive integers less than or equal to x are of this form, so that

$$\prod_{\substack{p \leq x \\ p \text{ prime}}} \frac{1}{1-1/p} > \sum_{k=1}^{\lfloor x \rfloor} \frac{1}{k} > \int_1^{\lfloor x \rfloor + 1} \frac{1}{u}\, du > \log x.$$

$\square$

Lemma 2. For any real number $t > -1, \quad t \neq 0$, we have $\dfrac{t}{1+t} < \log(1+t) < t$.

proof. Let $t > -1$, with $t \neq 0$, if we define the function $f(u) = \log(1+u)$ for $u > -1$, then the mean value theorem implies the existence of a real number T between 0 and t such that

$$f(t) - f(0) = \log(1+t) - \log(1) = t \cdot \frac{d}{du} \log(1+u)\bigg|_{u=T},$$

that is, $\log(1+t) = \dfrac{t}{1+T}$ for some T between 0 and t.

Now, since the function $g(u) = \dfrac{1}{1+u}$ is strictly decreasing on the interval $-1 < u < \infty$, if $t < T < 0$, then $\dfrac{1}{1+T} < \dfrac{1}{1+t}$, and since $t < 0$, then $\dfrac{t}{1+T} > \dfrac{t}{1+t}$.

Similarly, if $0 < T < t$, then $\dfrac{1}{1+t} < \dfrac{1}{1+T}$, and since $t > 0$, then $\dfrac{t}{1+t} < \dfrac{t}{1+T}$.

Thus, $\log(1+t) > \dfrac{t}{1+t}$ for all $t > -1$, with $t \neq 0$.

Also, since the function $f(u) = \log(1+u)$ is concave down on the interval $-1 < u < \infty$, the entire graph lies below the tangent line to the curve at $u = 0$, that is,

$$\log(1+t) < t$$

for all $t > -1$, with $t \neq 0$. $\square$

Theorem. The series $\displaystyle\sum_{p \text{ prime}} \frac{1}{p}$ diverges. In fact, $\displaystyle\sum_{\substack{p\le x\\ p \text{ prime}}} \frac{1}{p} > \frac{1}{2}\log\log x$.

proof. From Lemma 1 we have

$$\log \prod_{\substack{p\le x\\ p \text{ prime}}} \left(1-\frac{1}{p}\right) = \sum_{\substack{p\le x\\ p \text{ prime}}} \log\left(1-\frac{1}{p}\right) < -\log\log x.$$

Now, since

$$\frac{t}{1+t} \ge 2t$$

for $0 > t \ge -\frac{1}{2}$, and since $p \ge 2$, then from the left-hand side of the inequality in Lemma 2 we have

$$-\frac{2}{p} < \log\left(1-\frac{1}{p}\right)$$

for all primes p, and therefore

$$\sum_{\substack{p\le x\\ p \text{ prime}}} \frac{2}{p} > -\sum_{\substack{p\le x\\ p \text{ prime}}} \log\left(1-\frac{1}{p}\right) > \log\log x.$$

$\square$

As another application of the fundmental theorem of arithmetic, we prove a special case of Dirichlet's theorem, which says that if a and b are relatively prime positive integers, then the arithmetic progression

$$a\cdot n + b, \quad n \ge 0$$

contains infinitely many primes.

Theorem. There are infinitely many primes of the form $4n-1$, where n is a positive integer.

Proof. Note that any odd integer is of the form $4n-1$ or $4n+1$, and the product of any two odd integers $a = 4k-1$ and $b = 4\ell-1$, or the product of an two odd integers $a = 4k+1$ and $4\ell+1$, is of the form $4n+1$.

Suppose that there are only finitely many primes of the from $4n-1$, say $p_1, p_2, \ldots, p_k$, where $p_1 = 3$, and let

$$Q = 4p_2\cdots p_k - 1,$$

then Q is not divisible by any of the primes $p_1, p_2, \ldots, p_k$. However, this implies that every prime divisor of Q is of the form $4n+1$, and as noted above, this implies that Q itself if of the form $4n+1$, which is a contradiction. Therefore there are an infinite number of primes of the form $4n-1$.