MATH 362

Elementary Number Theory Notes, 2019

Kieka Mynhardt

Contents

Section 1

Integers

Week 1

1.1 Mathematical Induction

We begin by revising one of the most basic methods of proof in mathematics – mathematical induction. What is it, why does it "work" and how do we use it?

Well-Ordering Principle or **Least-integer Principle:**

Every non-empty set S of positive integers contains a smallest element. That is, there is some integer $a \in S$ such that $a \leq b$ for each $b \in S$.

The Well-Ordering Principle is an **axiom** which we accept, without proof, as a fact. We use the Well-Ordering Principle to prove the

Principle of Finite Induction (Mathematical Induction):

Let S be a set of positive integers with the properties

(*i*) $1 \in S$

(*ii*) *whenever the positive integer k is contained in S, then the next integer $k+1$ is contained in S.*

Then S is the set of all positive integers.

Proof.
By contradiction: Suppose to the contrary that S does not contain all positive integers. Let T be the set of all positive integers that are not contained in S. By our assumption, T is non-empty.

By the Well Ordering Principle, T contains a smallest element, say a. Since $1 \in S$, it is clear that $a \neq 1$ and so $a-1$ is a positive integer. But $a-1 < a$ and so by the choice of a as smallest element of T, $a-1 \notin T$. The only possibility is $a-1 \in S$. By (ii), this implies that $a \in S$, a contradiction. ■

Note: This is not a demonstration of how to prove results by the method of Mathematical Induction, but a proof of the validity of the Principle of Mathematical Induction.

The following result can be proved similarly.

Principle of Finite Induction (Mathematical Induction):

Let S be a set of integers with the properties

(i) $n_0 \in S$ *for some integer* n_0;

(ii) *whenever the integer* $k \geq n_0$ *is contained in* S, *then* $k+1$ *is contained in* S.

Then S *contains all the integers* $n_0, n_0+1, n_0+2, \ldots$.

There is also the following (equivalent) form of induction:

Second Principle of Finite Induction (Strong form of Mathematical Induction):

Let S be a set of integers with the properties

(i) $n_0 \in S$ *for some* $n_0 \in \mathbb{Z}$ (*where* $\mathbb{Z}$ *denotes the set of all integers*),

(ii) *whenever the integers* $n_0, n_0+1, \ldots, k$ *are all contained in* S, *then the next integer* $k+1$ *is contained in* S.

Then S *contains all the integers greater than or equal to* n_0.

Rephrasing the Principle of Induction:

Let $\mathrm{P}(n)$ *be a statement about the integer* n. *If*

(i) $\mathrm{P}(1)$ *is true, and*

(ii) *the truth of* $\mathrm{P}(k)$, *for an arbitrary integer* $k \geq 1$, *implies the truth of* $\mathrm{P}(k+1)$,

then $\mathrm{P}(n)$ *is true for all positive integers* n.

Or more general:

Let $\mathrm{P}(n)$ *be a statement about the integer* n*. If*

(i) $\mathrm{P}(n_0)$ *is true, and*

(ii) *the truth of* $\mathrm{P}(k)$*, for an arbitrary integer* $k \geq n_0$*, implies the truth of* $\mathrm{P}(k+1)$*,*

then $\mathrm{P}(n)$ *is true for all integers* $n \geq n_0$*.*

Note: We are not concerned with the actual truth (or not) of the statement $\mathrm{P}(k)$, but with the fact that the truth of $\mathrm{P}(k)$ implies the truth of $\mathrm{P}(k+1)$.

1.2 Division of Integers

Let a and b be integers. We say that "a **divides** b" and write $a|b$ if there exists an integer d such that $ad = b$. The proofs of the following two lemmas are easy and omitted.

Lemma 1.1 *If* $d|a$ *and* $d|b$*, then* $d|(a+b)$*.*

Lemma 1.2 *If* $d|a_1$, $d|a_2$,..., $d|a_n$*, then* $d|(c_1a_1+c_2a_2+\cdots+c_na_n)$ *for any integers* $c_1, c_2, ..., c_n$*.*

Example: Use induction to prove that $6|(n^3-n)$ for all positive integers n.

Solution

Let $\mathrm{P}(n)$ be the statement $6|(n^3-n)$.

Basis Step: Is $\mathrm{P}(1)$ true?

If $n = 1$, then $n^3 - n = 1 - 1 = 0$. Clearly, $6|0$ and so $\mathrm{P}(1)$ is true.

Induction hypothesis:

Assume that $\mathrm{P}(k)$ is true for some integer $k \geq 1$, that is, $k^3 - k = 6d$ for some $d \in \mathbb{Z}$.

To prove: $\mathrm{P}(k+1)$ is true, that is, $(k+1)^3 - (k+1) = 6d'$ for some $d' \in \mathbb{Z}$.

ATTENTION!!!

Do not confuse the statement above of

what is to be proved when $n = k+1$

with **the start of your proof!**

Start your proof by beginning **with one side of the equation only**, working until you prove it equal to the other side. The obvious side to start with here is the left hand side:

$$\begin{aligned}(k+1)^3-(k+1) &= k^3+3k^2+3k+1-(k+1)\\ &= k^3-k+(3k^2+3k)\\ &= 6d+(3k^2+3k)\end{aligned}$$

by the induction hypothesis. By Lemma 1.1 we only need to show that $6|(3k^2+3k)$.

