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

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 30
2.2 Lecture 2 31
2.2.1 Linear Congruence 31
2.3 Lecture 3 35
2.3.1 Simultaneous Linear Congruences 35
2.3.2 Chinese Remainder Theorem 35
2.4 Lecture 4 39
2.4.1 System of Congruences with Non-coprime Moduli 39
2.5 Lecture 5 42
2.5.1 Linear Congruences Modulo Prime Powers 42
2.5.2 Non-linear Congruences Modulo Prime Powers 43
2.5.3 Hensel's Lemma 44
2.6 Lecture 6 46
2.6.1 Fermat's Little Theorem 46
2.6.2 Wilson's Theorem 47
2.7 Lecture 7 49
2.7.1 Pseudo-primes 49
2.7.2 Carmichael Numbers 51
2.8 Exercises 53

3 Number Theoretic Functions **55**

3.1 Lecture 1 55

3.1.1 Greatest Integer Function 55

3.1.2 Applications 58

3.2 Lecture 2 60

3.2.1 Euler's ϕ-function 60

3.2.2 Multiplicativity of Euler's ϕ-function 61

3.2.3 Euler's Theorem 62

3.3 Lecture 3 65

3.3.1 RSA cryptosystem 65

3.4 Lecture 4 69

3.4.1 Arithmetic Functions 69

3.4.2 Perfect Numbers 71

3.5 Lecture 5 73

3.5.1 Mobius Function 73

3.5.2 Mobius Inversion Formula 74

3.6 Lecture 6 78

3.6.1 Dirichlet Product 78

3.7 Exercises 83

4 Primitive Roots **86**

4.1 Lecture 1 86

4.1.1 Units Modulo an Integer 86

4.1.2 Order of a Unit Modulo an Integer 87

4.1.3 Primitive Roots 88

4.2 Lecture 2 90

4.2.1 Existence of Primitive Roots for Primes 90

4.3 Lecture 3 92

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 . . . 119

6 Binary Quadratic Forms **121**
6.1 Lecture 1 . . . 121
6.1.1 Definition and Examples . . . 121

6.1.2 Unimodular substitution . . . 122
6.1.3 Equivalent Forms . . . 123
6.1.4 Proper Representation . . . 124
6.2 Lecture 2 . . . 126
6.2.1 Discriminant of a Quadratic Form . . . 126
6.2.2 Definite and Indefinite Forms . . . 127
6.3 Lecture 3 . . . 129
6.3.1 Proper Representation and Equivalent Forms . . . 129
6.3.2 Reduction of Binary Quadratic Forms . . . 130
6.3.3 Reduced Forms of a Given Discriminant . . . 131
6.4 Lecture 4 . . . 133
6.4.1 Uniqueness of Equivalent Reduced Form . . . 133
6.5 Lecure 5 . . . 136
6.5.1 Class Number . . . 136
6.6 Exercises . . . 138

7 Integers of Special Form **139**

7.1 Lecture 1 . . . 139
7.1.1 Fermat Primes . . . 139
7.1.2 Mersenne Primes . . . 140
7.2 Lecture 2 . . . 142
7.2.1 Primes Expressible as a Sum of Two Squares . . . 142
7.2.2 Integers Expressible as a Sum of Two Squares . . . 144
7.3 Lecture 3 . . . 146
7.3.1 Sum of Three Squares . . . 146
7.3.2 Sum of Four Squares . . . 147
7.3.3 Waring's Problem . . . 149
7.4 Exercises . . . 151

8 Continued Fractions **153**

8.1 Lecture 1 . . . 153

8.1.1 Finite Continued Fractions . . . 153

8.1.2 General Continued Fraction . . . 155

8.2 Lecture 2 . . . 157

8.2.1 Euler's Rule . . . 157

8.2.2 Convergents . . . 158

8.2.3 Application in Solving Linear Diophantine Equations . . . 160

8.3 Lecture 3 . . . 161

8.3.1 Infinite Continued Fractions . . . 161

8.4 Lecture 4 . . . 165

8.4.1 Periodic Continued Fractions . . . 165

8.4.2 Quadratic Irrationals and Their Continued Fractions . . . 165

8.5 Lecture 5 . . . 168

8.5.1 Conjugate of a Quadratic Irrational . . . 168

8.5.2 Reduced Quadratic Irrational . . . 169

8.6 Lecture 6 . . . 172

8.6.1 Continued Fractions of Reduced Quadratic Irrationals . . . 172

8.6.2 Continued Fraction for $\sqrt{N}$ . . . 173

8.6.3 Continued Fraction for Any Quadratic Irrational . . . 173

8.7 Lecture 7 . . . 175

8.7.1 Best Rational Approximation to an Irrational . . . 175

8.7.2 A Sufficiently Close Rational is a Convergent . . . 176

8.8 Lecture 8 . . . 178

8.8.1 Pell's Equation . . . 178

8.8.2 Fundamental Solution . . . 180

8.9 Exercises . . . 182

9 Riemann Zeta Function **184**

9.1 Lecture 1 . . . 184

9.1.1 Riemann Zeta Function . . . 184

9.1.2 Convergence . . . 185

9.1.3 Euler Product . . . 187

9.1.4 Riemann Hypothesis . . . 188

9.2 Lecture 2 . . . 189

9.2.1 Dirichlet series . . . 189

9.2.2 Euler Product for Dirichlet Series . . . 190

10 Additional Topics **193**

10.1 Lecture 1 . . . 193

10.1.1 Lucas Test for primality . . . 193

10.1.2 Miller-Rabin Test for Primality . . . 197

10.2 Lecture 2 . . . 199

10.2.1 Pollard's ρ-Method for Factorization . . . 199

10.2.2 Pollard's $(p-1)$-Method for Factorization . . . 200

10.3 Lecture 3 . . . 202

10.3.1 Fermat's Factorization . . . 202

10.3.2 Continued Fraction Method . . . 203

10.4 Lecture 4 . . . 206

10.4.1 Fermat's Conjecture . . . 206

10.4.2 Pythagorean Triples . . . 207

10.4.3 Method of Infinite Descent . . . 208

Notation

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

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

$\mathbb{Q}$: 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, $\mid x \mid$ denotes the absolute value of x, i.e.,
$\mid x \mid = x$ if $x \geq 0$ and $\mid x \mid = -x$ if $x < 0$.

#S: the number of elements is 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. We will discuss the division algorithm for integers, which is crucial to most of our subsequent results.

Keywords: divisibility, greatest common divisor, well-ordering, 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 integers a, b, c. These operations give the structure of a commutative ring to the set $\mathbb{Z}$. However, you need not be familiar with concepts of ring theory to understand these lectures. Divisibility can be studied in other set-up too, for example, in the set of polynomials with rational coefficients, or more generally, in any commutative ring.

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 form 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 $m \neq 0$ then $a \mid b$ if and only if $ma \mid mb$.*
4. *If $d \mid a$ 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)

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

(6) By (4) above,

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

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 is a subset of natural numbers such that

1. $1 \in S$ and

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

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

$$\begin{aligned} 3^{k+1} &= 3.3^k \\ &\geq 3.(2k+1) = 6k+3 \\ &> 2k+2. \end{aligned}$$

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 ad 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

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

By the well-ordering principle, S has a least element r, which has to be of the form $a-qb$ 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, $r-r_1 = (q-q_1)b \geq 1.b = b$. 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 $0 \leq r < -b = |b|$. □

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 $n = 2a + 1$. Then $n^2 = 4a^2 + 4a + 1 = 4a(a + 1) + 1$. Now one of a or $a + 1$ must be even, hence $n^2 = 8k + 1$ for some integer k. □

1.2 Lecture 2

Preamble: We will show why any positive integer has a unique decimal expansion. Then we will define the greatest common divisor (gcd). We will show that the gcd of two integers can be expressed as a linear combination of the two integers.

Keyword: decimal expansion, greatest common divisor, Bezout's theorem

1.2.1 Decimal expansion of a Positive Integer

We take it for granted that any positive integer has a decimal expansion. Now we will give a rigorous proof based on division algorithm. Our proof will work for not just base 10 but any base $b > 1$.

PROPOSITION 1.5. *Let $b > 1$ be a positive integer. Any integer n can be written uniquely as*

$$n = c_k.b^k + c_{k-1}.b^{k-1} + \cdots + c_1.b + c_0, \qquad 0 \leq c_i < b, \;\; b_k \neq 0$$

for some non-negative integer.

Proof: We will first show the existence of such an expansion. If $n < b$, then $n = c_0$ is the required expansion. If $n \geq b$, by division algorithm we can write

$$n = bq + c_0, \qquad 0 \leq c_0 \leq b, \;\; q \geq 1.$$

If $q < b$, then the above is the expansion we are looking for. If $q > b$, we write

$$q = bq_1 + c_1, \qquad 0 \leq c_1 \leq b, \;\; q_1 \geq 1$$

and obtain

$$n = b(bq_1 + c_1) + c_0 = b^2q_1 + bc_1 + c_0.$$

As before, we get the required expansion if $q_1 < b$. If $q_1 > b$, we again use the division algorithm. As n is a fixed integer, n will be less than some power of b and we must have $1 < q_k < b$ for some k. This proves the existence. Now suppose we have two such expansions for the same integer n, i.e.,

$$c_k.b^k + c_{k-1}.b^{k-1} + \cdots + c_1.b + c_0 = d_k.b^k + d_{k-1}.b^{k-1} + \cdots + d_1.b + d_0.$$

Let i be the first suffix for which $c_i \neq d_i$. Then, we have

$$\begin{aligned} & b^{i+1} \mid \Big[\big(c_k.b^k + \cdots + c_{i+1}.b^{i+1} + c_i.b^i\big) - \big(d_k.b^k + \cdots + d_{i+1}.b^{i+1} + d_i.b^i \bmod b^{i+1}\big)\Big] \\ \implies \quad & b^{i+1} \mid \big(c_i.b^i - d_i.b^i\big) \\ \implies \quad & b \mid (c_i - d_i). \end{aligned}$$

As $0 \leq c_i, d_i < b$, the last congruence must imply $c_i - d_i = 0$, which is a contradiction. This proves the uniqueness. □

1.2.2 Greatest Common Divisor

DEFINITION 1.6. *Let a and b be two integers (not both 0). If an integer d divides both a and b, we say that d is a* **common divisor** *of a and b. The* **greatest common divisor** *of two integers a and b is the unique* **positive** *integer d satisfying*
(1) $d \mid a$ and $d \mid b$.
(2) If $c \mid a$ and $c \mid b$ then $c \leq d$.
We denote the greatest common divisor of a and b by $gcd(a, b)$ or simply by (a, b).

When talking about $gcd(a, b)$, we avoid the case of both the integers a and b being 0 as any non-zero integer is a common divisor for both, and it would not be possible to define the greatest amongst those. The definition of gcd can easily be extended to any finite set of integers (not all 0).

For example, the set of positive divisors of -32 and 44 are 1, 2 and 4. Hence $gcd(-32, 44) = 4$. Similarly, $gcd(12, 42) = 6$. Observe that

$$\begin{aligned} gcd(-32, 44) &= 8 = -32 \times (-3) + 44 \times (-2) \\ gcd(12, 42) &= 6 = 12 \times 4 + 42 \times 9 - 1). \end{aligned}$$

In the above two examples, the gcd of two integers turns out to be an (integral) linear combination of the integers. The following theorem states that it is always true. This result is known as Bezout's theorem.

THEOREM 1.7. *If a and b are two integers, not both zero, then their gcd can be written as $ax + by$ for some integers x and y.*

Proof: Consider the set

$$S = \{ax + by > 0 | x, y \in \mathbb{Z}\}$$

The set S is clearly nonempty, as

$$0 < a.a + b.b \in S.$$

By well-ordering principle, S has a least element d. It is enough to show that d is the gcd of a and b, because d must have the form $ax_0 + by_0$ for some integers x_0 and y_0 as $d \in S$. Observe that if c is a common divisor of a and b, then c also divides $ax + by$ for any choice of integers x and y. Therefore, c divides d, and in particular, $c \leq d$. We next show that d divides a and b. By division algorithm, $a = dq + r$ for some $0 \leq r < d$. Then $r = a - dq = a - (ax_0 + by_0) = a(1 - x_0) + b(-y_0)$. If $r > 0$, r will be an element in S which is smaller than d. This is a contradiction to the minimality of d in S. Hence, $r = 0$ and $d \mid a$. Similarly, $d \mid b$. Thus, $d = ax_0 + by_0$ is the gcd. □

Note that such a linear combination is not unique. In fact, there are infinitely many integers x and y such that $d = ax + by$. If $d = ax_0 + by_0$, then clearly $d = a(x_0 + bn) + b(y_0 - an)$ for any integer n. The above theorem confirms only the existence of a linear combination of two integers a and b expressing the gcd d, but it does not tell us how to find the integers x and y giving $d = ax + by$. In the next lecture we will introduce Euclid's algorithm, which will provide us a method of determining x and y from a and b. Before discussing Euclid's algorithm, we need to characterize the gcd of two integers in the following way as well:

PROPOSITION 1.8. *Let a and b are two integers, not both zero. Then a positive integer d is the gcd of a and b if and only if*

1. $d \mid a, \;\; d \mid b$
2. $c \mid a, \;\; c \mid b \implies c \mid d$

Proof: If d is the gcd of a and b, the first property clearly holds. Now, by the preceding theorem, we have $d = ax_0 + by_0$ for some integers x_0 and y_0. Hence, any c dividing a and b will divide $ax_0 + by_0 = d$. Conversely, if an integer d satisfies the two properties mentioned above, then any common divisor c of a and b will divide d, and hence will be less that d. □

1.3 Lecture 3

Preamble: We will discuss Euclid's algorithm for finding the greatest common divisor of two non-zero integers. The algorithm not only determines the gcd, but it also allows us to express the gcd as an integral linear combination of the two integers.

Keywords: Euclid's algorithm, Fibonacci sequence

1.3.1 Euclid's Algorithm

While finding the gcd of two integers (not both 0), we can of course list all the common divisors and pick the greatest one amongst those. However, if a and b are very large integers, the process is very much time consuming. However, there is a far more efficient way of obtaining the gcd. That is known as the *Euclid's algorithm*. This is based on the division algorithm for integers.

LEMMA 1.9. *If $a = qb + r$ then the $gcd(a, b) = gcd(b, r)$.*

Proof: Let $d = gcd(a, b)$ and $d_1 = gcd(b, r)$. Then, $d|a$, $d|b$ implies $d|(a - qb)$ i.e, $d|r$. Thus d is a common divisor of b and r and hence $d|d_1$. Similarly, $d_1|b, d_1|r$ implies $d_1|(bq + r)$ i.e., d_1 divides both a and b. then, $d_1|d$. Thus, $d = d_1$, as both d and d_1 are positive by our definition of gcd. □

Euclid' algorithm is an efficient way of computing the gcd of two integers by repeated application of the above lemma to reduce the size of the integers concerned at each step. Suppose we want to find the gcd of two integers a and b, neither of them being 0. As $gcd(a, b) = gcd(a, -b) = gcd(-a, b) = gcd(-a, -b)$, we may assume $a > b > 0$. By performing division algorithm repeatedly, we obtain

$$\begin{aligned}
a &= bq_1 + r_1, && 0 \le r_1 < b \\
b &= r_1q_2 + r_2, && 0 \le r_2 < r_1 \\
r_1 &= r_2q_2 + r_3, && 0 \le r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1}q_n + r_n, && 0 \le r_n < r_{n-1} \\
r_{n-1} &= r_nq_{n+1} + r_{n+1}, && 0 \le r_{n+1} < r_n
\end{aligned}$$

As we have a decreasing sequence of non-negative integers $b > r_1 > r_2 > \ldots > r_n > r_{n+1}$ we must have $r_{n+1} = 0$ for some n. Then, by applying the previous lemma repeatedly, we find that

$$gcd(a, b) = gcd(r_1, b) = gcd(r_2, r_1) = \ldots = gcd(r_{n-1}, r_{n-2}) = gcd(r_n, r_{n-1}) = r_n.$$

Thus, the last non-zero remainder r_n in in the above process gives us the remainder. □

For example, let $a = 66$ and $b = 26$. Then, we have

$$\begin{aligned} 66 &= 26 \times 2 + 14 \\ 26 &= 14 \times 1 + 12 \\ 14 &= 12 \times 1 + 2 \\ 12 &= 2 \times 6 + 0. \end{aligned}$$

The last non-zero remainder in the above process is 2, hence, $gcd(66, 26) = 2$.

Moreover, by going backwards, we can write the gcd as an integral linear combination of a and b:

$$\begin{aligned} 2 &= 14 - 12 \\ &= 14 - (26 - 14 \times 1) \\ &= 14 \times 2 - 26 \times 1 \\ &= (66 - 2 \times 26) \times 2 - 26 \times 1 \\ &= 66 \times 2 - 26 \times 5. \end{aligned}$$

Thus, from Euclid's algorithm we can explicitly find integers x and y such that $gcd(a, b) = ax + by$. Hence it provides a constructive proof of Bezout's theorem that we discussed in the previous lecture. This is very useful when we solve linear Diophantine equations or linear congruences, which will be discussed later. We will also see the utility of Euclid's algorithm in sections 3.3, 10.1 and 10.2.

1.3.2 Fibonacci Sequence

As another application of Euclid's algorithm, we will show that two consecutive terms of the Fibonacci sequence are coprime.

