

Number Theory

NPTEL - II Web Course

Anupam Saikia

Department of Mathematics
Indian Institute of Technology Guwahati

Contents

1	Divisibility and Primes	1
1.1	Lecture 1	1
1.1.1	Introduction	1
1.1.2	Well-ordering Principle	3
1.1.3	Division Algorithm	4
1.2	Lecture 2	6
1.2.1	Decimal Expansion of a Positive Integer	6
1.2.2	Greatest Common Divisor	7
1.3	Lecture 3	9
1.3.1	Euclid's Algorithm	9
1.3.2	Fibonacci Sequence	10
1.4	Lecture 4	12
1.4.1	Coprime Integers	12
1.4.2	Least Common Multiple	13
1.4.3	Linear Diophantine Equations	14
1.5	Lecture 5	16
1.5.1	Prime Numbers	16
1.5.2	Fundamental Theorem of Arithmetic	17
1.5.3	Infinitude of Primes	18
1.6	Lecture 6	20

CONTENTS

1.6.1	Prime Number Theorem	20
1.6.2	Conjectures about Primes	21
1.6.3	Goldbach Conjecture	22
1.7	Exercises	23
2	Congruence	26
2.1	Lecture 1	26
2.1.1	Congruence	26
2.1.2	Properties of Congruence	28
2.1.3	Divisibility Criterion for 9 and 11	29
2.2	Lecture 2	31
2.2.1	Linear Congruence	31
2.3	Lecture 3	34
2.3.1	Simultaneous Linear Congruences	34
2.3.2	Chinese Remainder Theorem	34
2.4	Lecture 4	38
2.4.1	System of Congruences with Non-coprime Moduli	38
2.5	Lecture 5	41
2.5.1	Linear Congruences Modulo Prime Powers	41
2.5.2	Non-linear Congruences Modulo Prime Powers	42
2.5.3	Hensel's Lemma	43
2.6	Lecture 6	45
2.6.1	Fermat's Little Theorem	45
2.6.2	Wilson's Theorem	46
2.7	Lecture 7	48
2.7.1	Pseudo-primes	48
2.7.2	Carmichael Numbers	50
2.8	Exercises	52

3	Number Theoretic Functions	54
3.1	Lecture 1	54
3.1.1	Greatest Integer Function	54
3.1.2	Applications	57
3.2	Lecture 2	59
3.2.1	Euler's ϕ -function	59
3.2.2	Multiplicativity of Euler's ϕ -function	60
3.2.3	Euler's Theorem	61
3.3	Lecture 3	64
3.3.1	The RSA Cryptosystem	64
3.4	Lecture 4	68
3.4.1	Arithmetic Functions	68
3.4.2	Perfect Numbers	70
3.5	Lecture 5	72
3.5.1	Mobius Function	72
3.5.2	Mobius Inversion Formula	73
3.6	Lecture 6	77
3.6.1	Dirichlet Product	77
3.7	Exercises	82
4	Primitive Roots	85
4.1	Lecture 1	85
4.1.1	Units Modulo an Integer	85
4.1.2	Order of a Unit Modulo an Integer	86
4.1.3	Primitive Roots	87
4.2	Lecture 2	89
4.2.1	Existence of Primitive Roots for Primes	89
4.3	Lecture 3	92

CONTENTS

4.3.1	Primitive Roots for Powers of 2	92
4.3.2	Primitive Roots for Powers of Odd Primes	93
4.3.3	Characterization of Integers with Primitive Roots	94
4.3.4	Application of Primitive Roots	95
4.4	Exercises	97
5	Quadratic Residues	100
5.1	Lecture 1	100
5.1.1	Definition and Examples	100
5.1.2	Euler's Criterion	101
5.1.3	The Legendre Symbol	102
5.2	Lecture 2	104
5.2.1	Gauss Lemma	104
5.2.2	An Application of Gauss Lemma	106
5.3	Lecture 3	107
5.3.1	Quadratic Reciprocity	107
5.4	Lecture 4	111
5.4.1	Quadratic Residues of Powers of an Odd Prime	111
5.4.2	Quadratic Residues of Powers of 2	112
5.4.3	Quadratic Residues of Arbitrary Moduli	113
5.5	Lecture 5	115
5.5.1	The Jacobi Symbol	115
5.5.2	The Jacobi Symbol of -1 and 2	116
5.5.3	Quadratic Reciprocity for the Jacobi Symbol	118
5.6	Exercises	120
6	Binary Quadratic Forms	122
6.1	Lecture 1	122
6.1.1	Definition and Examples	122

