1 Lecture 11 (2/24/2011)

1.1 Even and odd integers

The set of even integers is

$$\{\cdots, -4, -2, 0, 2, 4, 6, \cdots\}$$

Thus an integer m *is even iff it is of the form* $m = 2k$ *for some integer* k.

Similarly the set of odd integers is

$$\{\cdots, -3, -1, 1, 3, 5, 7, \cdots\}$$

Thus an integer m *is odd iff it is of the form* $m = 2k$ *for some integer* k.

Every integer is either even or odd but not both, therefore in $U = \mathbb{Z}$

$$\sim(m \text{ is even}) \text{ is equivalent to } (m \text{ is odd}) \text{ and vice versa}$$

Theorem 1 *If an integer is even then its square is even.*

Proof.

1. Let m be an integer.
2. Assume m is even.
3. Then $m = 2k$ for some integer k
4. Squaring both sides we get
$$m^2 = 4k^2 = 2l \text{ where } l = 2k^2 \tag{1}$$
5. Since k is an integer, $2k^2$ is an integer.
6. Therefore by (1) and by definition m^2 is even.

■

We now prove the converse of this theorem.

Theorem 2 *If the square of an integer is even then the integer is even.*

This theorem is a little hard to prove as it stands, so we will prove instead its *contrapositive* which is equivalent to Theorem 2. The contrapositive statement is "if an integer is not even then its square is not even", or equivalently

Theorem 3 *If an integer is odd then its square is odd.*

Proof.

1. Let m be an integer.
2. Assume m is odd.

3. Then $m = 2k + 1$ for some integer k

4. Squaring both sides we get

$$m^2 = 4k^2 + 4k + 1 = 2l + 1 \text{ where } l = 2k^2 + 2k \tag{2}$$

5. Since k is an integer, $2k^2 + 2k$ is an integer.

6. Therefore by (2) and by definition m^2 is odd.

■

1.2 Rational and irrational numbers

Recall that a real number x is said to be *rational* if we can express x in the form $x = p/q$ where p, q are integers and $q \neq 0$. If x is not rational we say that x is *irrational*.

A rational number x can have many expressions of form p/q; for example $1/2, 2/6, 74/148$ are all expressions of the same rational number. In fact if p, q have a common divisor say l, then we can write $p = lp_1, q = lq_1$ for some integers p_1, q_1 and then we have

$$\frac{p}{q} = \frac{lp_1}{lq_1} = \frac{p_1}{q_1}$$

We say an expression p/q is *reduced* if p, q have no common divisors other than ± 1.

Theorem 4 *Every rational number has a reduced expression.*

We postpone the proof of this theorem. The main idea is that we can always cancel common divisors of the numerator and denominator to arrive at a reduced expression. To make this argument precise requires a little bit of work.

1.3 Irrationality of $\sqrt{2}$

We now come to the main result of this lecture.

Theorem 5 $\sqrt{2}$ *is an irrational number.*

This is hard to prove as it stands, therefore we give a proof by contradiction; *i.e.* we assume that $\sqrt{2}$ is rational and derive a contradiction. The assumption that $\sqrt{2}$ is rational gives us a place to start the proof; namely we can write $\sqrt{2}$ in the form p/q. The hard part (creative part) of the proof consists of figuring out how to derive a contradiction.

Proof.

1. Assume by way of contradiction that $\sqrt{2}$ is rational.

2. By Theorem 4, $\sqrt{2}$ has a reduced expression

$$\sqrt{2} = p/q \tag{3}$$

for some integers p, q

3. By definition p, q have no common divisors other than ± 1.

4. Thus p, q are not both divisble by 2, *i.e.* p, q are not both even.

5. Squaring (3) we get $2 = p^2/q^2$ and hence

$$p^2 = 2q^2 \tag{4}$$

6. Therefore p^2 is even and hence by Theorem 2, p is even.

7. Thus $p = 2k$ for some integer, and substituting in (4) we get

$$2q^2 = p^2 = (2k)^2 = 4k^2$$

8. Cancelling 2 we get

$$q^2 = 2k^2$$

9. Thefore q^2 is even and hence by Theorem 2, q is even.

10. Statements 4, 6, 9 constitute a contradiction.

11. Therefore $\sqrt{2}$ must be irrational, contrary to our assumption.

■

1.4 Infinitely many primes

Recall that a natural number p is said to be prime if $p > 1$ and the only divisors of p are 1 and p.

A basic result about prime numbers is the following

Theorem 6 *Every natural number bigger than* 1 *has a prime divisor.*

We postpone the proof of this theorem as well, until after we discuss mathematical induction.

Next we have the following "easy" theorem, whose proof we leave as an exercise.

Theorem 7 *If k is a natural number then $k, k+1$ have no common divisors other than* 1.

We come now to another mathematical theorem with a beautiful proof.

Theorem 8 *There are infinitely many primes numbers.*

We will prove this by contradiction also. Thus we assume that there are finitely many primes, and derive a contradiction. The main idea is that if there were finitely many primes, we could write them all down and multuiply them together.

Proof.

1. Suppose to the contrary that there are only finitely many primes, say

$$p_1, p_2, \ldots, p_m$$

2. Then the product $k = p_1 p_2 \ldots p_m$ is a natural number.

3. Every prime number divides k.

4. By Theorem 7, no prime number divides $k + 1$.

5. Since $k + 1 > 1$, this contradicts Theorem 6.

6. Therefore there must be infinitely many primes.

■

1.5 Exercises

1. Prove that if x is rational and y is irrational then $x + y$ is irrational.

   [Hint: $P \wedge Q \Rightarrow R$ is equivalent to $P \wedge (\sim R) \Rightarrow (\sim Q)$. Use this to get an equivalent retsatement of the assertion, which is easier to prove.]

2. Prove that there are infinitely many irrational numbers.

3. Prove Theorem 7.

   [Hint: Argue by contradiction, i.e. assume $k, k+1$ have a common divisor $l > 1$, and derive a contradiction.]