DEFINITION 1.10. *The Fibonacci sequence is a sequence of positive integers defined recursively by*

$$F_0 = 1,\ F_1 = 1,\ F_2 = 2,\ \ldots,\ F_n = F_{n-1} + F_{n-2} \quad \forall n \geq 2.$$

THEOREM 1.11.

$$gcd(F_{n+1}, F_n) = 1.$$

Proof: By definition, we have

$$\begin{aligned} F_{n+1} &= 1.F_n + F_{n-1} \\ F_n &= 1.F_{n-1} + F_{n-2} \\ F_{n-1} &= 1.F_{n-2} + F_{n-3} \\ \vdots &\quad \vdots \\ F_3 &= 1.F_2 + F_1 \\ F_2 &= 1.F_1. \end{aligned}$$

The steps above are nothing but Euclid's algorithm for the gcd of F_{n+1} and F_n. Hence we can conclude that $F_1 = 1$ is the gcd, and hence F_{n+1} and F_n are coprime. □

1.4 Lecture 4

Preamble: In this lecture, we will discuss coprime integers. We will then discuss the least common multiple of two non-zero integers. Finally, we will look into linear equation in two variables with integral coefficients.

Keywords: co-prime integers, least common multiple, linear Diophantine equations

1.4.1 Coprime Integers

DEFINITION 1.12. *Two integers a and b are called mutually coprime if their greatest common divisor is* 1.

For example, 9 and 34 are mutually coprime, or coprime in short.

PROPOSITION 1.13. *Two integers a and b are mutually coprime if and only if there exist integers x and y such that $ax + by = 1$.*

Proof: If a and b are coprime, by Bezout's theorem there exist integers x and y such that $ax + by = 1$. Conversely, if $ax + by = 1$ for some integers x and y, then $d \mid a$ and $d \mid b$ imply that $d \mid (ax + by)$, i.e., $d \mid 1$. Thus, $gcd(a, b) = 1$. □

COROLLARY 1.14. *If $d = gcd(a, b)$, then $\frac{a}{d}$ and $\frac{b}{d}$ are coprime.*

Proof: We have $d = ax + by$, hence $1 = \frac{a}{d}x + \frac{b}{d}y$, and by the proposition above, $\frac{a}{d}$ and $\frac{b}{d}$ are coprime. □

COROLLARY 1.15. *If a and b are coprime and $a \mid bc$ then $a \mid c$.*

Proof: If $(a, b) = 1$, we have $ax + by = 1$ for some integers x and y. Multiplying both sides by c, we obtain

$$acx + bcy = c.$$

Clearly, $a \mid acx$ and $a \mid bc$, hence $a \mid bcy$, hence $a \mid c$. □

COROLLARY 1.16. *If a and b are coprime, then $a \mid c$ and $b \mid c$ imply that $ab \mid c$.*

Proof: There are integers m and n such that $c = am$ and $c = bn$. We also have $ax+by = 1$ for some integers x and y. Hence,

$$\begin{aligned} c &= c(ax + by) \\ &= (bn)ax + (am)by \\ &= ab(nx + my). \qquad \square \end{aligned}$$

1.4.2 Least Common Multiple

Let a and b be two integers. An integer m is called a *common multiple* of a and b if $a \mid m$ and $b \mid m$. If we take S to be the set of all non-negative common multiples of a and b, then S is clearly non-empty as $|ab| \in S$. By the Well-ordering Principle, S has a least element l. That element l is called the *least common multiple* of a and b, written as $lcm(a, b)$ or $[a, b]$ in short. As the name suggest, $[a, b]$ is the least integer amongst all the non-negative common multiples of a and b. A non-negative integer l is the lcm of a and b if and only if
(1) $a \mid l$ and $b \mid l$.
(2) If $c \geq 0$ with $a \mid c$ and $b \mid c$, then $l \leq c$.
Remark: In stead of (2) above, we can also write the second condition as
(2)$'$ If $a \mid c$ and $b \mid c$, then $l \mid c$.

Verify that for any two non-zero integers a and b, if l is the non-negative integer satisfying (1) and (2) and l' is the non-negative integer satisfying (1) and (2)$'$ above, then $l = l'$.

Example: $[24, -36] = 72$.

It is clear from definition that that

$$[a, -b] = [-a, b] = [-a, -b] = [a, b].$$

PROPOSITION 1.17. *For any two integers a and b (not both zero), we have $(a, b)[a, b] = ab$.*

Proof: We may assume a and b are both positive. Let $d = (a, b)$. Then $a = da_1,\ b = db_1$. We need to show that $[a, b] = da_1b_1$. Clearly, da_1b_1 is a common multiple of a and b as $a \mid (da_1)b_1$ and $b \mid a_1(db_1)$.

It is now enough to show that any common multiple of a and b is divisible by da_1b_1. Now suppose c is an integer such that $a \mid c$ and $b \mid c$. Then, $a_1 \mid \frac{c}{d}$ and $b_1 \mid \frac{c}{d}$. As

$(a_1, b_1) = 1$, by corollary 1.5 we have $a_1 b_1 \mid \frac{c}{d}$, i.e., $a_1 b_1 q = \frac{c}{d}$, i.e., $c = (da_1 b_1)q$ and it concludes the proof. $\square$

1.4.3 Linear Diophantine Equations

Diophantus was a Greek mathematician of the 3rd century BC. He considered polynomial equations with coefficients in integers and their solutions in integers or rational numbers. Such equations are known as Diophantine equations. By *linear Diophantine equation*, we mean an equation of the form

$$ax + by = c,$$

where a, b, c are integers and x and y are two unknowns that we want to solve in integers. First, we will derive a necessary and sufficient condition involving the coefficients a, b and c which guarantee the existence of a solution. Then, we will show how one can obtain all the solutions by applying Euclid's algorithm to find the gcd of a and b.

PROPOSITION 1.18. *The linear Diophantine equation $ax + by = c$ has solution in integers if and only if $d = gcd(a, b)$ divides c.*

Proof: If there is a solution (x_0, y_0) in integers, we have $d \mid ax_0$ and $d \mid by_0$, hence $d \mid (ax_0 + by_0)$, i.e., $d \mid c$.
Conversely, suppose $gcd(a, b) = d$ and $d \mid c$, say $c = dc_1$. Then, $d = ax_1 + by_1$ where x_1 and y_1 are integers (which can be determined by Euclid's algorithm). Multiplying the last equality by c_1, we obtain $c = dc_1 = ac_1x_1 + bc_1y_1$ so that we can take c_1x_1 and c_1y_1 as solutions. $\square$

COROLLARY 1.19. *Let $d = gcd(a, b)$. If $d \mid c$ and $(x_0,\ y_0)$ is a solution of the linear Diophantine equation $ax + by = c$, then all integral solutions are given by*

$$x = x_0 + \frac{bn}{d},\ \ y = y_0 - \frac{an}{d},\ \ n \in \mathbb{Z}.$$

Proof: Clearly, if (x_0, y_0) is a solution of $ax + by = c$ then so is

$$\left(x_0 + \frac{bn}{d}, y_0 - \frac{an}{d}\right)$$

for any $n \in \mathbb{Z}$. It remains to show that any other solution (x_1, y_1) is of the given form for some integer n. Suppose $a = da_1,\ \ b = db_1$, then $gcd(a_1, b_1) = 1$. But

$$\begin{aligned} a(x_1 - x_0) + b(y_1 - y_0) &= 0 \\ \implies (x_1 - x_0)a_1 &= (y_1 - y_0)(-b_1) \\ \implies a_1 \mid (x_1 - x_0) \qquad & b_1 \mid (y_1 - y_0) \qquad \text{as } gcd(a_1, b_1) = 1 \\ \implies \frac{(x_1 - x_0)}{b_1} &= \frac{(y_1 - y_0)}{-a_1} = n \end{aligned}$$

for some integer n, and the corollary follows. $\square$

Example: Find all the solutions of $24x + 34y = 6$.

First observe that $gcd(24, 34)$ is 2 which divides 6, so there are solutions to the above linear Diophantine equation. By applying Euclid's algorithm for the gcd of 24 and 34, we see that

$$\begin{aligned} 34 &= 24 \times 1 + 10, \\ 24 &= 10 \times 2 + 4 \\ 10 &= 4 \times 2 + 2 \\ 4 &= 2 \times 2. \end{aligned}$$

Hence,

$$\begin{aligned} 2 &= 10 - 4 \times 2 \\ &= 10 - (24 - 10 \times 2) \times 2 \\ &= 24 \times (-2) + 10 \times 5 \\ &= 24 \times (-2) + (34 - 24) \times 5 \\ &= 24 \times (-7) + 34 \times 5 \\ \text{Thus, } 6 &= 24 \times (-21) + 34 \times 15. \end{aligned}$$

Hence $x_0 = 15,\ y_0 = -21$ is a solution, and the set of all solutions is given by

$$\{x = -21 + \frac{24}{2}n = -21 + 12n, \quad y = 15 - \frac{34}{2}n = 15 - 17n,\ n \in \mathbb{Z}\}.$$

1.5 Lecture 5

Preamble: In this lecture, we will discuss prime numbers. We will then state and prove the fundamental theorem of arithmetic. We will also mention certain results and conjectures concerning the distribution of primes in the set of natural numbers.

Keywords: primes, fundamental theorem of arithmetic, prime number theorem.

1.5.1 Prime Numbers

Prime numbers hold the crucial key in our understanding of numbers. They are the building blocks from which all other integers can be composed as products.

DEFINITION 1.20. *A natural number p is called prime if it has exactly two factors, namely* 1 *and p itself.*

For example, 2, 3, 5, etc are prime numbers. The integer 1 is not considered as prime as 1 has only one factor. Note that we can extend our definition to include negative integers having no non-trivial factors, where trivial factors of an integer n mean ± 1 and $\pm n$. This notion can be readily generalized to integral domains other than the ring of integers, giving us what are known as *irreducible elements*.

PROPOSITION 1.21. *Let p is a prime number and a, b are integers such that $p \mid ab$. Then $p \mid a$ or $p \mid b$.*

Proof: Suppose $p \nmid a$. Then $(p, a) = 1$ as p has no other divisors except 1 and p. By corollary 1.4 of lecture 2, we must have $p \mid b$. $\square$

The above property can be considered in commutative rings other that $\mathbb{Z}$ and it lead to the notion of *prime elements* in a commutative ring. Note that the above proposition readily gives the following corollary.

COROLLARY 1.22. *If p is a prime number such that $p \mid a_1.a_2.\ldots.a_n$, then $p \mid a_i$ for some $1 \leq i \leq n$.*

1.5.2 Fundamental Theorem of Arithmetic

THEOREM 1.23. *Any natural number $n > 1$ can be written as a product*

$$n = p_1^{e_1} p_2^{e_2} \ldots . p_r^{e_r},$$

where p_i's are distinct primes dividing n and e_i are positive integers. This decomposition is unique up to reordering of the prime powers.

For example, $18 = 2^1 3^2$, $1000 = 2^3.5^3$.

Proof: *Existence*: We can use induction on n. clearly, the statement is trivially true for $n = 2$, as 2 is a prime anyway. Suppose the statement is true for $n = 2,\ 3,\ \ldots,\ k$. Now consider $k + 1$. It is either a prime, in which case the theorem is valid. If $k + 1$ is not prime, we have $k+1 = ab$ where $1 < a \leq k$ and $1 < b \leq k$. By the induction hypothesis, we both a and b can be written as a product of prime powers, giving us ab as product of prime powers too.

Uniqueness If possible, let

$$n = p_1^{e_1} p_2^{e_2} \ldots . p_r^{e_r} = q_1^{f_1} q_2^{f_2} \ldots . p_k^{f_k}.$$

As $p_1 \mid n$, it divides $q_1^{f_1} q_2^{f_2} \ldots . p_k^{f_k}$, and by the previous corollary, p divides some prime q_j. We can assume, if necessary by renumbering the primes q_j, that p_1 divides q_1. But q_1 is a prime itself, hence $p_1 = q_1$. If $e_1 > f_1$, then after canceling p^{f_1} from both sides, we will see that $p_1 = q_1$ divides $q_2^{f_2} \ldots . p_k^{f_k}$, which will imply that the prime q_1 divides some other prime $q_j \neq q_1$, which is not possible. Similarly, $e_1 < f_1$ leads to a contradiction. Hence we must have $e_1 = f_1$, so that we can cancel $p_1^{e_1}$ from both the factorizations. Now we can argue similarly for p_2, and then for its index e_2. We can not have some primes left in one of the factorizations, as it will lead to 1 being expressed as a product of primes. □

As an application, let us prove the following:

PROPOSITION 1.24. *If a and b are relatively prime natural numbers such that their product is a perfect square, then both a and b must be perfect squares.*

Proof: As ab is a square, we have

$$ab = \left(p_1^{e_1} . \cdots . p_r^{e_r}\right)^2,$$

where p_i's are distinct primes. If some $p_j \mid a$, then $p_j \nmid b$ as $gcd(a, b) = 1$ and we must have $p_j^{2e_j} \mid a$. By uniqueness of factorization, a can not have any prime powers other than those occurring in the factorization of ab. Thus the factorization of a involve only even powers of primes, and it must be a perfect square. Similarly, b must be a perfect square. □

1.5.3 Infinitude of Primes

The following observation was made by the Greek mathematician Euclid in his book *Elements* written in the third century BC.

THEOREM 1.25. *There are infinitely many primes.*

Proof: If possible, suppose there are only finitely many primes $p_1,\ p_2,\ \ldots,\ p_k$. Consider $N = p_1.p_2.\ldots.p_k + 1$. Now N is not divisible by any of the primes $p_1,\ p_2,\ \ldots,\ p_k$. Hence either N is a prime, or it is divisible by a prime which is not one of $p_1,\ p_2,\ \ldots,\ p_k$. This leads to a contradiction. □

Clearly, any prime number other than 2 is either of the form $4k + 1$ or $4k + 3$. This follows from division algorithm, when we look at the remainder upon division by 4. One can easily show that there are infinitely many primes of the form $4k + 3$.

THEOREM 1.26. *There are infinitely many primes of the form* $4k + 3$.

Proof: The proof is analogous to Euler's proof of existence for infinitely many primes. If possible, assume that there are only finitely many primes of the form $4k + 3$. Suppose we denote them by $3 = p_1,\ p_2 \cdots\ p_n$. Now consider the number

$$N = 4p_2 \cdots p_n + 3.$$

Now, $p_i \mid N$ for $i > 1$ would imply $p_i \mid 3$, which is not possible. Moreover, $3 \mid N$ would mean $3 \mid p_j$ for some prime $p_j > 3$ which is also not possible. Therefore, N is not divisible by any of the listed primes p_i. Therefore, N is either a prime number or is divisible by some prime q other tan p_i's. If all the prime factors of N are of the form $4k + 1$, then N will also be of the form $4k + 1$, which is clearly not the case. Therefore, there must be a prime factor of N of the form $4k + 3$, which is not in $\{p_1,\ \cdots,\ p_n\}$. □

Note that 3, 7, 11, 15, $\cdots$ is an arithmetic progression, which contains infintely many primes by our theorem. One can prove a much stronger result about existence of primes

in an arithmetic progression. The stronger result is due to French mathematician Dirichlet.

THEOREM 1.27. *Let $a,\ a+d,\ a+2d,\ \ldots$ be an infinite arithmetic progression. If a and d are cop-rime, there are infinitely many primes in this progression.*

For example, one can say that there are infinitely many primes in the sequence 14, 19, 24, 29, ... The proof of the above involves Dirichlet L-function and is beyond the scope of these notes. Roughly speaking, one shows that the sum of the reciprocals of all the primes of the form $a+nd$ (where $\gcd(a,d)=1$ and n is a positive integer) is infinite. It follows that the number of primes in such a progression must be infinite.

The next two results show that while there are arbitrarily large gaps between two successive primes, we can still guarantee the existence of the n-th prime within $\{1,\ 2,\ , 2^{2^{n-1}}\}$.

THEOREM 1.28. *For any integer n, there exist n consecutive composite numbers. In other words, the gaps between two successive primes is arbitrarily large.*

Proof: We simply have to observe that each of the consecutive integers

$$(n+1)!+2,\ (n+1)!+3,\ \cdots,\ (n+1)!+n+1$$

is composite. □

THEOREM 1.29. *If p_n is the n-th prime number, then*

$$p_n < 2^{2^{n-1}}.$$

Proof: We will prove by induction on n. The assertion is clearly true for $n=1$. Suppose it is true for $n=k$. We know that $M = p_1p_2\cdots p_k+1$ is coprime to each p_i, $i \le k$. Therefore, either M is a prime or has a prime factor other than the $p_1,\ \cdots,\ p_k$. Therefore, the $(k+1)$st rime p_{k+1} can not exceed M. Hence,

$$\begin{aligned} p_{k+1} &\le p_1p_2\cdots p_k+1 \\ &< 2.2^2.2^{2^2}.\cdots.2^{2^{k-1}} \\ &= 2^{1+2+2^2+\cdots+2^{k-1}} \\ &= 2^{2^k-1}. \qquad \square \end{aligned}$$

1.6 Lecture 6

Preamble: In this lecture we will discuss how primes are distributed amongst the set of natural numbers.

Keywords: prime number theorem, Goldbach conjecture, twin prime conjecture

1.6.1 Prime Number Theorem

One way to look at how prime numbers are distributed is to count the number of integers not exceeding a real number x. This gives us a function, which we denote by $\pi(x)$. By definition,

$$\pi(x) = \#\{p \leq x \mid p \text{ is a prime}\}.$$

For example, $\pi(9.5) = 4$. The *Prime Number Theorem* tells us about the *asymptotic* behavior of $\pi(x)$, i.e., the behavior of $\pi(x)$ as a function when x is very large. Gauss, one of the most influential mathematician, conjectured in 1793 that the value of $\pi(x)$ is very close to the value of the more familiar function

$$li(x) = \int_2^x \frac{dt}{lnt}$$

in the sense that

$$\frac{\pi(x)}{li(x)} \to 1 \text{ as } x \to \infty.$$

This was later proved by by Hadamard and de la Valleé Poussin in 1896, and is known as the *Prime Number Theorem*. The proof is beyond the scope of these notes. By applying l'Hospital's rule, one can observe that

$$\lim_{x\to\infty} \frac{li(x)}{x/lnx} = 1.$$

The the Prime number theorem can be restated as

$$\frac{\pi(x)}{x/lnx} \to 1 \text{ as } x \to \infty,$$

and interpreted as showing that the proportion $\frac{\pi(x)}{x}$ of primes amongst the positive integers $n \leq x$ is approximately $\frac{1}{\ln x}$ for large x. Since $\frac{1}{\ln x} \to 0$ as $x \to \infty$, the theorem says that the primes occur less and less frequently among larger integers.

