

MATH 362

Elementary Number Theory

Notes, 2019

Kieka Mynhardt

Contents

1	Integers	1
	Week 1	1
	1.1 Mathematical Induction	1
	1.2 Division of Integers	3
	1.3 Greatest common divisor	5
	1.4 The Division Algorithm	5
	Week 2	7
	1.5 The Euclidean Algorithm	7
2	Unique Factorization	9
	2.1 Prime Numbers	9
	2.2 The Unique Factorization Theorem	12
3	Linear Diophantine Equations	16
4	Congruences	19
	Week 3	19
	4.1 Definition and Equivalent Conditions	19
	4.2 Properties of the Congruence Relation	20
	4.3 Divisibility by 9	23
5	Linear Congruences	24
	5.1 Solutions of Linear Congruences	25
	5.2 The Chinese Remainder Theorem	29
6	Fermat's and Wilson's Theorems	31
	Week 4	31
	6.1 Fermat's Theorem	31

6.2	Wilson's Theorem	36
7	The Divisors of an Integer	39
7.1	Number of Divisors of an Integer	39
7.2	Sum of Divisors of an Integer	40
8	Perfect Numbers	42
	Week 5	42
8.1	Euclid's Theorem	43
8.2	Euler's Theorem	43
8.3	Mersenne Primes	45
8.4	Last Digits of Perfect Numbers	45
8.5	Other Special Types of Numbers	46
9	Euler's Generalization of Fermat's Theorem	47
9.1	Euler's Phi Function	50
	Week 6	54
9.2	An Application to Cryptography	54
	Week 7	60
10	Primitive roots	60
10.1	The Order of a modulo m	60
10.2	Primitive Roots	64
10.3	Finding Primitive Roots	66
10.4	Integers with Primitive Roots	67
11	Quadratic Congruences	69
	Week 8	69
11.1	Simple Form of a Quadratic Congruence	69
11.2	Number of Solutions of Quadratic Congruences	70
11.3	Quadratic Residues and Nonresidues	71
11.4	Euler's Criterion	72
11.5	The Legendre Symbol	73
11.6	Evaluating Legendre Symbols	75
12	Quadratic Reciprocity	77

<i>CONTENTS</i>	iii
12.1 Gauss's Lemma	77
Week 9	80
12.2 The value of $(2/p)$	80
12.3 Equivalent Form of the Quadratic Reciprocity Theorem	82
13 Numbers in other bases	83
13.1 Writing Base 10 Integers in Other Bases	83
13.2 Converting Integers in Other Bases to Base 10	85
13.3 Working in Other Bases	85
13.4 Decimals in Other Bases	85
14 Duodecimals	86
15 Decimals	87
15.1 Terminating Decimal Expansions	87
Week 10	90
15.2 Non-Terminating Decimal expansions	90
15.3 Expansions in Other Bases	93
16 Pythagorean Triangles	96
16.1 Fundamental Pythagorean Triangles	96
Week 11	99
17 Infinite Descent and Fermat's Conjecture	102
Week 12	102
17.1 The Equation $x^4 + y^4 = z^2$	102
17.2 Infinite Descent	103
18 Sums of Squares	105
18.1 Numbers Representable as Sums of Two Squares	106
18.2 Proof of Necessity (Contrapositive)	106
18.3 Proof of Sufficiency	107
18.3.1 Some Lemmas	107
18.3.2 A result based on Wilson's Theorem	109
18.3.3 Thue's Lemma	109

Week 13	111
18.3.4 Summary	112
18.3.5 Sum of three squares	113
18.3.6 Sum of four squares	113
18.3.7 Sum of cubes	113
18.3.8 Sum of k^{th} powers	113
18.3.9 Goldbach Conjecture	113
19 More About Primes	114
19.1 The Prime Number Theorem	114
19.2 Primes in Arithmetic Progression	116
20 Continued Fractions	118
20.1 Finite Continued Fractions	118
20.2 Infinite Continued Fractions	125

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 $n_0, n_0 + 1, n_0 + 2, \dots$.

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 $n_0, n_0 + 1, \dots, k$ 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 $P(n)$ be a statement about the integer n . If

- (i) $P(1)$ is true, and
- (ii) the truth of $P(k)$, for an arbitrary integer $k \geq 1$, implies the truth of $P(k + 1)$,

then $P(n)$ is true for all positive integers n .

Or more general:

Let $P(n)$ be a statement about the integer n . If

(i) $P(n_0)$ is true, and

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

then $P(n)$ is true for all integers $n \geq n_0$.

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

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 $d|a_1, d|a_2, \dots, d|a_n$, then $d|(c_1a_1 + c_2a_2 + \dots + c_na_n)$ for any integers c_1, c_2, \dots, c_n .

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

Solution

Let $P(n)$ be the statement $6|(n^3 - n)$.

Basis Step: Is $P(1)$ true?

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

Induction hypothesis:

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

To prove: $P(k+1)$ 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 $P(k)$ implies the truth of $P(k+1)$ and the result follows by the principle of induction.

Example: (Omitted in class, read on your own) Let $P(n)$ be the statement

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

Prove that $P(n)$ is true for all nonnegative integers n .

Solution

Basis Step: $P(0)$ 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 $P(k)$ is true for some $k \geq 0$, that is, assume that

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

To prove: $P(k+1)$ 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 $P(k+1)$ is true and the result follows by the principle of induction.

1.3 Greatest common divisor

Let a and b be integers, not 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

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

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 $T = \{a, a - b, a - 2b, \dots\}$. Let $S = \{s \in T : s \geq 0\}$. Then $S \neq \emptyset$ 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

$$a = bq + r, \quad (1.2)$$

where

$$0 \leq r < b \quad (1.3)$$

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

$$a = bq_1 + r_1, \quad (1.4)$$

where

$$0 \leq r_1 < b. \quad (1.5)$$

Subtracting (1.4) from (1.2) we get

$$0 = b(q - q_1) + (r - r_1). \quad (1.6)$$

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,

$$r - r_1 = bt \quad (1.7)$$

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.