CONTENTS

6.1.2	Unimodular Substitution	123
6.1.3	Equivalent Forms	124
6.1.4	Proper Representation	125
6.2	Lecture 2	127
6.2.1	Discriminant of a Quadratic Form	127
6.2.2	Definite and Indefinite Forms	128
6.3	Lecture 3	130
6.3.1	Proper Representation and Equivalent Forms	130
6.3.2	Reduction of Binary Quadratic Forms	131
6.3.3	Reduced Forms of a Given Discriminant	132
6.4	Lecture 4	134
6.4.1	Uniqueness of Equivalent Reduced Form	134
6.5	Lecture 5	137
6.5.1	Class Number	137
6.6	Exercises	139
7	Integers of Special Forms	140
7.1	Lecture 1	140
7.1.1	Fermat Primes	140
7.1.2	Mersenne Primes	141
7.2	Lecture 2	144
7.2.1	Primes Expressible as a Sum of Two Squares	144
7.2.2	Integers Expressible as a Sum of Two Squares	146
7.3	Lecture 3	148
7.3.1	Sum of Three Squares	148
7.3.2	Sum of Four Squares	149
7.3.3	Waring's Problem	151
7.4	Exercises	153

8	Continued Fractions	155
8.1	Lecture 1	155
8.1.1	Finite Continued Fractions	155
8.1.2	General Continued Fraction	157
8.2	Lecture 2	159
8.2.1	Euler's Rule	159
8.2.2	Convergents	160
8.2.3	Application in Solving Linear Diophantine Equations	162
8.3	Lecture 3	163
8.3.1	Infinite Continued Fractions	163
8.4	Lecture 4	166
8.4.1	Periodic Continued Fractions	166
8.4.2	Quadratic Irrationals	167
8.4.3	Purely Periodic Continued Fractions	167
8.5	Lecture 5	169
8.5.1	Conjugate of a Quadratic Irrational	169
8.5.2	Reduced Quadratic Irrational	170
8.6	Lecture 6	173
8.6.1	Continued Fractions of Reduced Quadratic Irrationals	173
8.6.2	Continued Fraction for \sqrt{N}	174
8.6.3	Continued Fraction for Any Quadratic Irrational	175
8.7	Lecture 7	177
8.7.1	Best Rational Approximation to an Irrational	177
8.7.2	A Sufficiently Close Rational is a Convergent	178
8.8	Lecture 8	180
8.8.1	Pell's Equation	180
8.8.2	Fundamental Solution	182
8.9	Exercises	184

CONTENTS

9	Riemann Zeta Function	186
9.1	Lecture 1	186
9.1.1	Riemann Zeta Function	186
9.1.2	Convergence	187
9.1.3	Euler Product	189
9.1.4	Riemann Hypothesis	190
9.2	Lecture 2	191
9.2.1	Dirichlet Series	191
9.2.2	Euler Product for Dirichlet Series	192
9.3	Exercises	195
10	Additional Topics	196
10.1	Lecture 1	196
10.1.1	Lucas Test for Primality	196
10.1.2	Miller-Rabin Test for Primality	200
10.2	Lecture 2	202
10.2.1	Pollard's ρ -Method for Factorization	202
10.2.2	Pollard's $(p - 1)$ -Method for Factorization	203
10.3	Lecture 3	205
10.3.1	Fermat's Factorization	205
10.3.2	Factorization by Continued Fraction	206
10.4	Lecture 4	209
10.4.1	Fermat's Conjecture	209
10.4.2	Pythagorean Triples	210
10.4.3	Method of Infinite Descent	211
10.5	Exercises	213
	Index	215

Notation

\mathbb{N} : the set of natural numbers, i.e., $\{1, 2, \dots\}$

\mathbb{Z} : the set of integers, i.e., $\{0, \pm 1, \pm 2, \dots\}$

\mathbb{Q} : the set of rational numbers, i.e., $\{\frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0\}$

\mathbb{R} : the set of real numbers

For a real number x , $|x|$ denotes the absolute value of x , i.e.,
 $|x| = x$ if $x \geq 0$ and $|x| = -x$ if $x < 0$.