1.6.2 Conjectures about Primes

There are many open questions and *conjectures* involving primes. A *conjecture* is a statement for which there is enough evidence but which is not still proved mathematically. Twin prime conjecture is one such famous conjectures involving primes.

DEFINITION 1.30. *If p is a prime number such that $p+2$ is also a prime, the p and $p+2$ are called twin primes.*

The Twin Prime Conjecture: There are infinitely many twin primes. I.e., there are infinitely many pairs of primes such as $(3,5)$, $(5,7)$, $(11,13)$, ...

A more general conjecture is **Polignac's conjecture**, which states that for any integer n there are infinitely many primes p such that $p+2n$ is also a prime. The twin-prime conjecture is a special case of Polignac's conjecture with $n=1$.

Another unanswered question involves the Fibonacci sequence F_n, which defined as $F_0 = 1$, $F_1 = 1$, $F_2 = 1+1 = 2$, $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. The question whether there are infinitely many primes in the Fibonacci sequence is still open.

Bertrand Conjecture: For each natural number $n \geq 2$, there exists a prime number p such that p lis between n and $2n$.

The above conjecture has been verified up to large values by Bertrand, who formulated it in 1845. It was proved by Tchebysheff in 1852. As a consequence of this conjecture, one can show that the n-th prime does not exceed 2^n for $n \geq 2$.

THEOREM 1.31. *If p_n denotes the n-th prime, then $p_n < 2^n$ for $n \geq 2$.*

Proof: We use induction on n. The assertion is clear for $n = 2$. Assume it is true for $n = k \geq 2$. Then, by Bertrand's conjecture there is a prime p such that $2^k < p < 2^{k+1}$. Then, $p_k < p$. Therefore, we have found a prime bigger than the first k primes which is less than 2^{k+1}. $\square$

1.6.3 Goldbach Conjecture

Goldbach Conjecture: Any even number greater than 4 can be expressed as th sum of two odd primes.

For example, $6 = 3+3,\ 8 = 3+5,\ 10 = 3+7 = 5+5$ etc. One can take as large an even number as possible and find two primes of which the given number is a sum. However, a proof has been elusive for more than 240 years, since Goldbach first put this question to Euler, who as one of the leading mathematicians of that era. A similar open question is that *any even number can be written as the difference of two primes*, for example $2 = 5-3,\ 4 = 7-3,\ 6 = 11-5,\ \ldots$ etc.

Note that if Goldbach conjecture is true, then any odd integer $n > 7$ will be a sum of three odd primes: $n-3$ is an even integer bigger than 4, hence $n-3 = p_1+p_2$ for two odd primes p_1 and p_2 by Goldbach conjecture and $n = 3+p_1+p_2$. In a major progress, Hardy and Littlewood showed that under another conjecture (known as the Riemann Hypothesis, which we will allude to towards the final lectures) every sufficiently large odd integer can be expressed as the sum of of three odd primes. It has also been proved that 'almost all' even integers satisfy Goldbach conjecture in the following sense: if $g(x)$ is the number of even integers n not exceeding a real number x, then

$$\lim_{x\to\infty} \frac{g(x)}{x} = 0.$$

However, note that the above result does not rule out the possibility that there still may be infinitely many even integers which are not expressible as sum of two primes. What it says is that such occurrence will be very rare.

1.7 Exercises

1. Show that no integer in the following sequence can be a perfect square:

$$99,\ 999,\ 9999,\ 99999,\ \ldots$$

2. Prove that a cube of an integer must be of the form of $5n$ or $5n \pm 1$.

3. Prove that $7k + 3$ can not be a perfect square for any integer a.

4. Prove that if an integer is simultaneously a square and a cube, then it must be of the form $7n$ or $7n + 1$.

5. Prove that if a and b are integers with $b > 0$, then there exist unique integers q and r satisfying $a = qb + r$, where $5b \leq r < 6b$.

6. Find $gcd(174, 204)$ using Euclid's algorithm.

7. Show that the gcd of $(n + 1)! + 1$ and $n! + 1$ is 1.

8. (A) Let a, b and c be three integers such that $abc \neq 0$ and $a \mid bc$. Show that

$$a \mid gcd(a, b)gcd(a, c).$$

   (B) Now let $a \mid b_1 b_2 \cdots b_n$ where $ab_1 \cdots b_n \neq 0$. Show that

$$a \mid gcd(a, b_1) \cdots gcd(a, b_n).$$

9. Show that $5n + 3$ and $7n + 4$ are relatively prime for any natural number n.

10. If a and b are coprime integers, show that $a + b$ and $a^2 + ab + b^2$ are also coprime.

11. If a and b are coprime integers and $3 \mid a$, show that $a + b$ and $a^2 - ab + b^2$ are also coprime.

12. Find $gcd(2002 + 2,\ 2002^2 + 2,\ 2002^3 + 2,\ \ldots)$.

13. Let $a > 1$ be an integer, and m and n $(M > n)$ are any two distinct positive integers.

   (A) Hence show that $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

   (B) Show that $gcd(a^n + 1, a^m + 1)$ divides $a^{gcd(m,n)} + 1$.

14. Find all the solutions of $174x + 204y = 18$.

15. Show that for any integer n, the rational number $\frac{55n+7}{33n+4}$ is irreducible (i.e., the numerator and the denominator are co-prime).

16. Show that $101x + 257y = n$ has solutions in integers for any integer n.

17. If $d = gcd(a, b)$, then what is the gcd of a^n and b^n? What will be the gcd of a^m and b^n?

18. If p is a prime and k is an integer such that $1 \leq k < p$, then show that
$$p \mid \binom{p}{k}.$$

19. A *Pythagorean triple* consists of three positive integers $a,\ b,\ c$ such that $a^2 + b^2 = c^2$. Such a triple is called *primitive* if $gcd(a, b, c) = 1$. Show that any primitive Pythagorean triple can be expressed as $m^2 - n^2,\ 2mn,\ m^2 + n^2$ where m and n are two coprime integers. (For example, for $(3, 4, 5)$ $[3^2 + 4^2 = 5^2]$, we can take $m = 2$ and $n = 1$.)

20. Show that there are infinitely many positive integers A such that $2A$ is a square, $3A$ is a cube and $5A$ is a fifth power.

21. If a, b, c are three natural numbers with $gcd(a, b, c) = 1$ such that
$$\frac{1}{a} + \frac{1}{b} = \frac{1}{c},$$
then show that $a + b$ is a perfect square.

22. Show that there are no positive integers a b and c satisfying
$$a^2 + b^2 + c^2 = a^2b^2.$$

23. Show that
$$1! + 2! + 3! + \ldots + n!$$
is a perfect power if and only if $n = 3$.

24. Show that
$$(1!)^3 + (2!)^3 + (3!)^3 + \ldots + (n!)^3$$
is a perfect square if and only if $n = 3$.

25. Show that
$$(1!)^3 + (2!)^3 + (3!)^3 + \ldots + (n!)^3$$
is a perfect power if and only if $n \leq 3$.

26. Can there be three consecutive odd numbers be primes? How many such triples exist?

27. Show that there are infinitely many primes of the form $6k + 5$.

28. Prove that $\sqrt{p}$ is irrational for any prime number p.

29. Find all prime numbers p such that $p^2 + 2$ is also a prime.

30. Let p_n denoted the n-th prime number. Show that $p_1 p_2 . \cdots . p_n + 1$ is never a square.

31. Let R_n be an integer consisting only of n number of 1's in its decimal expansion. If R_n is prime, show that n must be prime.

32. Show that there are infinitely many primes which do not belong to any pair of twin primes. (You may assume Dirichlet's theorem that there are infinitely many primes in any arithmetic progression with relatively prime first term and common difference.)

33. Show that the sum of any pair of twin primes except $(3, 5)$ is divisible by 12.

Module 2

Congruence

2.1 Lecture 1

Preamble: In this lecture we will introduce the notion of congruence. We will show that for any integer n, congruence modulo n defines an equivalence relation on the set of integers. We will define the complete system of residues and the reduced system of residues. We will deduce divisibility criterion for 9 and 11 as a simple application of the notion of congruence.

Keywords: Congruence, equivalence relation, residues, reduced residues

2.1.1 Congruence

Definition 2.1. *Consider the set $\mathbb{Z}$ of integers and let n be any non-zero integer. Define a relation*

$$\equiv \ mod\ n$$

on $\mathbb{Z}$ by

$$a \equiv b \ mod\ n \text{ if and only if } n \mid (a-b).$$

For example,

$$12 \equiv 3 \bmod 9, \qquad 31 \equiv 6 \bmod 5.$$

Proposition 2.2. *The relation $\equiv$ modulo n' is an equivalence relation.*

Proof: We have to show that the relation is

1. reflexive (i.e., every element is related to itself),
2. symmetric (i.e., if a is related to b then b is related to a), and
3. transitive (i.e., if a is related to b, and b is related to c, then a is related to c).

Now,

- $a \equiv a$ modulo n $\forall a \in \mathbb{Z}$ as $n \mid (a-a)$.
- $a \equiv b$ modulo n implies $b \equiv a$ modulo n as

$$n \mid (a-b) \implies n \mid (b-a) \ \ \forall a, b \in \mathbb{Z}.$$

- $a \equiv b$ modulo n and $b \equiv c$ modulo n imply $a \equiv c$ modulo n, as

$$n \mid (a-b), \qquad n \mid (b-c) \implies n \mid \big[(a-b)+(b-c)\big] \qquad \forall a, b, c \in \mathbb{Z}. \qquad \square$$

DEFINITION 2.3. *The equivalence class of an integer a a is be denoted by $[a]$, is referred to as the congruence class or residues class of a. Thus,*

$$[a] = \{b \in \mathbb{Z} \mid b \equiv a \ mod \ n.$$

The set of all equivalence classes modulo n is called a complete residue system. The set of all equivalence classes modulo n, i.e., the complete residue system of n is denoted by $\mathbb{Z}_n$.

It is enough to consider n to be a positive integer, as

$$n \mid (a-b) \Leftrightarrow (-n) \mid (a-b).$$

From now, we will consider n to be a positive integer.

PROPOSITION 2.4. *$a \equiv b \ mod \ n$ if and only if they leave the same remainder upon division by n.*

Proof: By division algorithm, we can write

$$\begin{aligned} a &= nq + r, \qquad 0 \le r \le n-1, \\ b &= nl + r, \qquad 0 \le s \le n-1, \\ \implies (a-b) &= n(p-l) + (r-s). \end{aligned}$$

If $r = s$, it is clear from the last line that n divides $a - b$. Conversely, if $a \equiv b \bmod n$, that the last step above tells us that $n \mid (r - s)$. But

$$\begin{aligned} & 0 \leq r \leq n-1, \qquad 0 \leq s \leq n-1 \\ \implies \quad & -(n-1) \leq (r-s) \leq (n-1). \end{aligned}$$

Hence $n \mid (r - s)$ implies $r - s = 0$. $\square$

The following corollary is obvious form the proposition.

COROLLARY 2.5. *If r is the remainder of a upon division by n, then they are in the same congruence class modulo n, i.e., $[a] = [r]$.*

COROLLARY 2.6. *For any integer n, there are n distinct congruence classes.*

Proof: The only possible remainders upon division by n are $0,\ 1,\ \cdots,\ n-1$. So any integer a must be congruent to one of these n remainders. So the number of congruence classes is not more than n. Any two distinct remainders in the above list can not be equivalent by the proposition. Hence the corollary follows. $\square$.

DEFINITION 2.7. *A set of congruence classes is called a complete residue system if any given integer belongs to one of the congruence classes in the set.*

Thus, the set $\{[0],\ [1],\ \cdots,\ [n-1]\}$ is an example of a complete residue system for n.

2.1.2 Properties of Congruence

Congruence modulo n has many interesting properties which simplify a lot of computations. Some of these properties are listed below.

1. $x \equiv y \bmod n \implies x + c \equiv y + c \bmod n \ \ \forall c \in \mathbb{Z}$.
2. $x \equiv y \bmod n,\ \ z \equiv w \bmod n \implies xz \equiv yw \bmod n \ \ \forall c \in \mathbb{Z}$.
3. $x \equiv y \bmod n \implies cx \equiv cy \bmod n \ \ \forall c \in \mathbb{Z}$.
4. $x \equiv y \bmod n \implies x^k \equiv y^k \bmod n \ \ \forall k \in \mathbb{N}$.
5. $x \equiv y \bmod n \implies f(x) \equiv f(y) \bmod n$ for $f \in \mathbb{Z}[x]$.
6. $x \equiv y \bmod n \implies x \equiv y \bmod d$ for any divisor d of m.

7. $ax \equiv ay \bmod n \implies x \equiv y \bmod \frac{m}{gcd(a,m)}$.
8. $ax \equiv ay \bmod n \implies x \equiv y \bmod n$ if $gcd(a, m) = 1$.
9. $x \equiv y \bmod m_i \implies x \equiv y \bmod lcm(m_i)$ for positive integers $m_1. \cdots, m_r$.

The first of the above properties follow easily from definition of congruence. Observe that $a \equiv b \bmod n$ implies that we can write as $a = b + nk$ for some integer k. For the second property above,

$$x = y + nk,\ z = w + nl \implies xz = yw + n(yl + kz + nkl) \equiv yw \bmod n.$$

The third property follows from the second by taking $z = w = c$. The fourth property follows from the second by taking $z = x$, $w = y$ to start with, then $z = x^2$, $w = y^2$ etc. Then the fifth is a consequence of the preceding properties. The sixth property is clear too, as

$$d \mid n,\ \ n \mid (a - b) \implies d \mid (a - b).$$

For the seventh property, we cancel the gcd d of $n = d_{n_1}$ and $a = da_1$ to obtain

$$\begin{aligned} & n \mid a(x - y) \\ \implies\ & n_1 \mid a_1 a(x - y) \\ \implies\ & n_1 \mid (x - y) \end{aligned}$$

as $gcd(a_1, x - y) = 1$. The next property is special case of the seventh. The last property follows from the definition of the lcm. □

Proposition 2.8. *Let d be the gcd of a and n. Then*

$$ax \equiv ay\ mod\ n \implies x \equiv y\ mod\ \frac{n}{d}.$$

In particular, if a and n are coprime, then

$$ax \equiv ay\ mod\ n \implies x \equiv y\ mod\ n.$$

Proof:

$$ax \equiv ay \bmod n \implies n \mid a(x - y).$$

By canceling the gcd, we have

$$\frac{n}{d} \mid (x - y) \implies x \equiv y \bmod \frac{a}{d}. \qquad \square$$

2.1.3 Divisibility Criterion for 9 and 11

We will now demonstrate the usefulness of the notion of congruence with some simple applications. We will derive divisibility criterion for integers like 9, 11 etc using congruence.

PROPOSITION 2.9. *A positive integer is divisible by* 9 *(by* 3*) if and only if the sum of its digits in its decimal expansion is divisible by* 9 *(by* 3*).*

Proof: Let m be an integer whose decimal expansion is

$$m = b_k.10^k + b_{k-1}.10^{k-1} + \cdots + b_1.10 + b_0, \qquad 0 \leq b_i < 10.$$

and let

$$S = b_k + b_{k-1} + \cdots + b_1 + b_0.$$

Now,

$$\begin{aligned} 10 &\equiv 1 \bmod 9 \\ \implies 10^k &\equiv 1 \bmod 9 \\ \implies b_k.10^k + b_{k-1}.10^{k-1} + \cdots + b_1.10 + b_0 &\equiv b_k + b_{k-1} + \cdots + b_1 + b_0 \bmod 9 \\ \implies m &\equiv S \bmod 9. \end{aligned}$$

Thus $9 \mid m$ if and only if $9 \mid S$. The proof for divisibility by 3 is identical. □

PROPOSITION 2.10. *A positive integer is divisible by* 11 *if and only if the sum of its digits with alternate signs in its decimal expansion is divisible by* 11*.*

Proof: Let m be an integer whose decimal expansion is

$$m = b_k.10^k + b_{k-1}.10^{k-1} + \cdots + b_1.10 + b_0, \qquad 0 \leq b_i < 10.$$

and let

$$A = (-1)^k b_k + (-1)^{k-1} b_{k-1} + \cdots - b_1 + b_0. \text{ Now,}$$

$$\begin{aligned} 10 &\equiv -1 \bmod 11 \\ \implies 10^k &\equiv (-1)^k \bmod 11 \\ \implies b_k.10^k + b_{k-1}.10^{k-1} + \cdots + b_1.10 + b_0 &\equiv (-1)^k b_k + (-1)^{k-1} b_{k-1} + \cdots - b_1 + b_0 \bmod 11 \\ \implies m &\equiv A \bmod 11. \end{aligned}$$

Thus $11 \mid m$ if and only if $11 \mid A$. □

We leave it as an exercise now to prove the divisibility criterion for 4 and 8.

2.2 Lecture 2

Preamble: In this lecture, we will show how to find solutions of linear congruence. We will derive a necessary and sufficient condition for existence of solutions of a equation of the form $ax \equiv b \bmod n$. We will also discuss uniqueness of solutions.

