An Introduction to the Theory of Numbers

Nicholas Giannoulis

Contents

The purpose of these notes is to document my survey of Hardy and Wright's 'An Introduction to the Theory of Numbers'. It is my hope that it will be useful as a reference for others also.

1 Notation and Introductory Concepts

1.1 $a|b$

We will denote by $a|b$, where a and b are understood to be positive integers, that a divides b. That is, there exists some integer m such that $am = b$.

1.2 GCD

The greatest commond divisor of two integers a and b, denoted (a, b), is the greatest integer which diivides both a and b

1.3 Coprime

Two integers a and b are said to be coprime if their only common positive divisor is 1. i.e.

$$(a, b) = 1$$

1.4 Big O

Suppose ϕ is some real valued function on a particular domain. Then by $O(\phi)$ we denote the class of complex valued functions f such that there exists a constant A with

$$|f| < A\phi$$

over the entirety of the domain.

1.5 Little o, $\prec$

Suppose ϕ is as before. Then by $o(\phi)$ we denote the class of functions f with

$$f/\phi \to 0$$

By $f \prec \phi$ we mean that $f \in o(\phi)$

1.6 $\sim$

By $f \sim \phi$ we mean that

$$f/\phi \to 1$$

2 Primes

2.1 Preliminary Results

Theorem 2.1 (Bezout's Identity). *If $(a, b) = 1$ if and only if there exist integers x and y such that $ax + by = 1$*

Proof. Prove that $(a, b) = (a - b, b)$. From this the forward direction follows by induction. To see the other direction, observe that any common divisor of a and b must also divide $ax + by = 1$. □

Lemma 2.1 (Euclid's Lemma). *Let p be a prime diving ab. Then $p|a$ or $p|b$.*

Proof. Write $pd = ab$. Suppose p does not divide a. Then $(a, p) = 1$. By Theorem 2.1 for some integers x and y;

$$\begin{aligned} ax + py &= 1 \\ abx + bpy &= b \\ p(dx + by) &= b \end{aligned}$$

□

Theorem 2.2 (The Fundamental Theorem of Arithmetic). *Every positive integer greater than 1 has a unique (up to permutation) decomposition into a product of primes.*

Proof. Exercise 1 □

2.2 Euclid's Theorem

Theorem 2.3 (Euclid's Theorem). *There are infinitely many prime numbers*

The classical proof is by contradiction.

Proof. Assume there are only finitely many primes $p_1, ..., p_n$. Let $q = p_1p_2...p_n+1$. Then

$$q - p_1...p_n = 1$$

By the converse of Bezout's identity q and $p_1, ..., p_n$ are coprime. But then none of the primes p_1 through p_n can divide q. We conclude that none of the prime divisors of q are amongst this list of primes. □

Remark. *If one takes* $q_n = p_1 ... p_n + 1$ *where the* p_i *are the first* n *primes, then Euclid's proof allows for the following recursive bound on the* $n+1$*th prime number. For* $n > 1$ *it is clear that*

$$q_n < p_n^n + 1$$

At least one of the primes larger than p_n *must divide* q*, and can therefore be at most as large as* q*. Hence*

$$p_{n+1} < p_n^n + 1$$

One can turn Euclid's argument on certain subsets of the primes.

Theorem 2.4. *There are infinitely many primes of the form* $4n + 3$

Proof. Let q be the product of 4 and all of the odd primes up to p, the largest prime of the form $4n + 3$, minus one

$$q = 4 \cdot 3 \cdot 5 \cdot ... \cdot p - 1$$

Then q is of the form $4n + 3$. q must contain at least one prime factor of the form $4n + 3$ because a product of numbers of the form $4n + 1$ is of the same kind (in fact it must contain an odd number of such factors counting multiplicity). None of the primes of this form up to p can divide q, therefore another such prime must exist. □

Other proofs of Euclid's theorem are often fruitful also.

Proof. Let $2, 3, ..., p_j$ be the first p_j primes. Let $N(x)$ be the number of integers less than or equal to x which are not divisible by any prime p with $p > p_j$. Suppose n is such an integer. Write

$$n = n_1^2 m$$

where m is 'squarefree', that is, not divisible by the square of any positive integer other than 1 (why is this possible, why is this decomposition unique). m must be of the form $p_1^{b_1} ... p^{b_j}$ where the b_i are all either 0 or 1. Hence there are exactly 2^j values m may take. It is easily observed that $n_1 \leq \sqrt{x}$. Hence;

$$N(x) \leq 2^j \sqrt{x}$$

Suppose there are exactly j primes. Then $N(x) = x$ (if x is a positive integer). But then

$$x \leq \sqrt{x}2^j$$

for all x, but this is plainly untrue.

$\square$

Remark. *A similar argument shows that* $\sum \frac{1}{p}$ *is divergent.*

Proof. Suppose $\sum \frac{1}{p}$ converges. Then for some j,

$$\frac{1}{p_j} + \frac{1}{p_{j+1}} + ... < \frac{1}{2}$$

Every integer n not exceeding x is either divisible only by primes less than p_j, or is otherwise divisible by at least one of the primes $p_j, p_{j+1}, ...,$. For each such prime p_i, there are at most $\frac{x}{p_i}$ multiples n of p_i. Therefore if x is a positive integer

$$x \leq N(x) + \frac{x}{p_j} + \frac{x}{p_{j+1}} + ...$$
$$x \leq N(x) + \frac{x}{2}$$
$$\frac{x}{2} \leq N(x)$$

But this gives rise to the same contradiction as in the prior proof of Theorem 2.2.

$\square$

2.3 Exercises

1. Prove Theorem 2.2
2. Prove that there are infinitely many primes of the form $6n + 5$.
3. Let $F_n = 2^{2^n} + 1$. Show that all distinct F_n are coprime. Hence show that there are infinitely many primes.
4. If $a > 1$ and $a^n + 1$ is prime, show that a is even and n is of the form 2^m.

5. If $n > 1$ and $a^n - 1$ is prime, show that $a = 2$ and n is prime.

6. Prove that no polynomial $f(n)$ with integral coefficients can be prime for all n, or for all sufficiently large n.