$\#S$: the number of elements in a set S .

$Re(s)$: the real part of a complex number s .

Module 1

Divisibility and Primes

1.1 Lecture 1

Preamble: In this lecture, we will look into the notion of divisibility for the set of integers. Then we will discuss the division algorithm for integers, which is crucial to most of our subsequent results.

Keywords: divisibility, well-ordering principle, induction, division algorithm.

1.1.1 Introduction

We will start by discussing the notion of divisibility for the set \mathbb{Z} of integers. We will be frequently using the fact that both addition and multiplication in \mathbb{Z} are associative, commutative and we also have distributivity property $a(b+c) = ab+ac$ for any integers a, b, c . These operations give the structure of a commutative ring to the set \mathbb{Z} . Divisibility can be studied more generally in any commutative ring, for example, the ring of polynomials with rational coefficients. However, you need not be familiar with concepts of ring theory to understand these lectures as our focus will be on integers.

DEFINITION 1.1. *If a and $b \neq 0$ are integers and $a = qb$ for some integer q , then we say that b divides a , or that a is a multiple of b , or that b is a factor/divisor of a . If b divides a , we denote it by $b \mid a$, and if b does not divide a we denote it by $b \nmid a$.*

For example, $6 \mid 36$ but $7 \nmid 36$. Note that $b \mid 0$ for any non-zero integer b and $1 \mid a$

for any integer a . When we write $b \mid a$, it is tacitly assumed that b is a non-zero integer. We can easily deduce the following properties from the definition of divisibility itself.

PROPOSITION 1.2. *Let a, b, c, d be any non-zero integers.*

1. *If $a \mid b$ and $b \mid c$ then $a \mid c$.*
2. *If $a \mid b$ and $c \mid d$ then $ac \mid bd$.*
3. *If m is a non-zero integer then $a \mid b$ if and only if $ma \mid mb$.*
4. *If d is a non-zero integer such that $d \mid a$ and $a \neq 0$ then $|d| \leq |a|$.*
5. *If a divides x and y then a divides $cx + dy$ for any integers c, d .*
6. *$a \mid b$ and $b \mid a$ if and only if $a = \pm b$.*

Proof: 1. Suppose $b = na$ and $c = mb$, where $n, m \in \mathbb{Z}$. Then $c = m(na) = (mn)a$ and so $a \mid c$.

2. Suppose $b = na$ and $d = mc$ where $n, m \in \mathbb{Z}$. Then $bd = (na)(mc) = (mn)(ac)$, i.e., $ac \mid bd$.

3. Suppose $b = na$. Then $mb = m(na) = n(ma)$ and $ma \mid mb$. Conversely, let $mb = d(ma) = m(da)$. Then $m(b - da) = 0$. But $m \neq 0$, hence $b = da$, i.e., $b \mid a$.

4.

$$\begin{aligned} a = dq &\implies |a| = |dq| = |d| |q| \\ a \neq 0 \implies q \neq 0 &\implies |a| = |d| |q| \geq |d|. \end{aligned}$$

5.

$$\begin{aligned} x = an, \quad y = am \\ \implies cx + dy &= c(an) + d(am) \\ &= a(cn + dm). \end{aligned}$$

6. By (4) above,

$$\begin{aligned} a \mid b &\implies |a| \leq |b|, \\ b \mid a &\implies |b| \leq |a| \\ &\implies |a| = |b|, \\ &\implies a = \pm b. \quad \square \end{aligned}$$

1.1.2 Well-ordering Principle

We begin this section by mentioning the well-ordering principle for non-negative integers.

Well-ordering Principle: *If S is a non-empty set of non-negative integers, then S has a least element, i.e., there is an integer $c \in S$ such that $c \leq x$ for all $x \in S$.*

The principle of mathematical induction follows directly from well-ordering principle. We will use the principle of induction in several arguments later.