Keywords: linear congruence

2.2.1 Linear Congruence

Let n be a positive integer. Consider the following linear congruence

$$ax \equiv b \bmod n,$$

where a is an integer which is not divisible by n. We want to find all integers x which satisfy the above congruence. It is clear that solutions will be congruence classes modulo n. In other words, if r is a solution, so is any $s \in [r]$. Hence we would not distinguish between two solutions which are congruent modulo n. We would also like to know when we have a unique congruence class as solution. If we look at a few examples, we find that it is possible to have linear congruence which has no solutions, only one solution or more than one solutions. For example, the linear congruence

$$2x \equiv 5 \bmod 6$$

has no solution: if r is a solution, then 6 must divide $2r - 5$, which implies in particular that $2r - 5$ must be even. But that is not possible as $2r$ is even but 5 is odd. Now consider

$$2x \equiv 1 \bmod 3.$$

If we look at three congruence classes modulo 3, we find that [0] and [1] are not solutions, but [2] is a solution. Therefore, this congruence has a unique equivalence class of solutions. Now consider the congruence

$$4x \equiv 2 \bmod 6.$$

We can check the 6 elements of a complete residue system of 6, and observe that both [2] and [5] are solutions.

We will first find a necessary and sufficient condition for existence of solutions of a linear congruence. Then we will investigate the number of inequivalent solutions.

THEOREM 2.11. *The congruence*

$$ax \equiv b \ mod \ n$$

has a solution if and only if the gcd of a and n divides b.

Proof: Let d be the gcd of a and n. First assume that the above congruence has a solution r. Then,

$$\begin{aligned} & ar && \equiv && b \bmod n \\ \implies & n && \mid && (b - ar) \\ \implies & d && \mid && (b - ar), \quad d \mid a \\ \implies & d && \mid && (b - ar + ar) \\ \implies & d && \mid && b. \end{aligned}$$

Conversely, suppose d divides b. We will now exhibit a solution for the above congruence. We can write $b = db_1$ for some integer b_1. By Euclid's algorithm, we can find integers r_1 and s_1 such that

$$\begin{aligned} ar_1 + ns_1 &= d \\ \implies b_1(ar_1 + ns_1) &= db_1 \\ \implies a(b_1 r_1) + n(b_1 s_1) &= b \\ \implies a(b_1 r_1) &\equiv b \bmod n. \end{aligned}$$ □

The examples that we saw above are consistent with the theorem. The congruence $2x \equiv 5 \bmod 6$ had no solution as the gcd 2 of 2 and 6 does not divide 5. But $2x \equiv 1 \bmod 3$ has a solution as the gcd of 2 and 3 divides 1. In the third example too, the gcd of 4 and 6 divides 2, and we could find solutions.

THEOREM 2.12. *Consider the congruence*

$$ax \equiv b \ mod \ n,$$

where the gcd d of a and n divides b. Let x_0 be a solution. Then all the other solutions are precisely given by the following set:

$$x_0, \ \ x_0 + \frac{n}{d}, \ \ x_0 + \frac{2n}{d}, \ \ \cdots, \ \ x_0 + \frac{(d-1)n}{d}.$$

Proof: First we verify that for all i with $0 \leq i \leq (d-1)$, $x_0 + \frac{in}{d}$ is a solution of the given congruence:

$$\begin{aligned} a(x_0 + \frac{in}{d}) &= ax_0 + in\frac{a}{d} \\ &= ax_0 + ina_1 \qquad (d \mid a \implies a = da_1) \\ &\equiv ax_0 \bmod n \\ &\equiv b \bmod n. \end{aligned}$$

Next, we show that any two distinct elements in the above set are inequivalent modulo n. As d divides n, we can write $n = dk$ for some integer k. Consider i, j such that $0 \leq i, j \leq (d-1)$. Then ,

$$\begin{aligned} x_0 + \frac{in}{d} &\equiv x_0 + \frac{jn}{d} \bmod n \\ \implies \frac{in}{d} &\equiv \frac{jn}{d} \bmod n \\ \implies ik &\equiv jk \bmod dk \qquad (n = dk) \\ \implies dk &\mid k(i-j) \\ \implies d &\mid (i-j). \end{aligned}$$

But $-(d-1) \leq (i-j) \leq (d-1)$, hence $d \mid (i-j)$ implies $i = j$. Thus, two distinct elements in the above set can not be congruent modulo n.

Finally, we will have to show that any solution x_1 must be congruent to one of the d elements in the set modulo n. We have

$$\begin{aligned} & ax_1 \equiv b \equiv ax_0 \bmod n \\ \implies \quad & n \mid a(x_1 - x_0) \\ \implies \quad & k \mid (x_1 - x_0) \\ \implies \quad & x_1 = x_0 + ik \qquad \text{for some integer } i \\ \implies \quad & x_1 = x_0 + i\frac{n}{d}. \end{aligned}$$

It is enough to consider the above integer i in the range $\{0,\ 1,\ ,(d-1)\}$, as

$$i \equiv i' \bmod d \implies x_0 + \frac{in}{d} \equiv x_0 + \frac{i'n}{d} \bmod n. \ \square$$

COROLLARY 2.13. *The congruence*

$$ax \equiv b \ mod \ n$$

has a unique solution if and only if a and n are coprime.

In the examples that we have discussed in this lecture, we saw that $2x \equiv 1 \bmod 3$ has a unique solution [2], as 2 and 3 are coprime. On the other hand, $4x \equiv 2 \bmod 6$ has more than one solution, as 4 and 6 are not coprime.

2.3 Lecture 3

Preamble:In this lecture, we will discuss more than one linear congruences. Under certain conditions, we will show that that such simultaneous congruences have a solution. We will also discuss the uniqueness of such a solution. For solving such congruences, there is a well-known method known as the Chinese Remainder Theorem.

Keywords: Simultaneous congruences, Chinese Remainder Theorem

2.3.1 Simultaneous Linear Congruences

Consider the congruences

$$x \equiv 3 \bmod 10, \qquad x \equiv 2 \bmod 8.$$

Clearly, there is no common solution to both. The first one indicates that a solution x_0 must be an odd integer, as $x_0 - 3$ is divisible by 2, whereas the second one can have only even integers as solutions. On the other hand, the congruences

$$x \equiv 3 \bmod 10, \qquad x \equiv 2 \bmod 7.$$

We can verify that 23 is a common solution, and so is 93. We will now determine a sufficient condition for such congruences to have have common solutions. We will also see when such solutions are unique. Note that in the second set of congruences, the moduli 10 and 7 are coprime. We will first show that when we have coprime moduli the simultaneous congruences will always have a solution.

2.3.2 Chinese Remainder Theorem

The following theorem is known as the Chinese Remainder Theorem. It gives us a sufficient condition for existence of solutions to simultaneous linear congruences.

THEOREM 2.14. *Consider the linear congruences*

$$\begin{aligned} x &\equiv a_1 \ mod \ m_1, \\ x &\equiv a_2 \ mod \ m_2, \\ &\vdots \qquad \vdots \\ x &\equiv a_n \ mod \ m_n. \end{aligned}$$

If the m_i are pairwise coprime, then these congruences have a common solution x_0. Further, such a common solution is unique modulo $M = m_1.\cdots.m_n$.

Proof: Let us define n integers

$$M_i = \frac{M}{m_i} = m_1.\cdots.m_{i-1}.m_{i+1}.\cdots.m_n, \qquad 1 \leq i \leq n.$$

As m_i's are pairwise coprime, each M_i is coprime to the corresponding m_i. For each i $(1 \leq i \leq n)$, consider the linear congruence

$$M_i x \equiv 1 \bmod m_i.$$

As M_i and m_i are coprime, the above congruence has a solution. So there is an integer $\tilde{m}_i$ such that

$$M_i \tilde{m}_i \equiv 1 \bmod m_i.$$

We claim that

$$x_0 = a_1 M_1 \tilde{m}_1 + \cdots + a_i M_i \tilde{m}_i + \cdots + a_n M_n \tilde{m}_n$$

satisfies all the given congruences in the theorem. Observe that

$$\begin{aligned} x_0 &= a_1 M_1 \tilde{m}_1 + \cdots + a_i M_i \tilde{m}_i + \cdots + a_n M_n \tilde{m}_n \\ &\equiv a_i M_i \tilde{m}_i \bmod m_i \\ &\equiv a_i \bmod m_i. \end{aligned}$$

As for the uniqueness of common solutions, let x_1 be another common solution to the above system of linear congruences. Then, for each i, we have

$$x_1 \equiv a_i \equiv x_0 \bmod m_i \implies m_i | (x_1 - x_0).$$

As the m_i's are coprime, we have

$$(m_1.\cdots.m_n) | (x_1 - x_0) \implies x_1 \equiv x_0 \bmod M. \qquad \square$$

Let us illustrate the method with the following example.

Exercise: Solve the following system of linear congruences

$$x \equiv 2 \bmod 6, \quad x \equiv 1 \bmod 5, \quad x \equiv 3 \bmod 7.$$

Solution: Observe that the moduli are pairwise coprime. Here,

$$M = 6.5.7 = 210, \qquad M_1 = 5.7 = 35, \qquad M_2 = 6.7 = 42, \qquad M_3 = 6.5 = 30.$$

Now,

$$\begin{aligned} 35\tilde{m}_1 \equiv 1 \bmod 6 &\implies -\tilde{m}_1 \equiv 1 \bmod 6 \implies \tilde{m}_1 \equiv 5 \bmod 6 \\ 42\tilde{m}_2 \equiv 1 \bmod 5 &\implies 2\tilde{m}_2 \equiv 1 \bmod 5 \implies \tilde{m}_2 \equiv 3 \bmod 5 \\ 30\tilde{m}_3 \equiv 1 \bmod 7 &\implies 2\tilde{m}_3 \equiv 1 \bmod 7 \implies \tilde{m}_3 \equiv -3 \bmod 7 \end{aligned}$$

Hence, by Chinese Remainder Theorem, we have a solution

$$x_0 = 2.35.5 + 1.42.3 + 3.30.(-3) = 350 + 126 - 270 = 206.$$

The solution is unique modulo $M = 6.5.7 = 210$. □

It may appear that the Chinese Remainder Theorem does not cover a general system of linear congruences with coprime moduli, as we have not really taken congruences of the type

$$b_i x \equiv a_i \bmod m_i, \quad 1 \leq i \leq n, \quad gcd(m_i, m_j) = 1 \text{ when } i \neq j.$$

But we can reduce a congruence of this form to a form considered in the above theorem, provided $gcd(b_i, m_i) = 1$. This condition is necessary as well as sufficient: we know that $b_i c_i \equiv 1 \bmod m_i$ has a solution if and only if $gcd(b_i, m_i) = 1$. Then,

$$b_i x \equiv a_i \bmod m_i \Leftrightarrow x \equiv c_i a_i \bmod m_i,$$

and we obtain a linear congruence which is in the desired form so that the Chinese Remainder Theorem can be applied. Let us demonstrate this with an example:

Exercise: Solve the system of linear congruences

$$5x \equiv 1 \bmod 6, \quad 3x \equiv 2 \bmod 5, \quad 4x \equiv 5 \bmod 7.$$

Solution: Observe that each of the above congruences is solvable, for example, in the first one, 5 is coprime to 6. We have $5.5 \equiv 1 \bmod 6$, so we can multiply the first congruence by 5 to obtain $x \equiv 5 \bmod 6$. Similarly, we multiply the second congruence by 2 (as $3.2 \equiv 1 \bmod 5$) to obtain $x \equiv 4 \bmod 5$. We multiply the the congruence above by 2 to obtain $x \equiv 10 \equiv 3 \bmod 7$. Thus, the given system is reduced to

$$x \equiv 5 \bmod 6, \quad x \equiv 4 \bmod 5, \quad x \equiv 3 \bmod 7.$$

Proceeding as in the previous example, we have

$$M = 6.5.7 = 210, \qquad M_1 = 5.7 = 35, \qquad M_2 = 6.7 = 42, \qquad M_3 = 6.5 = 30.$$

and

$$\begin{aligned} 35\tilde{m}_1 \equiv 1 \bmod 6 \quad &\Longrightarrow \quad \tilde{m}_1 \equiv 5 \bmod 6 \\ 42\tilde{m}_2 \equiv 1 \bmod 5 \quad &\Longrightarrow \quad \tilde{m}_2 \equiv 3 \bmod 5 \\ 30\tilde{m}_3 \equiv 1 \bmod 6 \quad &\Longrightarrow \quad \tilde{m}_3 \equiv -3 \bmod 7 \end{aligned}$$

Hence, by Chinese Remainder Theorem, we have a solution

$$x_0 = 5.35.5 + 4.42.3 + 3.30.(-3) = 875 + 504 - 270 = 1109 \equiv 59 \bmod 210.$$

The solution is unique modulo 210. □

2.4 Lecture 4

Preamble: In this lecture, we will discuss a generalization of the Chinese Remainder Theorem. We will show how to solve a system of linear congruences even when the moduli are not pairwise coprime.

Keywords: Non-coprime moduli

2.4.1 System of Congruences with Non-coprime Moduli

We have seen that the system of linear congruences congruences

$$x \equiv 3 \bmod 10, \qquad x \equiv 2 \bmod 8$$

has no common solution. The first congruence can have only odd integers as solutions, whereas the second one has only even integers as solutions. On the other hand, consider the system of linear congruences

$$x \equiv 3 \bmod 10, \qquad x \equiv 1 \bmod 8.$$

We can verify that 33 is a common solution, and so is 73. We will now see under which conditions such congruences are guaranteed to have a common solution. We will also discuss whether such a solution is unique. Note that in the second set of congruences, the gcd of the two moduli divides $3 - 1$. We will first show that such a system of congruences will always have a solution if we have such a condition for each pair of moduli.

THEOREM 2.15. *Consider the linear congruences*

$$\begin{aligned} x &\equiv a_1 \ mod\ m_1, \\ x &\equiv a_2 \ mod\ m_2, \\ &\vdots \qquad \vdots \\ x &\equiv a_n \ mod\ m_n, \end{aligned}$$

where the moduli m_i's are not necessarily pairwise coprime. Let $d_{i,j} = gcd(m_i, m_j)$ for $i \neq j$. Then the above system has a simultaneous solution if and only if $d_{i,j}$ divides $(a_i - a_j)$ for all $i \neq j$. Further, such a solution is unique modulo the lcm of $m_1, \cdots, m_n$.

Proof: If a simultaneous solution exists, it is easy to show that $d_{i,j}$ divides $(a_i - a_j)$. Let x_0 be a common solution. Then for each pair $i \neq j$,

$$\begin{aligned} x_0 \equiv a_i \bmod m_i \quad &\Longrightarrow \quad m_i|(x_0 - a_i) \quad \Longrightarrow \quad d_{i,j}|(x_0 - a_i) \\ x_0 \equiv a_j \bmod m_j \quad &\Longrightarrow \quad m_j|(x_0 - a_j) \quad \Longrightarrow \quad d_{i,j}|(x_0 - a_j) \\ \Longrightarrow \quad d_{i,j}|[(x_0 - a_j) - (x_0 - a_i)] \quad &\Longrightarrow \quad d_{i,j}|(a_i - a_j). \end{aligned}$$

For the converse, we will show that the above system can be reduced to a system of linear congruences with coprime moduli, which definitely has a solution. First observe that if

$$m = p_1^{e_1}.p_2^{e_2}.\cdots.p_r^{e_r},$$

where p_k's are distinct primes, then $x \equiv a \bmod m$ if and only if $x \equiv a \bmod p_k^{e_k}$ for each p_k in the factorization of m. Now, suppose $d_{i,j}|(a_i - a_j)$ for all $i,\ j$. Let p be a prime factor of the lcm l of the moduli m_i's, and e be the highest p dividing l. Then p^e must divide one of the moduli, say it divides m_i. Let p^{e_j} be the highest power of p dividing m_j. Thus, in our notation $e = e_i$, and $e_j \leq e = e_i$. Now

$$x \equiv a_i \bmod p^{e_i} \implies x \equiv a_i \bmod p^{e_j}.$$

But $p^{e_j}|d_{i,j}$, and $d_{i,j}|(a_i - a_j)$, hence $a_i \equiv a_j \bmod p^{e_j}$, and

$$x \equiv a_i \bmod p^{e_i} \implies x \equiv a_i \bmod p^{e_j} \implies x \equiv a_j \bmod p^{e_j} \quad \forall j.$$

Thus, the given system will have a solution provided the system of linear congruences

$$x \equiv a_i \bmod p^{e_i},$$

for each prime p dividing the lcm l (where e_i is the highest power of p dividing l, occurring in the modulus m_i) has a solution. By he Chinese Remainder Theorem, the latter system has a solution.

Now we examine whether a common solution is unique. If x_0 and x_1 are two solutions of the given system, we will have

$$\begin{aligned} & x_1 \equiv a_i \equiv x_0 \bmod m_i \ \ \forall i \\ \Longrightarrow \quad & m_i|(x_1 - x_0) \ \ \forall i \\ \Longrightarrow \quad & lcm(m_1.\cdots.m_n)|(x_1 - x_0) \\ \Longrightarrow \quad & x_1 \equiv x_0 \bmod l. \end{aligned}$$

Therefore the solutions is unique modulo the lcm of the moduli. □

Let us illustrate the theorem with the following example.