Suppose k is even. Then $k=2r$ for some integer r, so

$$3k^2+3k = 12r^2+6r = 6(2r^2+r),$$

which is clearly divisible by 6. Suppose k is odd. Then $k=2s+1$ for some integer s, so

$$\begin{aligned}3k^2+3k &= 12s^2+12s+3+6s+3\\ &= 6(2s^2+3s+1),\end{aligned}$$

which is also clearly divisible by 6. Hence the truth of $\mathrm{P}(k)$ implies the truth of $\mathrm{P}(k+1)$ and the result follows by the principle of induction.

Example: **(Omitted in class, read on your own)** Let $\mathrm{P}(n)$ be the statement

$$7^n-2^n \text{ is divisible by } 5.$$

Prove that $\mathrm{P}(n)$ is true for all nonnegative integers n.

Solution

Basis Step: $\mathrm{P}(0)$ is the statement

$$7^0-2^0 \text{ is divisible by } 5,$$

which is obviously true because $7^0-2^0=1-1=0$.

Induction hypothesis: Assume that $\mathrm{P}(k)$ is true for some $k\geq 0$, that is, assume that

$$7^k-2^k \text{ is divisible by } 5, \text{ i.e. } 7^k-2^k=5d \text{ for some } d\in\mathbb{Z}. \tag{1.1}$$

To prove: $\mathrm{P}(k+1)$ is true, that is, using (1.1) we must show that

$$7^{k+1}-2^{k+1} \text{ is divisible by } 5.$$

Now,

$$\begin{aligned}7^{k+1}-2^{k+1} &= 7\cdot 7^k-2\cdot 2^k\\ &= 5\cdot 7^k+2\cdot 7^k-2\cdot 2^k\\ &= 5\cdot 7^k+2(7^k-2^k)\\ &= 5(7^k+2d)\end{aligned}$$

by (1.1). It follows that $7^{k+1}-2^{k+1}$ is divisible by 5. Hence $\mathrm{P}(k+1)$ is true and the result follows by the principle of induction.

1.3 Greatest common divisor

Let a and b be integers, noth both equal to 0. We say of an integer d that

"d is the greatest common divisor of a and b"

and write $(a, b) = d$ (other books also write $\gcd(a, b)$), if and only if

(i) $d|a$ and $d|b$, and

(ii) if c is any number such that $c|a$ and $c|b$, then $c \leq d$.

Theorem 1.1 *If $(a, b) = d$, then $(a/d, b/d) = 1$.*

Proof.
Suppose $c = (a/d, b/d)$.
We must prove that $c = 1$. We do this by proving that $c \leq 1$ and $c \geq 1$.
Firstly, $c \geq 1$ is obvious, because 1 is a common divisor of any pair of integers, thus the greatest common divisor of any pair of integers is always at least 1.

$c \leq 1$: Since $c|(a/d)$ and $c|(b/d)$, there exist integers q and r such that

$$\begin{aligned} a/d = cq \qquad &\text{and} \qquad b/d = cr, \\ \text{i.e. } \; a = cqd = (cd)q \qquad &\text{and} \qquad b = crd = (cd)r. \end{aligned}$$

Thus cd is a common divisor of a and b and hence is no greater than the greatest common divisor of a and b, which is d, i.e. $cd \leq d$. Since d is positive, this gives $c \leq 1$ as required.
Hence $c = 1$. ■

1.4 The Division Algorithm

We now prove another result that you already know to be true: the division algorithm.

Theorem 1.2 (The Division Algorithm) *Given positive integers a and b, there exist unique integers q and r, with $0 \leq r < b$, such that*

$$a = bq + r.$$

Proof.
Consider the set of integers $T = \{a, a - b, a - 2b, ...\}$. Let $S = \{s \in T : s \geq 0\}$. Then $S \neq \varnothing$ because $a > 0$ and $a \in T$, so $a \in S$. Also, S consists of nonnegative integers. By the Well-Ordering Principle, S has a smallest element, say $a - qb$. Note that

- $a - qb \geq 0$ (definition of S) and
- $a - qb < b$, for if $a - qb \geq b$, then $a - (q+1)b \geq 0$ and thus $a - (q+1)b \in S$; but then $a - (q+1)b$ is a smaller element of S than $a - qb$, which is not the case.

Let $r = a - qb$. Then
$$a = bq + r, \tag{1.2}$$
where
$$0 \leq r < b \tag{1.3}$$
as required.
We must still prove that q and r are the only integers with this property.
Suppose q_1 and r_1 are integers such that
$$a = bq_1 + r_1, \tag{1.4}$$
where
$$0 \leq r_1 < b. \tag{1.5}$$
Subtracting (1.4) from (1.2) we get
$$0 = b(q - q_1) + (r - r_1). \tag{1.6}$$
Since b divides the left-hand side of (1.6) and the first term on the right-hand side, b also divides the remaining term $(r - r_1)$, that is,
$$r - r_1 = bt \tag{1.7}$$
for some integer t. Combining (1.3) and (1.5) gives
$$-b < r - r_1 < b.$$
Substituting (1.7) we get
$$-b < bt < b.$$
But the only integer t for which this inequality is true is $t = 0$, so $r - r_1 = 0$, i.e. $r = r_1$, and since $b \neq 0$ it follows from (1.6) that $q = q_1$. This proves the uniqueness of q and r. ■

Note: The fact that a multiple bt of an integer b which lies strictly between b and $-b$ can only be a zero multiple ($t = 0$) will be used several times in the course.