THEOREM 1.3. (Principle of Induction): *Let S be set of positive integers such that*

1. $1 \in S$
2. $k \in S \implies k + 1 \in S$

Then S is the the set \mathbb{N} of all natural numbers.

Proof: Consider the complement S' of the set S in \mathbb{N} :

$$S' = \mathbb{N} - S.$$

We want to show that S' is the empty set. Suppose S' is non-empty. Then by well-ordering principle it has a least element, say n' . Clearly, $n' \neq 1$ as $1 \in S$. Therefore $n' - 1$ is a natural number which is not in S' . Hence $n' - 1 \in S$. By hypothesis, $n' - 1 \in S \implies n' \in S$. Therefore, $n' \in S \cap S'$, which is a contradiction. Therefore S' must be empty, and $S = \mathbb{N}$. \square

There is a stronger form of the principle of induction. The stronger version says that if $S \subset \mathbb{N}$ such that

1. $1 \in S$ and
2. $1, 2, \dots, k \in S$ implies $k + 1 \in S$ for any natural number k ,

then $S = \mathbb{N}$. It is an easy exercise to see that both the versions are equivalent. We often use the induction principle in the following way. If a mathematical statement is (i) valid for $k = 1$, and (ii) valid for $k + 1$ if it is valid for k (for all positive integers from 1 to k in the stronger version), then the statement is valid for all positive integers.

Example: Show that $3^n \geq 2n + 1$ for all natural number n .

Proof: Clearly the statement is true for $n = 1$. Suppose it is true for $n = k$. Then,

$$\begin{aligned} 3^{k+1} &= 3 \cdot 3^k \\ &\geq 3 \cdot (2k + 1) = 6k + 3 \\ &> 2k + 3 = 2(k + 1) + 1. \end{aligned}$$

Thus the statement hold for $k + 1$ if it hold for k . Hence the statement holds for all integers n . \square

1.1.3 Division Algorithm

The division algorithm for integers is a fundamental property that we will utilize time and again. The division algorithm follows from the well-ordering principle. It can be stated as follows:

THEOREM 1.4. *If a and b are integers with $b \neq 0$, then there is a unique pair of integers q and r such that*

$$a = qb + r \text{ where } 0 \leq r < |b|.$$

Proof: First assume that $b > 0$. Let

$$S = \{a - nb \mid n \in \mathbb{Z}, a - nb \geq 0\}.$$

The set S is clearly non-empty, as it contains the element

$$a + |a|b \geq a + |a| \geq 0 \quad (\text{with } n = -|a|).$$

By the well-ordering principle, S has a least element r so that $r = a - qb$ for some integer q . So we have $a = qb + r$ with $r \geq 0$. It is now enough to show that $r < b$. If $r \geq b$, then $r - b = a - (q + 1)b \geq 0$ and $r - b$ is also contained in S , which contradicts the fact that r is the least element of S . Hence, we must have $0 \leq r < b$.

To prove uniqueness, suppose $a = qb + r = q_1b + r_1$ with $0 \leq r < b$ and $0 \leq r_1 < b$. If $q \neq q_1$, we can assume $q > q_1$ without loss of generality. Then, $r - r_1 = (q - q_1)b \geq 1 \cdot b = b$. But r and r_1 are both non-negative and are strictly less than b , hence $r - r_1$ can not be bigger than b . So, $q = q_1$ and hence $r = r_1$.

For the case $b < 0$, simply apply the result for $-b$ to obtain unique integers q and r such that $a = q(-b) + r = (-q)b + r$ where $0 \leq r < -b = |b|$. \square

For example, with $a = 54$ and $b = -24$, we have

$$54 = (-2)(-24) + 6, \text{ with } 0 \leq 6 < |-24|.$$

Application: If n is the square of an odd integer, then n leaves the remainder 1 when divided by 8, i.e., a perfect odd square must be of the form $8k + 1$.

Proof: Let $n = (2a + 1)^2 = 4a^2 + 4a + 1 = 4a(a + 1) + 1$. Now one of a or $a + 1$ must be even, hence $n = 8k + 1$ for some integer k . \square