Exercise: Solve the system of linear congruences

$$x \equiv 2 \bmod 12, \quad x \equiv 6 \bmod 10, \quad x \equiv 11 \bmod 45.$$

Solution: Observe that

$$gcd(12,10)|(6-2), \quad gcd(10,45)|(11-6), \quad gcd(12,45)|(11-2).$$

By the above theorem, the given system will have a solution. Here, the lcm l of 6, 10, 45 is $180 = 2^2.3^2.5$. Hence, the given system reduces to

$$x \equiv 2 \bmod 2^2, \quad x \equiv 6 \bmod 5, \quad x \equiv 11 \bmod 3^2.$$

For the above system with prime-power moduli which are pairwise coprime, we can apply Chinese Remainder Theorem with

$$M = 2^2.3^2.5 = 180 = l, \qquad M_1 = 5.9, \qquad M_2 = 4.9, \qquad M_3 = 4.5.$$

Now,

$$\begin{aligned} 5.9.\tilde{m}_1 \equiv 1 \bmod 4 \quad &\Longrightarrow \quad \tilde{m}_1 \equiv 1 \bmod 4 \\ 4.9.\tilde{m}_2 \equiv 1 \bmod 5 \quad &\Longrightarrow \quad \tilde{m}_2 \equiv 1 \bmod 5 \\ 4.5.\tilde{m}_3 \equiv 1 \bmod 9 \quad &\Longrightarrow \quad 2\tilde{m}_3 \equiv 1 \bmod 9 \Longrightarrow \quad \tilde{m}_3 \equiv -4 \bmod 9 \end{aligned}$$

Hence, by Chinese Remainder Theorem, we have a solution

$$x_0 = 2.(5.9).1 + 6.(4.9).1 + 11.(4.5).(-4) = -574 \equiv 146 \bmod 180.$$

The solution is unique modulo 180. □

2.5 Lecture 5

Preamble: In this lecture we will show how to find solution of congruences modulo powers of a prime. First, we will demonstrate the method for linear congruence, showing how we can lift a solution modulo a prime p to a solution modulo p^e. Then we will look at a non-linear congruence, and illustrate that while we can lift some of the solution modulo p to higher powers, we may not be able to do so for certain other solutions modulo p. p,. Finally, we will discuss Hensel's lemma which says precisely when a solution modulo a prime can be lifted to a solution modulo higher powers of the same prime

Keywords: linear congruence modulo prime powers, Hensel's lemma

2.5.1 Linear Congruences Modulo Prime Powers

We have seen before that it is easy to find solution x_1 of the linear congruences

$$ax \equiv b \bmod p$$

for any prime p. Now we will illustrate that we can find a solution x_2 of

$$ax \equiv b \bmod p^2$$

such that $x_2 \equiv x_1 \bmod p$. We refer to x_2 as a lift of the solution of x_1. Similarly, we can find a solution x_3 of

$$ax \equiv b \bmod p^3$$

such that it is a lift of x_2 (and of x_1 as well), i.e.,

$$x_3 \equiv x_2 \bmod p^2.$$

Note that any solution modulo higher powers must be a lift of a solution of the lower powers, as

$$az \equiv b \bmod p^{e+1} \implies az \equiv b \bmod p^e.$$

Let us take $= 7$ and consider the linear congruence

$$3x \equiv 5 \bmod 7^3.$$

Observing that 5 is the inverse of 3 modulo 7, we obtain a unique solution $x_1 = 4$ for the congruence

$$3x - 5 \equiv 0 \bmod 7.$$

We will first lift x_1 to a solution x_2 of

$$3x - 5 \equiv 0 \bmod 7^2,$$

and then lift x_2 to a solution x_3 of the given congruence. Let $x_2 = x_1 + 7a_1 = 4 + 7a_1$. Then

$$\begin{aligned} 3(4 + 7a_1) - 5 &\equiv 0 \bmod 7^2 \\ \Leftrightarrow 7 + 3.7.a_1 &\equiv 0 \bmod 7^2 \\ \Leftrightarrow 1 + 3.a_1 &\equiv 0 \bmod 7 \\ \Leftrightarrow a_1 &\equiv 2 \bmod 7^2 \end{aligned}$$

Thus, $x_2 = 4+7.2 = 18$ is a solution of the congruence modulo 7^2. Now, let $x_3 = x_2+7^2a_2$ be a solution of the given congruence (modulo 7^3). Then,

$$\begin{aligned} 3(18 + 7^2a_2) - 5 &\equiv 0 \bmod 7^3 \\ \Leftrightarrow 49 + 3.7^2.a_2 &\equiv 0 \bmod 7^3 \\ \Leftrightarrow 1 + 3.a_2 &\equiv 0 \bmod 7 \\ \Leftrightarrow a_2 &\equiv 2 \bmod 7^2 \end{aligned}$$

Thus, we obtain a solution $x_3 = 18 + 49.2 = 116$ which is a solution of the given congruence, and it is a lift of the solution $x_1 = 4$ for the congruence modulo 7.

2.5.2 Non-linear Congruences Modulo Prime Powers

Now we will do the above illustration for a non-linear congruence. We will take a non-linear polynomial $f(x)$ with integral coefficients and then show that we can lift one of its solution modulo p to a solution modulo p^e, whereas we can not do so for another solution modulo p.

Let us consider the cubic polynomial

$$f(x) = x^3 + 3x^2 - 2x + 5.$$

Let $p = 7$ and consider the linear congruence

$$f(x) \equiv 0 \bmod 7^3.$$

One can directly check that 1 and 2 are the only roots of $f(x)$ modulo 7. let us first take $x_1 = 2$and try to lift it to a solution $x_2 = 2 + 7.a_1$ of

$$f(x) \equiv 0 \bmod 7^2.$$

Substituting, we find that

$$\begin{aligned} (2+7a_1)^3 + 3(2+7a_1)^2 - 2(2+7a_1) + 5 &\equiv 0 \bmod 7^2 \\ \Leftrightarrow 2^3 + 3.2^2 - 2.2 + 5 + 7.(3.2^2 + 6.2 - 2)a_1 &\equiv 0 \bmod 7^2 \\ \Leftrightarrow 3 + a_1 &\equiv 0 \bmod 7 \\ \Leftrightarrow a_1 &\equiv 4 \bmod 7^2 \end{aligned}$$

Thus, $x_2 = 2 + 7.4 = 30$ is a solution of the congruence modulo 7^2, as we can check that $f(30) = 49.605$. Now, let $x_3 = x_2 + 7^2 a_2$ be a solution of the given congruence (modulo 7^3). Then,

$$\begin{aligned} (30 + 7^2 a2)^3 + 3(30 + 7^2 a_2)^2 - 2(2 + 7^2 a_2) + 5 &\equiv 0 \bmod 7^3 \\ \Leftrightarrow 49.605 + 7^2(3.30^2 + 6.30 - 2)a_2 &\equiv 0 \bmod 7^3 \\ \Leftrightarrow 3 + .a_2 &\equiv 0 \bmod 7 \\ \Leftrightarrow a_2 &\equiv 4 \bmod 7^2 \end{aligned}$$

Thus, we obtain a solution $x_2 = 30 + 49.4 = 226$ which is a solution of $f(x) \equiv 0 \bmod 7^3$, and it is a lift of the solution $x_1 = 2$ for the congruence modulo 7.

Now let us try to lift the other solution $x - 1 = 1$ of $f(x)$ modulo 7. If we put $x_2 = 1 + 7a_1$, then

$$\begin{aligned} (1+7a_1)^3 + 3(1+7a_1)^2 - 2(1+7a_1) + 5 &\equiv 0 \bmod 7^2 \\ \Leftrightarrow 1^3 + 3.1^2 - 2.1 + 5 + 7.(3.1^2 + 6.1 - 2)a_1 &\equiv 0 \bmod 7^2 \\ \Leftrightarrow 1 + 7a_1 &\equiv 0 \bmod 7 \end{aligned}$$

But there does not exists any a_1 satisfying the above congruence, hence the solution 1 ca not be lifted to a solution of $f(x) \equiv 0 \bmod 7^2$.

2.5.3 Hensel's Lemma

In the previous two sections, we looked at the possibility of lifting solutions of a polynomial. We now identify the properties of an initial solution which allows it to be lifted

to the next level. Consider a polynomial

$$f(x) = x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0, \qquad c_i \in \mathbb{Z}$$

Let p be a prime. Let x_1 be a solution of $f(x)$ modulo p. Then we can write

$$f(x_1) = pb_1, b_1 \in \mathbb{Z}$$

We are interested in lifting x_1 to a solution of $f(x)$ modulo p^2, and higher powers. Substituting $x_2 = x_1 + pa_1$ in $f(x) \equiv 0 \bmod p^2$, we find

$$\begin{aligned} f(x_1 + pa_1) &\equiv 0 \bmod p^2 \\ \Leftrightarrow f(x_1) + pa_1 f'(x_0) &\equiv 0 \bmod p^2 \\ \Leftrightarrow b_1 + a_1 f'(x_1) &\equiv 0 \bmod p \end{aligned}$$

When $f'(x_1) \not\equiv 0 \bmod p$, we can always find a unique a_1 modulo p satisfying the last congruence, and hence lift x_1 to a solution x_2 modulo p^2. However, if $f'(x_1) \equiv 0 \bmod p$ then we can solve for a_1 if and only if $b_1 \equiv 0 \bmod p$. Now assume that we have a solution x_i for $f(x) \equiv 0 \bmod p^i$ for some $i \geq 1$ and we want to lift it to a solution x_{i+1} of $f(x) \equiv 0$ modulo p^{i+1}. Let $f(x_i) = p^i b_i$. We look for a_i such that $x_{i+1} = x_i + p^i a_i$ is a solution of $f(x) \equiv 0 \bmod p^{i+1}$. As before, we find that

$$\begin{aligned} f(x_i + p^i a_i) &\equiv 0 \bmod p^{i+1} \\ \Leftrightarrow f(x_i) + p^i a_1 f'(x_0) &\equiv 0 \bmod p^{i+1} \\ \Leftrightarrow b_i + a_i f'(x_i) &\equiv 0 \bmod p \end{aligned}$$

When $f'(x_i) \not\equiv 0 \bmod p$, we can always find a unique a_i modulo p satisfying the last congruence, and hence lift x_i to a solution x_{i+1} modulo p^{i+1}. However, if $f'(x_i) \equiv 0 \bmod p$ then we can solve for a_i if and only if $b_i \equiv 0 \bmod p$. Further, in the case $f'(x_i) \equiv 0 \equiv b_i \bmod p$, any choice a_i will give a lift, hence we have p lifts of x_i. This result about lifting of solutions of a polynomial from modulo p to higher powers is known is a weak form of a result known as Hensels' lemma. It will be beyond the scope of these lectures to describe Hensel's lemma fully.

2.6 Lecture 6

Preamble: In this lecture, we will discuss congruence modulo a prime number p. When the modulus is prime, one can deduce several interesting results. We will discuss Fermat's Little Theorem and Wilson's theorem.

Keywords: Fermat's Little Theorem, Wilson's theorem

2.6.1 Fermat's Little Theorem

Consider the prime $p = 3$. Observe that

$$\begin{aligned} 1^2 &\equiv 1 \bmod 3, \\ 2^2 &\equiv 1 \bmod 3. \end{aligned}$$

Similarly, for the prime $p = 5$, we observe that

$$\begin{aligned} 1^4 &\equiv 1 \bmod 5, \\ 2^2 &\equiv 1 \bmod 5, \\ 3^4 &\equiv 1 \bmod 5, \\ 4^4 &\equiv 1 \bmod 5. \end{aligned}$$

The above congruences are not a coincidence, as the following theorem explains. This theorem is known as Fermat's Little Theorem.

THEOREM 2.16. *Let p be a prime number and a be any integer co-prime to p. Then,*

$$a^{p1} \equiv 1 \ mod\ p.$$

Proof: Consider the two sets

$$\{1,\ 2,\ 3,\ \cdots,\ (p-1)\}, \qquad \{a,\ 2a,\ 3a,\ \cdots,\ (p-1)a\}.$$

In the second set,

$$\begin{aligned} ia &\equiv ja \bmod p \\ \implies p &\mid (i-j)a \\ \implies p &\mid (i-j) \\ \implies i &= j, \end{aligned}$$

as $1 \leq i,\ j \leq (p-1)$. Thus each element in the second set is congruent to a unique element of the first set. Hence, the product over all the elements of the two sets are congruent modulo p. Hence,

$$\begin{aligned} a.2a.3a.\cdots.(p-1)a &\equiv 1.2.3.\cdots.(p-1) \bmod p \\ \implies \quad (p-1)!a^{p-1} &\equiv (p-1)! \bmod p \\ \implies \quad a^{p-1} &\equiv 1 \bmod p, \end{aligned}$$

as $(p-1)!$ is coprime to p. $\square$

COROLLARY 2.17. *Let p be a prime and a be any integer. Then,*

$$a^p \equiv a \ mod\ p.$$

Proof: If a is not coprime to p, then p divides both a and a^p, and

$$a^p \equiv 0 \equiv a \bmod p.$$

If a is co-prime to p, then by Fermat's Little Theorem given above, we have

$$a^{p-1} \equiv 1 \bmod p \quad \implies \quad a^p \equiv a \bmod p. \qquad \square$$

2.6.2 Wilson's Theorem

Observe that for the first few primes 3, 5 and 7

$$\begin{aligned} 2! = 2 &\equiv -1 \bmod 3 \\ 4! = 24 &\equiv -1 \bmod 5 \\ 6! = 720 &\equiv -1 \bmod 7 \end{aligned}$$

It is not mere coincidence. This is true for any prime p.

THEOREM 2.18. *Let p be a prime, Then,*

$$(p-1)! \equiv -1 \ mod\ p.$$

The above theorem is known as Wilson's theorem. We will later see that the converse of the above theorem is also true.

Proof: If $1 \leq a \leq p-1$, we know that $ax \equiv 1$ has a solution which is unique modulo p. Thus, each a $(1 \leq a \leq p-1)$ has a unique element b, $1 \leq b \leq p-1$ such that $ab \equiv 1 \bmod p$. The element b can be thought of the inverse of a in multiplication modulo p. Now, a will be its inverse modulo p if and only if $a^2 \equiv 1 \bmod p$, i.e.,

$$\begin{aligned} p \quad &| \quad (a^2-1) \\ \Leftrightarrow p \mid (a-1) \quad &\text{or} \quad p \mid (a+1) \\ \Leftrightarrow a \quad &\equiv \quad \pm 1 \bmod p \\ \Leftrightarrow a = 1 \quad &\text{or} \quad a = p-1. \end{aligned}$$

In the product $1.2.\cdots.(p-1)$, each factor $a \neq \pm 1$ will have its inverse $b \neq a$ modulo p, so that the product ab will just give 1 modulo p. The remaining factors 1 and $(p-1)$ will multiply to give -1 modulo p. Therefore,

$$1.2.\cdots.(p-1) \equiv 1.(p-1) \equiv -1 \bmod p. \qquad \square$$

Now, let us prove the converse.

THEOREM 2.19. *Let n be a positive integer such that*

$$(n-1)! \equiv -1 \ \textit{mod}\ n.$$

Then, n is a prime number.

Proof: Let n be a composite number. Then, $n = ab$ where $2 \leq a,\ b \leq n-1$. If $a \neq b$, both a and b occur as a factor in the product $1.2.\cdots.(n-1)$, hence the product is divisible by n, and in this case

$$(n-1)! \equiv 0 \bmod n.$$

If $a = b$, then $n = a^2$. If $2a < n$, then the product $1.2.\cdots.(n-1)$ contains both a and $2a$ as factors, and hence $(n-1)!$ is divisible by $a^2 = n$. Again, we have

$$(n-1)! \equiv 0 \bmod n.$$

The remaining cases are $n = a^2$ where $2a \geq a^2$. Thus, $a = 1$ or 2, and $n = 1$ or $n = 4$. If $n = 4$, we have $3! = 6 = 2 \bmod 4$. Thus,

$$\begin{aligned} (n-1)! \quad &\equiv \quad 0 \bmod n \quad \forall \text{ composite number } n > 4. \\ (4-1)! \quad &\equiv \quad 2 \bmod 4 \text{ when } n = 4. \\ (1-0)! \quad &\equiv \quad 0 \bmod 1. \end{aligned}$$

This concludes the converse. $\square$

2.7 Lecture 7

Preamble: In this lecture, we will introduce pseudo-primes. A pseudo-prime is a actually composite number, but it has certain properties which prime numbers have.

Keywords: Pseudo-primes, Carmichael numbers

2.7.1 Pseudo-primes

Prime numbers are the building blocks for integers. It is of considerable interest to know whether a given integer is prime or not. The process of testing whether a given natural number is prime or not is called primality testing. We will discuss certain primality tests in section 10.1. While Wilson's theorem and its converse give a characterization for a number to be prime, it is not a very effective way as one has to compute $(n-1)!$ modulo n. Hence there is a need for developing other tests. We will discuss various primality tests in chapter 9 after we develop the theory needed for those tests. By corollary to Fermat's little theorem in the previous lecture, we have seen that for any prime number p, we must have

$$a^p \equiv a \bmod p.$$

So given an integer n, if

$$a^n \not\equiv a \bmod n$$

for some natural number a, we can immediately conclude that n is not prime. For computation, it is easiest to try $a = 2$. If $2^n \not\equiv 2 \bmod n$, then n fails this primality test with 2 as base, and we can immediately conclude that n is composite. For example, $2^6 = 64 \not\equiv 2 \bmod 6$, hence 6 fails the test, and hence 6 has to be composite. However, even if n passes the test, it may still be composite.

For example, consider the composite number $n = 341 = 11.31$. We will show that

$$2^{341} \equiv 2 \bmod 341.$$

As 11 and 31 are prime numbers, we have

$$\begin{aligned} & 2^{10} \equiv 1 \bmod 11, \\ \implies & 2^{340} \equiv 1 \bmod 11 \\ \implies & 2^{341} \equiv 2 \bmod 11 \end{aligned}$$

and

$$\begin{aligned} & 2^{30} \equiv 1 \bmod 31 \\ \Longrightarrow \quad & 2^{330} \equiv 1 \bmod 31 \\ \Longrightarrow \quad & 2^{341} \equiv 2^{11} \bmod 31 \\ & \equiv (2^5)^2.2 \bmod 31 \\ & \equiv 2 \bmod 31. \end{aligned}$$

Thus, 2^{341} is divisible by both 11 and 31, and hence by $11.31 = 341$, and

$$2^{341} \equiv 2 \bmod 341.$$

Definition 2.20. *A composite numbers n such that*

$$2^n \equiv 2 \ mod \ n.$$

is called a pseduo-prime, or more precisely, pseudo-prime to the base 2.

