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* $n+1th$ *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

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

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.

3 Irrationality

3.1 Algebraic Numbers

Theorem 3.1. *If x is a root of the equation*

$$x^m + c_1 x^{m-1} + ... + c_m = 0$$

where the c_i are integral, then x is either integral or irrational.

Proof. WLOG we may assume c_m is not 0. Suppose $x = a/b$ with $(a, b) = 1$.

$$a^m = b(-c_1 a^{m-1} - c_2 a^{m-2} b - ... - c_m b^{m-1})$$

whence any prime divisor of b divides a. Therefore $b = 1$. □

Remark. *In a more general field such numbers are called algebraic integers for this reason.*

3.2 Exercises

1. Show that $\sqrt[m]{N}$ is irrational or integral.

4 Solutions

4.1 Primes

4.1.1 2.1

The existence of prime decompositions is a simple matter of induction. Let $p_1 p_2 ... p_m$ and $q_1 q_2 ... q_n$ be two equal prime decompositions. Then p_1 divides the product of the q_i. By Euclid's Lemma, it must divide some q_j. But then it follows that $p_1 = q_j$. Hence

$$p_2 p_3 ... p_m = q_1 ... q_{j-1} q_{j+1} ... q_m$$

One may continue this process until either one or both of the products is empty. If only one is empty, then it must be that a product of primes is equal to 1, which is clearly impossible. If they are both empty, then then the products were identical.

4.1.2 2.2

Suppose there are only finitely many primes of the form $6n + 5$. Let $q = 2 \cdot 3 \cdot ... \cdot p - 1$ where p is the largest prime of the form $6n + 5$. q is clearly of the form $6n + 5$, but then it must be divisible by at least one prime of the form $6n + 5$ since a product of the other remainders cannot be of this form. q is clearly coprime to all of the primes of this form. We reach the familiar contradiction.

4.1.3 2.3

Suppose $n > m \geq 1$

$$\begin{aligned} F_n - F_m &= 2^{2^n} - 2^{2^m} \\ &= 2^{2^m}(2^{2^m(2^{n-m}-1)}) - 1 \end{aligned}$$

If p is a common prime divisor of F_n and F_m it must be odd and it must divide their difference. Therefore, it must divide $2^{2^m(2^{n-m}-1)} - 1$. Let p be an odd prime divisor of $2^{2^m} + 1$. Then 2^{2^m} is congruent to -1 mod p. Because $n - m$ is at least 1, $2^{n-m} - 1$ is odd. But then $2^{2^m(2^{n-m}-1)} = \left(2^{2^m}\right)^{2^{n-m}-1}$ is congruent to -1 mod p. But then it follows that $F_n - F_m$ is not divisible by

p.

If the distinct F_n are all coprime, then each possesses a unique set of prime divisors and the infinitude of primes follows.

4.1.4 2.4

If a were odd then a^n+1 would be even and greater than 2. Suppose n had an odd divisor d with $n = dq$. Then,

$$\begin{aligned} a^{dq} + 1 &= (a^q)^d + 1 \\ &= (a^q+1)(a^{q(d-1)} - a^{q(d-2)} + ... + 1) \end{aligned}$$

but this is a non trivial factorisation of $a^n + 1$.

4.1.5 2.5

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} ... + 1)$$

If $a > 2$ this factorisation is immediately non trivial. Suppose $a = 2$ and $n = qd$ is not prime.

$$\begin{aligned} 2^{qd} &= (2^q)^d - 1 \\ &= (2^q - 1)(2^{q(d-1)} + 2^{q(d-2)} + ... + 1) \end{aligned}$$

4.1.6 2.6

Suppose $f(n) = \sum_{k=0}^{m} c_k n^k$ is a polynomial with integral coefficients. WLOG assume $c_m > 0$. Then $f(n) \to \infty$. Let N be such that $n \geq N \implies f(n) > 1$. Lastly, set $f(N) = y$. Then;

$$\begin{aligned} f(N+ry) &= \sum_{k=0}^{m} c_k (N+ry) \\ &= f(N) + yQ \end{aligned}$$

Where Q is some integer obtained by considering the terms of the binomial expansions which contain at least one copy of y. Therefore $f(n)$ is divisible by y every term of the arithmetic sequence $\{N + ry\}$. Because $f(n) \to \infty$, only finitely many of these can be at least as small as y (This is an issue only if y is prime). Therefore f is composite on a positive proportion of the integers.

4.2 Irrationality

4.2.1

$\sqrt[m]{N}$ is a root of the polynomial $f(X) = X^m - N$. The result follows from the Rational Root Theorem (3.1)