Section 3.7: Two Classic Theorems

In this section, we shall put the tools we learnt in the previous sections to prove two classical theorems in mathematics. This will illustrate the power behind the tools we have developed.

1. The Irrationality of $\sqrt{2}$

We shall first show that the number $\sqrt{2}$ is not rational (and hence must be irrational) using contradiction. First we need the following important results about integers and rational numbers (we shall not prove the first result).

Theorem 1.1. *(Unique Factorization) Suppose a is an integer and $a \neq \pm 1$. If a is positive then a can be factored uniquely as a product of prime numbers $a = p_1^{n_1} \cdots p_r^{n_r}$. If a is negative, then a can be factored uniquely as a product of distinct prime numbers $a = -p_1^{n_1} \cdots p_r^{n_r}$. In both cases, at a is divisible by at least one prime.*

Theorem 1.2. *Any rational number r can be written in the form*

$$\frac{a}{b}$$

where a and b have no common divisors.

Proof. We can prove this directly. Suppose that r is a rational number. Then

$$r = \frac{c}{d}$$

for some integers c and d. Then we can write c and d each uniquely as a product of distinct prime numbers. Suppose that k is the greatest common divisor of c and d i.e. k is the largest product of distinct primes which is a factor of c and d . Then $c = ak$ and $d = bk$ for some integers a and b with no common divisors. Therefore,

$$r = \frac{c}{d} = \frac{ak}{bk} = \frac{a}{b}$$

where a and b have no common divisors.

□

Theorem 1.3. *$\sqrt{2}$ is not rational*

Proof. Suppose that $\sqrt{2}$ is a rational number. Then there exists integers a and b such that

$$\sqrt{2} = \frac{a}{b}$$

where $b \neq 0$ and a and b have no common divisots. Using simple algebra, it follows that

$$2 = \frac{a^2}{b^2}$$

so

$$a^2 = 2b^2.$$

Therefore, by definition, a^2 is an even number. Since a^2 is an even number, so is a (by our previous results), and hence there exists a number k such that $a = 2k$. Substituting $a = 2k$ into the above equation, we have

$$a^2 = (2k)^2 = 4k^2 = 2b^2$$

and so $b^2 = 2k^2$. Therefore, b^2 is even, and so b is even. Thus it follows that both a and b are even and hence they have a common factor - 2. But this contradicts our initial assumption that a and b had no common divisors, so we have a contradiction. Therefore, out initial assumption must have been wrong and therefore $\sqrt{2}$ is not rational.

□

2. Infinitude of Primes

We shall now show that there are infinitely many prime numbers. In order to do this, we shall first prove a result which will be needed. Such results are usually called "Lemma's" (if they are only required to prove the Theorem", or "Proposition's" (if they are themselves of some interest, but not necessarily of great importance). Since the result we need to prove that there are infinitely many primes is interesting in its own right, we shall call it a "Proposition".

Proposition 2.1. *For any integer a and any prime p, if $p \mid a$ then $p \nmid (a+1)$.*

Proof. Suppose not. Then there exists an integer a and a prime p such that $p \mid a$ and $p \mid (a+1)$. Therefore, there exists integers k and l such that

$$a = pk, \text{ and } a + 1 = pl.$$

This means that

$$pk + 1 = pl \text{ and so } p(l - k) = 1.$$

It follows that $p \mid 1$ and since the only integer divisors of 1 are 1 and -1, we have $p = \pm 1$. However, neither 1 or -1 are prime, and hence p is prime and not prime. This is a contradiction, and thus our initial assumption must be false. It follows that for any integer a and any prime p, if $p \mid a$ then $p \nmid (a+1)$.

□

We shall now use this Proposition to prove that there are infinitely many primes.

Theorem 2.2. *There are infinitely many prime numbers*

Proof. Suppose not. Then there are finitely many primes. Let

$$\{p_1, \ldots, p_r\}$$

be the set of all primes and define

$$N = p_1 \cdots p_r + 1.$$

Clearly N is an integer and $N > 1$, so N can be factored as a product of primes (by unique factorization) and must be divisible by at least one prime number. Since the only primes are $p_1, \ldots, p_r$, at least one of these primes must divide N, say p_i. So we know $p_i \mid N = p_1 \cdots p_r + 1$. However, $p_i \mid p_1 \cdots p_r$, so p divides, $N - 1$ and N. By the last Proposition, this is not possible, so we have a contradiction. Thus our initial assumption must have been wrong and thus there are infinitely many primes.

□

These are two classical theorems which were proved many years ago. However, at some point, the truth of these statements were not known - that is, before a valid mathematical proof was known, it was not clear whether or not these were true statements. In general, if a given statement is thought to be true, but does not yet have a mathematical proof, it is called a conjecture. In elementary number theory, there are a number of conjectures which are easy to state, yet whose truth is still unknown. A couple of examples are:

(*i*) (Goldbachs Conjecture) Every even integer greater than 2 can be written as the sum of two primes
(*ii*) There are infinitely many primes p such that p + 2 is also prime.
(*iii*) (Catalans Conjecture) The only consecutive prime powers are 8=23 and 9=32.

It is thought that perhaps one day, simple proofs like we have considered here could be derived for such conjectures!

3. Other Examples

We finish with a couple more examples.

Example 3.1. Is the statement "The product of any two irrational numbers is irrational" true? if so, give a proof, else give a counter example.

This is not true - consider $x = \sqrt{2}$ and $y = \sqrt{2}$. Both are irrational, but $x \cdot y = 2$ which is rational.

Theorem 3.2. *Show that there exists a prime number p of the form $n^2 + 2n - 3$ where n is a positive integer.*

Proof. To prove this result, we need to show that such a prime exists, and it is unique. To see it exists, note that if $n = 2$, then $2^2+2\cdot 2-3 = 5$ which is prime. Therefore, there exists such a prime.
To show it is unique, observe that

$$p = n^2 + 2n - 3 = (n + 3)(n - 1).$$

In particular, if $n > 2$, then p will be divisible by at least two integers (namely $n + 3$ and $n - 1$) and thus it cannot be prime.

□

Homework

(i) From the book, pages 184-185: Questions: 1, 6, 7, 11, 14, 15, 19, 26, 32