From the above example, 341 is a pseudo-prime. In fact, it is the smallest pseudo-prime. There are infinitely many pseudo-primes, which we can deduce from the following proposition.

Proposition 2.21. *If n is a pseudo-prime, then so is $2^n - 1$.*

Proof: We have $2^n \equiv 2 \bmod n$, so we can write $2^n = 2 + nk$ for some positive integer k. Then,

$$\begin{aligned} 2^n - 1 &= 1 + nk \\ \Longrightarrow \quad 2^{2^n-1} &= 2^{1+nk} = 2.(2^n)^k \\ &= 2.(2^n - 1 + 1)^k \bmod (2^n - 1) \\ &\equiv 2.(1)^k \bmod (2^n - 1) \\ &\equiv 2 \bmod (2^n - 1). \end{aligned}$$

Now it is enough to show that $2^n - 1$ is composite when n is composite. Let $n = rs$, where $r > 1$and $s > 1$. Then

$$2^{rs} - 1 = (2^r - 1)[(2^r)^{s-1} + (2^r)^{s-1} + \cdots + (2^r)^{s-1} + 1].$$

For $r > 1$, the factor $(2^r - 1) > 1$, and for $s > 1$, the factor

$$(2^r)^{s-1} + (2^r)^{s-1} + \cdots + (2^r)^{s-1} + 1 > 1.$$

Thus, $2^{rs} - 1$ must be composite for $r > 1$ and $s > 1$. $\square$

2.7.2 Carmichael Numbers

By corollary to Fermat's little theorem in the previous lecture, we have seen that for any prime number p, we have

$$a^p \equiv a \bmod p.$$

If a natural number n passes the pseudo-prime test, i.e., $2^n \equiv 2 \bmod n$, n may still be composite. So we can check whether $3^n \equiv 3 \bmod n$. If n fails the test with base 3, then one can immediately conclude that n is composite. For example 341 is composite, for it fails the primality test with base 3:

$$\begin{aligned} 3^{341} &\equiv (3^{30})^{11}.3^{11} \bmod 31 \\ &\equiv 1^{11}.(3^3)^3.3^2 \bmod 31 \\ &\equiv (-4)^3.9 \bmod 31 \\ &\equiv (-2).9 \bmod 31 \\ &\not\equiv 3 \bmod 31 \\ \implies 3^{341} &\not\equiv 3 \bmod (31.11 = 341). \end{aligned}$$

But if n passes the test with base 3, we should check with another base, till we exhaust all the bases from 2 to $(n-1)$. In fact, once n passes the test for bases a and b, it will also pass the test for the base ab, so one need not actually check all the bases 2 to $(n-1)$. If n fails the test for some base, we can conclude that n is composite. However, it may happen that n passes the test for all bases from 2 to $n-1$, but still be composite. Such an integer is called a Carmichael number.

DEFINITION 2.22. *A composite number n such that*

$$a^n \equiv a \ mod \ n$$

for any integer a is called a Carmichael number.

Example: 561 is a Carmichael number.

It is clearly composite, as $561 = 3.11.17$. Let a be any integer. We will show that $a^{561} \equiv a$ modulo 3, 11 and 17. If a is divisible by 3 (or by 11 or 17 respectively), it trivially follows that $a^{561} \equiv a$ modulo 3 (or modulo 11 or 17 respectively). If a is co-prime to 3, we have

$$a^2 \equiv 1 \bmod 3 \implies a^{560} \equiv (a^2)^{280} \equiv 1 \bmod 3 \implies a^{561} \equiv a \bmod 3.$$

Similarly, if a is coprime to 11, we have

$$a^{10} \equiv 1 \bmod 11 \implies a^{560} \equiv (a^{10})^{56} \equiv 1 \bmod 11 \implies a^{561} \equiv a \bmod 11.$$

Similarly, if a is coprime to 17, we have

$$a^{16} \equiv 1 \bmod 17 \implies a^{560} \equiv (a^{16})^{35} \equiv 1 \bmod 17 \implies a^{561} \equiv a \bmod 17.$$

One can show that there are no Carmichael numbers smaller than 561. Carmichael conjectured in 1912 that there are infinitely many Carmichael numbers. It was proved in 1992 by Alford Granville and Pomerance.

PROPOSITION 2.23. *A square-free number n is either prime or a Carmichael number if $p-1$ divides $n-1$ for every prime divisor p of n.*

Proof: Suppose

$$n = p_1.p_2.\cdots.p_r,$$

where p_i's are distinct primes and $p_i - 1$ divides $n-1$ for each i. We need to show that $a^n \equiv a$ modulo p_i for each p_i. This congruence follows trivially if a is divisible by p_i. If a_i is coprime to p_i, we have

$$\begin{aligned} a^{p_i-1} &\equiv 1 \bmod p_i \\ \implies a^{n-1} &\equiv 1 \bmod p_i \\ \implies a^n &\equiv a \bmod p_i. \\ \implies a^n &\equiv a \bmod p_1.\cdots.p_r. \end{aligned}$$ □

For the Carmichael number 561 that we demonstrated earlier, we find that 560 is divisible by $3-1$, $11-1$ and $17-1$.

2.8 Exercises

1. Find the last two digits of 3^{100}.
2. Find the last three digits of 7^{9999}.
3. Find the last digit of $7^{7^{7^{\cdots^{7}}}}$ where there are 1001 number of 7's.
4. Show that 1982 divides $22222\cdots222$ (1980 2's).
5. Find the smallest positive integer ending in 1986 divisible by 1987.
6. (i) Show that if $2n+1$ and $3n+1$ are both squares, then 40 divides n.
   (ii) Show that if $3n+1$ and $4n+1$ are both squares, then 56 divides n.
7. Let $a,\ b$ be integers. If a^2+b^2 is divisible by 7, show that it is also divisible by 49.
8. Find all primes p such that p^2+8 is also a prime.
9. Let p and q be two distinct primes. Show that pq divides $p^{q-1}+q^{p-1}-1$.
10. Let p, q, r be three distinct odd primes such that $r-1$ is a multiple of both $p-1$ and $q-1$. Show that 2^q-1 is divisible by pqr.
11. Show that
$$(1234)^{4321}+(4321)^{1234}\equiv 7 \bmod 11.$$
12. (i) Show that $4^{545}+545^4$ is not a prime.
   (ii) Show that n^4+4^n is never a prime for any integer n.
13. If $2^p+3^p=a^n$ for any prime p, show that $n=1$.
14. Show that $2(56!)+1$ is divisible by 59.
15. Let p be an odd prime. Show that
$$\left[2.4.\cdots.(p-1)\right]^2\equiv -(-1)^{\frac{p-1}{2}} \bmod p.$$
16. If p is a prime of the form $4k+1$, show that the quadratic congruence $x^2\equiv -1 \bmod p$ has a solution.
17. Show that $61!+1$ is divisible by 71.
18. Show that $63!+24$ is divisible by 73.

19. Find solutions of the following simultaneous congruences:

    (A) $x \equiv 2 \bmod 6, \quad x \equiv -3 \bmod 7, \quad x \equiv 5 \bmod 11.$

    (B) $4x \equiv 2 \bmod 6, \quad 5x \equiv -3 \bmod 7, \quad 3x \equiv 5 \bmod 11.$

20. Find the smallest positive integer n such that it leaves remainder 1 when divided by 11, 2 when divided by 12 and 3 when divided by 13.

21. Find the smallest positive integer n such that n is a multiple of 3, $n+1$ is a multiple of 4, and $n+2$ is a multiple of 5.

22. Find the smallest triple of consecutive integers n, $n+1$ and $n+2$ such that each of them is not square-free.

23. Show that the linear congruences in two variables

$$ax + by \equiv w \bmod ncx + dy \equiv z \bmod n$$

    has a unique solution modulo n if and only if $gcd(ad - bc, n) = 1$.

24. Find solutions of the following simultaneous congruences:

    (A) $x \equiv 2 \bmod 6, \quad x \equiv 4 \bmod 8, \quad x \equiv 5 \bmod 9.$

    (B) $x \equiv 1 \bmod 4, \quad x \equiv 3 \bmod 6, \quad x \equiv 6 \bmod 9.$

25. Can you find a positive integer n such that it leaves remainder 2 when divided by 10, 3 when divided by 1 and 12 when divided by 13?

26. Find a solution x_0 of $2x \equiv 5 \bmod 7^3$ such that $x_0 \equiv -6 \bmod 7^2$.

27. Solve $x^3 + x - 68 \equiv 0 \bmod 5^3$.

Module 3

Number Theoretic Functions

3.1 Lecture 1

Preamble: In this lecture we will discuss the greatest integer function. Its domain is real numbers, and range is the set of integers. It will also be useful to us when we introduce continued fractions later in this course.

Keywords: Greatest integer function

3.1.1 Greatest Integer Function

Given any real number x, we can always find an integer n such that

$$n \leq x < n + 1.$$

We refer to the integer n above as the *integral part* of the real number x, and denote it by $\lfloor x \rfloor$.

Definition 3.1. *The greatest integer function is defined as*

$$\begin{array}{rccc} \lfloor\ \rfloor : & \mathbb{R} & \longrightarrow & \mathbb{Z} \\ & x & \mapsto & n \end{array}$$

where n is the integral part of x.

For every real number x, there is a unique real number θ such that

$$x = \lfloor x \rfloor + \theta, \qquad 0 \leq \theta < 1.$$

θ is called the fractional part of x and is denoted by $\{x\}$. Thus, we have

$$x = \lfloor x \rfloor + \{x\} \qquad \forall x \in \mathbb{R}.$$

For example,

$$\begin{aligned} \lfloor 3.5 \rfloor &= 3 \\ \lfloor -3.5 \rfloor &= -4 \\ \lfloor \sqrt{2} \rfloor &= 1 \\ \lfloor -\sqrt{2} \rfloor &= -2 \end{aligned}$$

Now we look list some of the properties of the function $\lfloor\ \rfloor$.

PROPOSITION 3.2. *The greatest integer function has the following properties for any $x,\ y \in \mathbb{R}$ and $m \in \mathbb{Z}$.*

$$\begin{aligned} &(i) && \lfloor x+m \rfloor && = \lfloor x \rfloor + m \\ &(ii) && \lfloor x \rfloor + \lfloor -x \rfloor && = \begin{cases} 0, & \text{if } x \in \mathbb{Z} \\ -1, & \text{if } x \notin \mathbb{Z} \end{cases} \\ &(iii) && \lfloor x \rfloor + \lfloor y \rfloor && \leq \lfloor x+y \rfloor \\ &(iv) && \left\lfloor \tfrac{x}{m} \right\rfloor && = \left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor \\ &(v) && l \left\lfloor \tfrac{m}{k} \right\rfloor && \leq l \left\lfloor \frac{m}{k} \right\rfloor \qquad \forall\ l,\ k \in \mathbb{N}. \end{aligned}$$

Proof: Let

$$x = n + \theta, \qquad n \in \mathbb{Z},\ \ 0 \leq \theta < 1$$

$$
\begin{aligned}
(i) \qquad x+m &= (n+m)+\theta, \qquad (n+m)\in\mathbb{Z},\ 0\le\theta<1\\
\implies \lfloor x+m\rfloor &= n+m \ = \ \lfloor x\rfloor + m.
\end{aligned}
$$

$$
\begin{aligned}
(ii) \qquad -x &= -n-\theta, \qquad 0\ge -\theta > -1\\
\implies -x &= (-n-1)+(1-\theta), \qquad 1\ge 1-\theta>0\\
\implies \lfloor -x\rfloor &= \begin{cases} -n-1 & \text{if } 1-\theta\neq 1\\ -n-1+1=-n, & \text{if } 1-\theta=1\Leftrightarrow\theta=0\Leftrightarrow x\in\mathbb{Z}.\end{cases}\\
\implies \lfloor x\rfloor+\lfloor -x\rfloor &= \begin{cases} -1, & \text{if } x\notin\mathbb{Z}\\ 0 & \text{if } x\in\mathbb{Z}.\end{cases}
\end{aligned}
$$

$$
\begin{aligned}
(iii) \qquad y &= r+\theta', \qquad r\in\mathbb{Z} \qquad 0\le\theta'<1\\
\implies x+y &= (n+r)+(\theta+\theta') \qquad 0\le(\theta+\theta')<2\\
&= \begin{cases} n+r & \text{if } \theta+\theta'<1\\ n+r+1 & \text{if } \theta+\theta'\ge 1\end{cases}\\
\implies \lfloor x\rfloor+\lfloor y\rfloor &= n+r \ \le \lfloor x+y\rfloor.
\end{aligned}
$$

$$
\begin{aligned}
(iv) \qquad \tfrac{x}{m} &= q+t, \qquad q\in\mathbb{Z},\ 0\le t<1\\
\implies x &= mq+mt, \qquad 0\le mt<m\\
&= m\Big\lfloor\frac{x}{m}\Big\rfloor+mt\\
\implies \lfloor x\rfloor &= m\Big\lfloor\frac{x}{m}\Big\rfloor+r \qquad 0\le r<m\\
\implies \tfrac{\lfloor x\rfloor}{m} &= \Big\lfloor\frac{x}{m}\Big\rfloor+\frac{r}{m} \qquad 0\le\frac{r}{m}<1\\
\implies \Big\lfloor\tfrac{\lfloor x\rfloor}{m}\Big\rfloor &= \Big\lfloor\frac{x}{m}\Big\rfloor.
\end{aligned}
$$

$$
\begin{aligned}
(v) \qquad m &= kq+r, \qquad 0\le r<k\\
\implies \tfrac{lm}{k} &= lq+\frac{l}{k}.r, \qquad 0\le\frac{l}{k}.r\\
\implies \Big\lfloor\tfrac{lm}{k}\Big\rfloor &\ge lq \ = \ l.\Big\lfloor\frac{m}{k}\Big\rfloor. \qquad \square
\end{aligned}
$$

3.1.2 Applications

Now we show how the function $\lfloor\ \rfloor$ can be utilized for computation.

PROPOSITION 3.3. *Let n be any positive integer and p be any prime. The highest power of a prime p dividing $n!$ is given by*

$$\sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Proof: First note that the sum above is not really an infinite sum, as $p^k \leq n < p^{k+1}$ for some k, and we will have $\lfloor \frac{n}{p^i} \rfloor = 0$ for all $i > k$. Among the first n positive integers, the ones divisible by p are

$$p,\ 2p,\ 3p,\ \cdots, lp,$$

where lp is the largest multiple of p less than n. Thus, $n = lp + r$ where $0 \leq r < p$, and hence $l = \lfloor \frac{n}{p} \rfloor$. Each of these integers contribute at least 1 to the power p in the factorization of $n!$. However, some of those multiples of p will also be multiples of p^2, and their additional contribution of 1 each to the power of p has to be added. The total contribution from the multiples of p^2 will be from the following:

$$p^2,\ 2p^2,\ 3p^2,\ \cdots, \left\lfloor \frac{n}{p^i} \right\rfloor . p^2.$$

But some of the above may be multiples of p^3, and we will next take into account their contribution. Continuing in this fashion, we find that the power of p appearing in the factorization of $n!$ is

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots . \ \square$$

Example: Find the number of zeros at the end of 100!.

Solution: We need to find the highest power of 10 dividing 100!. As $10 = 2.5$, we need to take the minimum of (m, n), where m is the highest power of the prime 2 dividing 100, and n is the highest power of the prime 5 dividing 100!. In fact $n < m$, as it is clear

that 2 will occur more frequently in 100! than 5. By the previous proposition,

$$\begin{aligned} n &= \sum_{i=1}^{\infty} \left\lfloor \frac{100}{5^i} \right\rfloor \\ &= \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{5^2} \right\rfloor + \left\lfloor \frac{100}{5^3} \right\rfloor \\ &= 20 + 4 + 0 \\ &= 24. \qquad \square \end{aligned}$$

COROLLARY 3.4. *The product of r consecutive integers is divisible by $r!$ for any natural number r.*

Proof: It is enough to show that for any prime p, the power of p dividing $r!$ is not bigger than the power of p dividing

$$(m+1)(m+2)\cdots(m+r) = \frac{(m+r)!}{m!}.$$

Therefore, we want to establish that

$$\sum_{i=1}^{\infty} \left\lfloor \frac{r}{p^i} \right\rfloor \leq \sum_{i=1}^{\infty} \left\lfloor \frac{m+r}{p^i} \right\rfloor - \sum_{i=1}^{\infty} \left\lfloor \frac{m}{p^i} \right\rfloor$$

By the third property of the greatest integer function $\lfloor\ \rfloor$ listed above, we have

$$\begin{aligned} \left\lfloor \frac{r}{p^i} \right\rfloor + \left\lfloor \frac{m}{p^i} \right\rfloor &\leq \left\lfloor \frac{m+r}{p^i} \right\rfloor \qquad \forall i \in \mathbb{N} \\ \implies \left\lfloor \frac{r}{p^i} \right\rfloor &\leq \left\lfloor \frac{m+r}{p^i} \right\rfloor - \left\lfloor \frac{m}{p^i} \right\rfloor, \end{aligned}$$

and summing over i, we get the desired result. $\square$

3.2 Lecture 2

Preamble: In this lecture we will introduce an Euler's ϕ-function and its properties.

Keywords: Euler's ϕ-function

3.2.1 Euler's ϕ-function

Let n be a positive integer. Let U_n denote the set of positive integers not greater than n and coprime to it. For example,

$$\begin{aligned} U_6 &= \{1,5\}, \\ U_{10} &= \{1,3,7,9\}, \\ U_{18} &= \{1,5,7,11,13,17\}. \end{aligned}$$

Euler's ϕ function counts the number of elements in U_n.

DEFINITION 3.5. *Euler's ϕ function is a function*

$$\phi : \mathbb{N} \longrightarrow \mathbb{N}$$

such that for any $n \in mathbbN$ $\phi(n)$ is the number of integers less than n and coprime to it.

