Elementary Number Theory
Math 175, Section 30, Autumn 2010
Shmuel Weinberger (shmuel@math.uchicago.edu)
Tom Church (tchurch@math.uchicago.edu)
www.math.uchicago.edu/~tchurch/teaching/175/

Script 2: Primes

Definition 2.1. Recall that if $g \in \mathbb{Z}$, an integer a is called a *divisor* of n if $a|n$. An integer $p > 1$ is called a *prime* provided that the only positive divisors of p are 1 and p itself. An integer $n > 1$ is called *composite* if it is not prime.

Theorem 2.2. Every integer $n > 1$ has at least one prime factor.

Theorem 2.3. Every integer $n > 1$ may be factored into a product of primes.

Theorem 2.4. Let p be a prime number. If $p|ab$, then $p|a$ or $p|b$.

Theorem 2.5 (Fundamental Theorem of Arithmetic)**.** Every integer $n > 1$ may be factored into a product of primes in a unique way up to the order of the factors. In other words, there exists a uniquely determined set of primes $\{p_1, \ldots, p_k\}$ and a uniquely determined set of corresponding positive integers $\{\alpha_1, \ldots, \alpha_k\}$ such that $n = p_1^{\alpha_1} \cdot \cdots \cdot p_k^{\alpha_k}$.

Theorem 2.6. If $a^2|b^2$, then $a|b$.

Exercise 2.7. For any positive real number $x \in \mathbb{R}$, there is a real number $\sqrt{x}$ (you may assume this). It is defined uniquely by the property that $\sqrt{x} > 0$ and $(\sqrt{x})^2 = x$.

Recall that a real number x is defined to be *rational* (and we write $x \in \mathbb{Q}$) if there exist integers p and q such that $q \cdot x = p$, and x is called *irrational* otherwise.

Show that if n is a positive integer that is not a perfect square (that is, there is no $a \in \mathbb{Z}$ such that $a^2 = n$), then $\sqrt{n}$ is irrational.

Definition 2.8. A positive integer $m \in \mathbb{Z}$ is called a *square* if $m = d^2$ for some $d \in \mathbb{Z}$. A positive integer $n \in \mathbb{Z}$ is called *squarefree* if n is not divisible by any square; formally, we say that n is squarefree if $d^2 | n \implies d^2 = 1$.

Theorem 2.9. Prove that every positive integer n can be written uniquely as $n = rs$, where $r > 0$ is squarefree and $s > 0$ is a square.

Theorem 2.10. Prove that the number of integers $m > 0$ for which $m \leq N$ and m is a square is at most $\sqrt{N}$. (Hint: prove that the number is exactly $\lfloor \sqrt{N} \rfloor$, the integer you get if you round $\sqrt{N}$ down to the nearest integer.)

Theorem 2.11. Let $\mathcal{S} = \{p_1, \ldots, p_k\}$ be a set of prime numbers. Prove that the number of squarefree integers $m > 0$ for which all the prime factors of m lie in the set $\mathcal{S}$ is 2^k.

Theorem 2.12. Let $\mathcal{S} = \{p_1, \ldots, p_k\}$ be a set of prime numbers. Prove that the number of positive integers $m \leq N$ for which all prime factors of m lie in the set $\mathcal{S}$ is at most $2^k \sqrt{N}$.

Theorem 2.13. Use the preceding theorems to prove that there are infinitely many primes.

Theorem 2.14. The prime-counting function $\pi(N)$ is defined to be the number of prime numbers less than or equal to N. Prove that $\pi(N) \geq \frac{1}{2} \log_2(N)$. (This is a stronger statement than Theorem 2.13—you should make sure you understand why.)

Challenge Problem 2.15. If you know another proof of Theorem 2.13: can you use your other proof to show that $\pi(N) \geq \frac{1}{2} \log_2(N)$? How about to show that $\pi(N) \geq \log_2(\log_2(N))$? What is the best bound on $\pi(N)$ which you can get from this other proof?