For example, $\phi(1) = 1,\ \phi(2) = 1,\ \phi(3) = 2,\ \phi(4) = 2,\ \phi(5) = 4,\ \phi(6) = 2$, etc.

PROPOSITION 3.6. *Let p be a prime. Then $\phi(p) = p - 1$.*

Proof: By definition, any natural number strictly less than p is coprime to p, hence $\phi(p) = p - 1$. $\square$

PROPOSITION 3.7. *Let p be a prime, and e be any positive integer. Then*

$$\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1).$$

Proof: Consider the successive p^e natural numbers not greater p^e arranged in the fol-

lowing rectangular array of p columns and p^{e-1} rows:

$$\begin{array}{cccc} 1 & 2 & \cdots & p \\ p+1 & p+2 & \cdots & 2p \\ \vdots & \vdots & \cdots & \vdots \\ p^e-p+1 & p^e-p+2 & \cdots & p^e \end{array}$$

Among these numbers, only the ones at the rightmost column are not coprime to p^e, and there are p^{e-1} numbers in that column. So

$$\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1). \qquad \square$$

For example, $\phi(8) = 2^3 - 2^2 = 4$ which counts the set number of elements in the set $U_8 = \{1,\ 3,\ 5,\ 7\}$.

By the fundamental theorem of arithmetic, we can write any natural number n as

$$n = p_1^{e_1} \cdots p_r^{e_r},$$

where p_i's are distinct primes and $e_i \geq 1$ are integers. We already know how to find $\phi(p_i^{e_i})$. We would like to see how $\phi(n)$ is related to the $\phi(p_i^{e_i})$s. This follows from a very important property of the Euler ϕ-function.

3.2.2 Multiplicativity of Euler's ϕ-function

THEOREM 3.8. *$\phi(m) = \phi(m)\phi(n)$ if m and n are coprime natural numbers.*

Proof: Consider the array of natural numbers not greater than mn arranged in m columns and n rows in the following manner:

$$\begin{array}{cccc} 1 & 2 & \cdots & m \\ m+1 & m+2 & \cdots & 2m \\ \vdots & \vdots & \cdots & \vdots \\ (n-1)m+1 & (n-1)m+2 & \cdots & (n-1)m+m = mn \end{array}$$

Clearly, each row of the above array has m distinct residues modulo m. Each column has n distinct residues modulo n: for $1 \leq i,\ i' \leq n-1$

$$\begin{array}{rrcl} & im+j & \equiv & i'm+j \bmod n \\ \implies & im & \equiv & i'm \bmod n \\ \implies & i & \equiv & i' \bmod n (\text{ as } gcd(m,n)=1) \\ \implies & i & = & i'. \end{array}$$

Each row has $\phi(m)$ residues coprime to m, and each column has $\phi(n)$ residues coprime to n. Hence, in total, there are $\phi(m)\phi(n)$ elements in the above array which are coprime to both m and n. It follows that $\phi(mn) = \phi(m)\phi(n)$. □

THEOREM 3.9. *Let n be any natural number. Then,*

$$\phi(n) = n\Big(1 - \frac{1}{p_1}\Big)\cdots\Big(1 - \frac{1}{p_r}\Big),$$

where p_i's are the distinct prime factors of n.

Proof: By fundamental theorem of arithmetic, we can write

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r},$$

where p_i are the distinct prime factors of n, and e_i are non-negative integers. By the previous theorem and proposition,

$$\begin{aligned}
\phi(n) &= \phi(p_1^{e_1})\cdots\phi(p_r^{e_r}) \\
&= p_1^{e-1}(p_1 - 1)\cdots p_r^{e-1}(p_r - 1) \\
&= p_1^{e}\Big(1 - \frac{1}{p_1}\Big).\cdots.p_r^{e}\Big(1 - \frac{1}{p_r}\Big) \\
&= n\Big(1 - \frac{1}{p_1}\Big).\cdots.\Big(1 - \frac{1}{p_r}\Big). \qquad \square
\end{aligned}$$

3.2.3 Euler's Theorem

We have seen while discussing Fermat's little theorem that $a^{p-1} \equiv 1 \bmod p$ for any integer a coprime to a prime number p. Note that the exponent $p-1$ equals $\phi(p)$. Let us now take a composite number, say $n = 12$ and another integer $a = 5$ coprime to 12. If we look at $a^{\phi(n)}$ modulo n, we find that

$$5^{\phi(12)} = 5^4 = 5^2.5^2 \equiv 1 \bmod 12.$$

The following theorem explains the above observation. The theorem is known as euler's theorem. It will be very useful for later discussions.

THEOREM 3.10. *Let a be an integer coprime to n. Then*

$$a^{\phi(n)} \equiv 1 \ mod\ n.$$

Proof: Let S be the set of positive integers less than n and coprime to it, say

$$S = \{a_1,\ a_2,\ \cdots,\ a_{\phi(n)}\}.$$

For any a coprime to n, consider the set

$$aS = \{aa_1, \cdots, aa_{\phi(n)}\}.$$

Each elements aa_i of aS is coprime to n. Moreover, any two distinct elements aa_i and aa_j of aS are distinct modulo n:

$$\begin{aligned} aa_i &\equiv aa_j \bmod n \\ \implies a_i &\equiv a_j \bmod n \\ \implies a_i &= a_j \end{aligned}$$

for $1 \leq a_i,\ a_j \leq n$. Hence, each element of $\{aa_1, \cdots, aa_{\phi(n)}\}$ is congruent to a unique element of S modulo n. Taking product of all elements of aS and comparing with the product of all elements of S, we obtain

$$\begin{aligned} aa_1.\cdots.aa_{\phi(n)} &\equiv a_1 \cdots a_{]phi(n)} \bmod n \\ \implies a^{\phi(n)}(a_1 \cdots a_{\phi(n)}) &\equiv a_1 \cdots a_{\phi(n)} \bmod n \\ \implies a^{\phi(n)} &\equiv 1 \bmod n. \end{aligned}$$

Note that as $a_1 \cdots a_{\phi(n)}$ is coprime to n, we can be cancel it from both sides of the congruence modulo n. $\square$

For example, consider $n = 18$. Then

$$\phi(18) = \phi(2)\phi(9) = (2-1)(3^2-3) = 6.$$

Euler's theorem says that $a^6 - 1$ is divisible by 18 for any integer a coprime to 18. Take $a = 5$. We can directly verify that

$$\begin{aligned} 5^6 &\equiv 25^3 \bmod 18 \\ &\equiv 7^3 \bmod 18 \\ &\equiv 7.(-5) \\ &\equiv 1 \bmod 18. \end{aligned}$$

THEOREM 3.11. *For any positive integer n,*

$$\sum_{d|n} \phi(d) = n.$$

Proof: Let us partition the set $\{1, 2, \cdots n\}$ into mutually disjoint subsets S_d for each $d \mid n$, where

$$\begin{aligned} S_d &= \{1 \leq m \leq n \mid gcd(m, n) = d\} \\ &= \Big\{1 \leq \frac{m}{d} \leq \frac{n}{d} \mid gcd\Big(\frac{m}{d}, \frac{n}{d}\Big) = 1\Big\}. \end{aligned}$$

Then,

$$\begin{aligned} n &= \sum_{d|n} \#S_d \\ &= \sum_{d|n} \#\phi\Big(\frac{n}{d}\Big) \\ &= \sum_{d|n} \phi(d), \end{aligned}$$

as for each divisor d of n, $\frac{n}{d}$ is also a divisor of n. □

3.3 Lecture 3

Preamble: In this lecture we will discuss an application of Euler's theorem in coding messages.

Keywords: Encryption, decryption, RSA

3.3.1 RSA cryptosystem

RSA cryptosystem is a way of coding and decoding messages which can be very hard to recover by any unwarranted third party without a secret key. Its security is based on the fact that it is very time-consuming even for very fast computers to factorize integers which are products of two distinct primes of big size (200 digits or so). A message is first converted to an integer and then that integer is converted to another integer (encryption) using a public key known to all. Then, the latter integer to the intended receiver. The receiver recovers the message with the help of his secret private key.

In order to convert the message into an integer, one uses the following dictionary for the alphabet:

$A = 00$	$K = 10$	$U = 20$	$1 = 30$
$B = 01$	$L = 11$	$V = 21$	$2 = 31$
$C = 02$	$M = 12$	$W = 22$	$3 = 32$
$D = 03$	$N = 13$	$X = 23$	$4 = 33$
$E = 04$	$O = 14$	$Y = 24$	$5 = 34$
$F = 05$	$P = 15$	$Z = 25$	$6 = 35$
$G = 06$	$Q = 16$	$, = 26$	$7 = 36$
$H = 07$	$R = 17$	$. = 27$	$8 = 37$
$I = 08$	$S = 18$	$? = 28$	$9 = 38$
$J = 09$	$T = 19$	$0 = 29$	$! = 39$

To indicate a space between two words, we use 99. For example, the message

Look inside the hall

becomes

$$M = 11141410990813180803049919070499070011111.$$

Let p and q be two distinct large primes of approximately same size, and let $n = pq$. Then,

$$\phi(n) = \phi(p)\phi(q) = (p-1)(q-1).$$

Let e be an integer coprime to $\phi(n)$. Then knowing $\phi(n)$, one can compute the inverse f of e modulo $\phi(n)$. In RSA cryptosystem, the pair (n, e) are public key. The integer f is the private key known only to the receiver. Using the public key, one can send a message M written as integer using the above dictionary by first encoding it as $M^e \bmod n$. The receiver receives the integer M^e. He can decrypt and recover the integer by performing $(M^e)^f$, where f is his secret key. Observe that

$$\begin{aligned} & ef &\equiv& \ 1 \bmod \phi(n) \\ \implies & ef &=& \ 1 + k\phi(n) \\ \implies & \left(M^e\right)^f &=& \ M^{1+k\phi(n)} \\ & &\equiv& \ M.M^{\phi(n)} \bmod n \\ & &\equiv& \ M \end{aligned}$$

Any eavesdropper may obtain the encrypted integer M^e, but it will take too much time for him/her to recover M from M^e without knowing f. Computation of f is possible when one knows the value of $\phi(n)$. But although n is made public, its factors p and q are not declared. It is too time consuming to factorize n which would enable one to compute $\phi(n)$.

Example: Let us demonstrate this with a simple example. We will take two small primes p and q so that the computations can be done with a small calculator. Let $p = 41$ and $q = 47$. We have $n = pq = 1927$ and $\phi(n) = 40.46 = 2^4.5.23 = 1840$. Let us choose an integer e coprime to 1840, say $e = 297$. Our encryption key will be e. For

decryption, we calculate the inverse f of e modulo $\phi(n) = 1840$ using Euclid's algorithm:

$$\begin{aligned}
1840 &= 297 \times 6 + 58 \\
297 &= 58 \times 5 + 7 \\
58 &= 7 \times 8 + 2 \\
7 &= 2 \times 3 + 1 \\
\implies 1 &= 7 - 2 \times 3 \\
&= 7 - 3 \times (58 - 7 \times 8) = 25 \times 7 - 3 \times 58 \\
&= 25 \times (297 - 58 \times 5) - 3 \times 58 = 25 \times 297 - 128(1840 - 297 \times 6) \\
&\equiv 793 \times 297 \bmod 1840. \\
\implies f &= 793.
\end{aligned}$$

To keep the computations small, let us demonstrate the encryption and decryption of the RSA cryptosystem with a small message. Assume that the message to be sent is

$$No.$$

This message is first converted to

$$M = 1314.$$

For encryption, we have to compute M^{297}. Observe that the binary expansion of 297 is

$$297 = 2^8 + 2^5 + 2^3 + 1 = 256 + 32 + 8 + 1.$$

In order to compute M^{297} modulo $n = 1927$ quickly, we will proceed as follows:

$$\begin{aligned}
M^2 = 1314^2 &\equiv 4 \bmod 1927 \\
M^4 = 4^2 &\equiv 16 \bmod 1927 \\
M^8 = 16^2 &\equiv 256 \bmod 1927 \\
M^{16} = 256^2 &\equiv 18 \bmod 1927 \\
M^{32} = 18^2 &\equiv 324 \bmod 1927 \\
M^{64} = 324^2 &\equiv 918 \bmod 1927 \\
M^{128} = 918^2 &\equiv 625 \bmod 1927 \\
M^{256} = 625^2 &\equiv 1371 \bmod 1927 \\
\implies M^{297} = M^{256}M^{32}M^8M &\equiv 1371.324.256.1314 \bmod 1927 \\
&= 364
\end{aligned}$$

The encrypted message is now $N = 364$. The receiver can get the original message M back from N by performing $N^f = 364^{793}$ as follows. Noting that that

$$793 = 2^9 + 2^8 + 2^5 + 2^3 + 1 = 512 = 256 + 16 + 8 + 1,$$

we proceed as

$$\begin{aligned}
N^2 &= 364^2 &&\equiv 1460 \bmod 1927\\
N^4 &= 1460^2 &&\equiv 338 \bmod 1927\\
N^8 &= 338^2 &&\equiv 551 \bmod 1927\\
N^{16} &= 551^2 &&\equiv 1062 \bmod 1927\\
N^{32} &= 1062^2 &&\equiv 549 \bmod 1927\\
N^{64} &= 549^2 &&\equiv 789 \bmod 1927\\
N^{128} &= 789^2 &&\equiv 100 \bmod 1927\\
N^{256} &= 100^2 &&\equiv 365 \bmod 1927\\
N^{512} &= 365^2 &&\equiv 262 \bmod 1927\\
\Longrightarrow N^{793} &= N^{512}N^{256}M^{16}N^8N &&\equiv 262.365.1062.551.364 \bmod 1927\\
&&&= 1314.
\end{aligned}$$

In this way the receiver can recover the original message M from the encrypted message N. □

3.4 Lecture 4

Preamble: In this lecture, we will discuss multiplicative functions. The multiplicative property of an arithmetic function yields interesting consequences. As an application of the notion of multiplicative function, we will characterize all even perfect numbers.

Keywords: Arithmetic function, multiplicative function, perfect numbers

3.4.1 Arithmetic Functions

A function $f : \mathbb{N} \longrightarrow \mathbb{C}$ is called an arithmetic function. An arithmetic function is called **multiplicative** if

$$f(mn) = f(m)f(n) \text{ when } gcd(m, n) = 1.$$

Examples:

1. $N_k(n) = n^k$ is multiplicative for any integer k.
2. Let n denote a natural number. Let $\phi(n)$ denote the number of positive integers less than n and prime to it. Recall that this function is known as Euler's ϕ-function and $\phi(mn) = \phi(m)\phi(n)$ if $gcd(m, n) = 1$.
3. $\omega : \mathbb{N} \longrightarrow \mathbb{Z} \geq 0$ given by $\omega(n) = \sum_{p|n} 1$ is also multiplicative:

$$\begin{aligned} m = p_1^{e_1}.\cdots.p_r^{e_r} &\implies \omega(m) = r \\ n = q_1^{f_1}.\cdots.q_s^{e_s} &\implies \omega(n) = s \\ mn = p_1^{e_1}.\cdots.p_r^{e_r}q_1^{f_1}.\cdots.q_s^{e_s} &\implies \omega(mn) = (-1)^{r+s}, \end{aligned}$$

   where p_i's and q_j's are pairwise distinct primes.

The following proposition is useful in constructing new multiplicative functions from known ones.

PROPOSITION 3.12. *Let f be a multiplicative arithmetic function and*

$$F(n) = \sum_{d|n} f(d).$$

Then F is also a multiplicative arithmetic function.

Proof: Let m and n be two coprime integers. If $d|mn$, we can write d uniquely as $d = d_1d_2$ such that $d_1|m$ and $d_2|n$. Conversely, if $d_1|m$ and $d_2|n$, then $d_1d_2|mn$. Clearly, if m and n are coprime, so are their divisors d_1 and d_2. Now,

$$\begin{aligned} F(mn) &= \sum_{d|n} f(d) \\ &= \sum_{d_1|m,\, d_2|n} f(d_1d_2) \\ &= \sum_{d_1|m,\, d_2|n} f(d_1)f(d_2) \\ &= \Big[\sum_{d_1|m} f(d_1)\Big]\Big[\sum_{d_2|n} f(d_2)\Big] \\ &= F(m)F(n) \qquad \square \end{aligned}$$

The above proposition gives us the following multiplicative functions:

1. Consider the arithmetic function τ given by

$$\tau(n) = \sum_{d|n} 1.$$

For any natural number n, $\tau(n)$ denotes the number of divisors of n. Now

$$\tau(n) = \sum_{d|n} 1 = \sum_{d|n} N_0(d),$$

where N_0 is the multiplicative functions that we saw previously. Hence $\tau(n)$ is multiplicative by the previous proposition.

2. Consider the function σ_k given by

$$\sigma_k(n) = \sum_{d|n} d^k = \sum_{d|n} N_k(d).$$

As N_k is multiplicative, so is $\sigma_k(d)$. We usually denote $\sigma_1(n)$ by $\sigma(n)$, thus

$$\sigma(n) = \sum_{d|n} d$$

is the sum of all the (positive) divisors of a natural number n and also a multiplicative function. Observe that $\tau = \sigma_0$.

If f is a multiplicative function, we need to know its values only for the prime powers.

PROPOSITION 3.13. *Let $n = p_1^{e_1} \cdots .p_r^{e_r}$ be the unique factorization of n. If f is a multiplicative function, then*

$$f(n) = f(p_1^{e_1}).\cdots .f(p_r^{e_r}).$$

Proof: It follows from the multiplicative property.

3.4.2 Perfect Numbers

We will now introduce perfect numbers. The multiplicative property of the function σ defined above is crucial in characterizing the perfect numbers.

DEFINITION 3.14. *A natural number n is called perfect if it is the sum of all its proper divisors, in other words,*

$$n = \sum_{d|n,\ 1\leq d<n} d.$$

In terms of the arithmetic function $\sigma(n)$, we can say that n is perfect if

$$2n = \sigma(n).$$

For example, 6 and 28 are perfect numbers, as $6 = 1+2+3$, and $28 = 1+2+4+7+14$. Now we first give a sufficient condition for a number to be perfect.

PROPOSITION 3.15. *Let p be a prime number such that $2^p - 1$ is also a prime. Then, $m = 2^{p-1}(2^p - 1)$ is a perfect number.*

Proof: It is enough to show that $\sigma(m) = 2m$. Observe that

$$\sigma(2^p - 1) = 1 + 2^p - 1$$

as $2^p - 1$ is a prime. Now,

$$\begin{aligned}
\sigma(m) &= \sigma(2^{p-1}(2^p - 1)) \\
&= \sigma(2^{p-1})\sigma(2^p - 1) \\
&= (1 + 2 + \cdots + 2^{p-1})(1 + 2^p - 1) \\
&= (2^p - 1)2^p \\
&= 2m. \qquad \square
\end{aligned}$$

The examples that we had mentioned earlier are in deed of the form $2^{2-1}(2^2 - 1) = 6$, and $2^{3-1}(2^3 - 1) = 28$. In fact any even perfect number that we find will necessarily of

this form, which we are going to prove in the next proposition.

PROPOSITION 3.16. *An even number is perfect only if it is of the form $2^p(2^{p-1}-1)$, where both p and 2^p-1 are primes.*

Proof: Let $m = 2^{k-1}l$, where $k \geq 2$ and l is odd. We want to show that l is a prime and that $l = 2^k - 1$. It will then follow that k is also prime, otherwise $k = rs$ with $r, s > 1$ would give two non-factors $2^r - 1$ and $2^s - 1$ of l. Note that l must be prime if $\sigma(l) = l + 1$. Now,

$$\begin{aligned} 2m = \sigma(m) &\implies 2^k l = \sigma(2^{k-1})\sigma(l) \\ &\implies 2^k l = (1 + 2 + \cdots + 2^{k-1})\sigma(l) \\ &\implies 2^k l = (2^k - 1)\sigma(l) \\ &\implies (2^k - 1)|l, \text{ say } l = (2^k - 1)t \\ &\implies 2^k t = \sigma(l). \end{aligned}$$

But t and $l = (2^k - 1)t$ are two divisors of l, which add up to

$$t + l = t + (2^k - 1)t = 2^k t = \sigma(l).$$

Hence t and $l = (2^k - 1)t$ are the only divisors of l, and l is a prime. As $2^k - 1 \geq 2^2 - 1$, we must have $t = 1$. Thus, $l = 2^k - 1$ is a prime, which implies k is prime too. □

3.5 Lecture 5

Preamble: In this lecture, we will an important arithmetic function called Mobius function, and discuss its properties.

Keywords: Mobius function, Mobius inversion formula

3.5.1 Mobius Function

DEFINITION 3.17. *The Mobius function $\mu : \mathbb{N} \longrightarrow \{0, \pm 1\}$ is defines as*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2 | n \text{ for some prime } p \\ (-1)^r & \text{if } n = p_1 p_2 \cdots .p_r, \text{ where } p_i \text{ are distinct primes} \end{cases}$$

For example,

$$\mu(1) = 1, \quad \mu(2) = -1, \quad \mu(3) = -1, \quad \mu(4) = 0,$$
$$\mu(5) = -1, \quad \mu(6) = 1, \quad \mu(7) = -1, \quad \mu(8) = 0.$$

If p is a prime, then $\mu(p) = 1$ and $\mu(p^e) = 0$ if $e \geq 2$.

THEOREM 3.18. *The Mobius function is a multiplicative, i.e.,*

$$gcd(m, n) = 1 \implies \mu(mn) = \mu(m)\mu(n).$$

Proof: Let m and n be coprime integers. We consider the following two cases.

Case 1: Let $\mu(mn) = 0$. Then there is a prime p such that $p^2 | mn$. As m and n are coprime, p can not divide both m and n. Hence either $p^2 | m$ or $p^2 | n$. Therefore, either $\mu(m) = 0$ or $\mu(n) = 0$, and we have $\mu(mn) = \mu(m)\mu(n)$.

Case 2: Now suppose $\mu(mn) \neq 0$. Then, mn is square-free, hence so are m and n. Let $m = p_1 \cdots p_r$ and $n = q_1 \cdots q_s$ where p_i and q_j are all distinct primes. Then, $mn = p_1 \cdots p_r q_1 \cdots q_s$ where all the primes occurring in the factorization of mn are distinct. Hence,

$$\mu(mn) = (-1)^{r+s} = (-1)^r (-1)^s = \mu(m)\mu(n). \qquad \square$$

THEOREM 3.19.

$$\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ if } n > 1 \end{cases}$$

where d runs through all the positive divisors of n.

Proof: Let

$$F(n) = \sum_{d|n} \mu(d).$$

As μ is multiplicative, so is $F(n)$ by proposition 1.1 of the previous lecture. Clearly,

$$F(1) = \sum_{d|n} \mu(d) = \mu(1) = 1.$$

For integers which are prime powers, i.e., of the form p^e for some $e \geq 1$,

$$\begin{aligned} F(p^e) &= \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^e) \\ &= 1 + (-1) + 0 + \cdots + 0 \\ &= 0. \end{aligned}$$

Now consider any integer n, and consider its prime factorization. Then,

$$\begin{aligned} n &= p_1^{e_1}.\cdots.p_r^{e_r}, \qquad e_i \geq 1 \\ \implies \quad F(n) &= \prod_i F(p_i^{e_i}) \\ &= 0. \qquad \square \end{aligned}$$

3.5.2 Mobius Inversion Formula

The following theorem is known as Mobius Inversion Formula.

THEOREM 3.20. *Let F and f be two functions from the set $\mathbb{N}$ of natural numbers to the field of complex numbers $\mathbb{C}$ such that*

$$F(n) = \sum_{d|n} f(d).$$

Then we can express $f(n)$ as

$$f(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big) F(d) = \sum_{d|n} \mu(d) F\Big(\frac{n}{d}\Big).$$

Proof: First, observe that if d is a divisor of n, so is $\frac{n}{d}$, and hence both the summations in the last line are the same. Now,

$$\sum_{d|n} \mu(d) F\Big(\frac{n}{d}\Big) = \sum_{d|n} \mu(d) \Big[\sum_{c|\frac{n}{d}} f(c)\Big]$$

The crucial step in the proof is to observe that the set S of pairs of integers (c, d) with $d|n$ and $c|\frac{n}{d}$ is the same as the set T of pairs of (c, d) with $c|n$ and $d|\frac{n}{c}$.

$$\begin{aligned}
\sum_{d|n} \mu(d) F\Big(\frac{n}{d}\Big) &= \sum_{d|n} \mu(d) \Big[\sum_{c|\frac{n}{d}} f(c)\Big] \\
&= \sum_{d|n} \sum_{c|\frac{n}{d}} \mu(d) f(c) \\
&= \sum_{(c,d)\in S} \mu(d) f(c) \\
&= \sum_{(c,d)\in T} \mu(d) f(c) \\
&= \sum_{c|n} f(c) \Big[\sum_{d|\frac{n}{c}} \mu(d)\Big] \\
&= f(n),
\end{aligned}$$

as $\sum_{d|\frac{n}{c}} \mu(d) = 0$ unless $\frac{n}{c} = 1$, which happens when $c = n$. □

Let us demonstrate this with $n = 15$:

$$\begin{aligned}
\sum_{d|15} \mu(d) F(\frac{15}{d}) &= \mu(1)[f(1) + f(3) + f(5) + f(15)] + \mu(3)[f(1) + f(5)] \\
&\quad + \mu(5)[f(1) + f(3)] + \mu(15) f(1) \\
&= f(1)[\mu(1) + \mu(3) + \mu(5) + \mu(15)] + f(3)[\mu(1) + \mu(5)] \\
&\quad + f(5)[\mu(1) + \mu(3)] + f(15)\mu(1) \\
&= f(1).0 + f(3).0 + f(5).0 + f(15) = f(15).
\end{aligned}$$

The above theorem leads to the following interesting identities:

1. We know that

$$\sum_{d|n} \phi(d) = n,$$

where $\phi(n)$ is Euler's ϕ-function. Hence

$$\phi(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big) d.$$

For example,

$$\phi(10) = \mu(1)10 + \mu(2)5 + \mu(5)2 + \mu(10).1 = 10 - 5 - 2 + 1 = 4.$$

2. Similarly,

$$\begin{aligned} \sigma(d) &= \sum_{d|n} d \\ \implies \quad n &= \sum_{d|n} \mu\Big(\frac{n}{d}\Big)\sigma(d). \end{aligned}$$

For example, with $n = 10$,

$$\begin{aligned} & \mu(10).1 + \mu(2).(1+5) + \mu(5).(1+3) + \mu(1).(1+3+5+10) \\ = \;& 1 - 1 - 5 - 1 - 3 + 1 + 3 + 5 + 10 \\ = \;& 10. \end{aligned}$$

We have seen before that if f is multiplicative, so is $F(n) = \sum_{d|n} f(d)$. But we can now prove the converse applying the Mobius inversion formula.

THEOREM 3.21. *Let F and f be two functions related by*

$$F(n) = \sum_{d|n} f(d).$$

If F is multiplicative, then so is f.

Proof: By the Mobius Inversion formula we know that

$$f(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big)F(d).$$

Let m and n be two coprime integers. Then, any divisor d of mn can be expressed uniquely as $d = d_1 d_2$ where $d_1|m$, $d_2|n$ and $gcd(d_1 d_2) = 1 = gcd(\frac{m}{d_1}, \frac{n}{d_2}))$. Conversely, if $d_1|m$ and $d_2|n$, then $d_1 d_2|mn$. Thus,

$$\begin{aligned} f(mn) &= \sum_{d|mn} \mu\Big(\frac{mn}{d}\Big)F(d) \\ &= \sum_{d_1|m,\, d_2|n} \mu\Big(\frac{mn}{d_1 d_2}\Big)F(d_1 d_2) \\ &= \sum_{d_1|m,\, d_2|n} \mu\Big(\frac{m}{d_1}\Big)\mu\Big(\frac{m}{d_2}\Big)F(d_1)F(d_2) \;\; \text{(as } \mu,\; F \text{ are multiplicative)} \\ &= \Big[\sum_{d_1|m} \mu\Big(\frac{m}{d_1}\Big)F(d_1)\Big]\Big[\sum_{d_2|n} \mu\Big(\frac{n}{d_2}\Big)F(d_2)\Big] \\ &= f(m)f(n). \qquad \square \end{aligned}$$

In view of the above theorem, we can say that as $N(n) = n$ is a multiplicative function, so is $\phi(n)$ because

$$\sum_{d|n} \phi(d) = n = N(n).$$

3.6 Lecture 6

Preamble: In this lecture, we will introduce Dirichlet product of two arithmetic functions. It will give the set of all arithmetic functions the structure of a monoid. Further, we will see how the Dirichlet product gives the structure of an abelian group to the set of all arithmetic functions which do not vanish at 1. The Mobius Inversion Formula also follows easily from Dirichlet product.

Keywords: Dirichlet Product, convolution

3.6.1 Dirichlet Product

DEFINITION 3.22. *Let f and g be two arithmetic function. The Dirichlet product or the convolution of f and g is an arithmetic function denoted by $f \star g$ and is defined by*

$$(f \star g)(n) = \sum_{d|n} f(d) g\Big(\frac{n}{d}\Big).$$

It is easy to observe that $f \star g = g \star f$. Recall the arithmetic functions I, u and N, defined respectively by

$$\begin{aligned} I(n) &= \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ if } n = 1. \end{cases} \\ u(n) &= 1 \qquad \forall n, \\ N(n) &= n \qquad \forall n. \end{aligned}$$

We have seen before that

$$\sum_{d|n} \phi(d) = n.$$

We can conclude that

$$\begin{aligned} \sum_{d|n} \phi(d) u\Big(\frac{n}{d}\Big) = n &= N(n) \\ \implies \phi \star u &= N. \end{aligned}$$

If two arithmetic functions F and f are related by $F(n) = \sum_{d|n} f(d)$, we can write this as $F = f \star u$. Therefore, we can rewrite the Mobius Inversion formula:

$$\begin{aligned} f(n) &= \sum_{d|n} \mu(d) F\Big(\frac{n}{d}\Big) \\ \implies f &= \mu \star F = F \star \mu. \end{aligned}$$

Let us now consider the operation $\star$ on the set A of all arithmetic functions. We have already seen that it defines a binary operation on A which is commutative. Now, we will show that $\star$ is associative, I is the identity for the operation $\star$ and an arithmetic function f with $f(1) \neq 1$ has an inverse in A with respect to the operation $\star$.

PROPOSITION 3.23. *let f, g, h be arithmetic functions. Then*

$$(f \star g) \star h = f \star (g \star h), \qquad f \star I = f = I \star f.$$

Proof:

$$\begin{aligned}
[(f \star g) \star h](n) &= \sum_{d|n} (f \star g)(d) h\Big(\frac{n}{d}\Big) \\
&= \sum_{d|n} \Big[\sum_{c|d} f(c) g\Big(\frac{d}{c}\Big)\Big] h\Big(\frac{n}{d}\Big) \\
&= \sum_{d|n,\, c|d} f(c) g\Big(\frac{d}{c}\Big) h\Big(\frac{n}{d}\Big)
\end{aligned}$$

If $d|n$ and $c|d$, then $c|n$. If c is a divisor of n, say $cm = n$, then $c|d$ and $d|n$ would imply $d = kc$ and $kc|cm$, i.e., $k|m$. Hence,

$$\begin{aligned}
[(f \star g) \star h](n) &= \sum_{c|n,\, k|m} f(c) \Big[g(k) h\Big(\frac{cm}{kc}\Big)\Big] \\
&= \sum_{c|n} f(c) \Big[\sum_{k|m} g(k) h\Big(\frac{m}{k}\Big)\Big] \\
&= \sum_{c|n} f(c) (g \star h)(m) \\
&= \sum_{c|n} f(c) (g \star h)\Big(\frac{n}{c}\Big) \\
&= [f \star (g \star h)](n).
\end{aligned}$$

Now,

$$\begin{aligned}
(f \star I)(n) &= \sum_{d|n} f(d) I\Big(\frac{n}{d}\Big) \\
&= \sum_{d=n} f(d).1 \\
&= f(n) \\
\Longrightarrow \quad f \star I &= f \ \ (= I \star f). \qquad \square
\end{aligned}$$

Let A^* denote the set of all arithmetic functions f with $f(1) \neq 0$. We can show that A^* is an abelian group under the Dirichlet product. First, we show that any arithmetic function with $f(1) \neq 0$ has an inverse for the Dirichlet product.

PROPOSITION 3.24. *let f be an arithmetic function with $f(1) \neq 0$, Let us define an arithmetic function g inductively by*

$$\begin{aligned} g(1) &= \frac{1}{f(1)}, \\ g(n) &= -\frac{1}{f(1)} \sum_{d|n,\ d<n} g(d) f\Big(\frac{n}{d}\Big) \text{ for } n > 1. \end{aligned}$$

Then,

$$g \star f = I = f \star g.$$

Proof: We need to show that $(g \star f)(1) = 1$ and $(g \star f)(n) = 0$ for $n > 1$. Clearly,

$$(g \star f)(1) = g(1)f(1) = 1.$$

For $n > 1$, we have

$$\begin{aligned} (g \star f)(n) &= g(n)f(1) + \sum_{d|n,\ d<n} g(d) f\Big(\frac{n}{d}\Big) \\ &= \Big[-\frac{1}{f(1)} \sum_{d|n,\ d<n} g(d) f\Big(\frac{n}{d}\Big)\Big] f(1) + \sum_{d|n,\ d<n} g(d) f\Big(\frac{n}{d}\Big) \\ &= 0. \qquad \square \end{aligned}$$

For example, the arithmetic functions $u(n) = 1$ for all n and the Mobius function $\mu(n)$ are inverses under Dirichlet product:

$$\begin{aligned} (u \star \mu)(1) &= 1, \\ (u \star \mu)(n) &= \sum_{d|n} u(d)\mu\Big(\frac{n}{d}\Big) \\ &= \sum_{d|n} \mu\Big(\frac{n}{d}\Big) \\ &= 0 \text{ for } n > 1 \\ \implies \quad u \star \mu &= I. \end{aligned}$$

Recall that $\star$ is a commutative operation, hence $\mu \star u = I$ as well.

PROPOSITION 3.25. *$(A^*, \star)$ is an abelian group.*

Proof: If $g, h \in A^*$ then $(g \star h)(1) = g(1)h(1) \neq 0$ hence A^* is closed under $\star$. We have seen $\star$ is associative, and I is the identity. By the previous proposition, each g in A^* has an inverse inside A^*. $\square$

PROPOSITION 3.26. *Let F and f be two arithmetic functions. Then*

$$F(n) = \sum_{d|n} f(d) \Leftrightarrow f(n) = \sum_{d|n} F(d)\mu\Big(\frac{n}{d}\Big).$$

Proof: Note that the forward implication is the Mobius inversion formula, which we have proved directly in the previous lecture. Here, we will prove it using the notion of convolution. Now,

$$\begin{aligned} F(n) &= \sum_{d|n} f(d) = \sum_{d|n} f(d)u\Big(\frac{n}{d}\Big) \\ \Leftrightarrow F &= f \star u \\ \Leftrightarrow F \star \mu &= (f \star u) \star \mu \\ \Leftrightarrow F \star \mu &= f \star (u \star \mu) \\ \Leftrightarrow F \star \mu &= f \star I = f \\ \Leftrightarrow f(n) &= \sum_{d|n} F(d)\mu\Big(\frac{n}{d}\Big). \qquad \square \end{aligned}$$

PROPOSITION 3.27. *If g and h are multiplicative, so is $g \star h$.*

Proof: Let m and n be two coprime integers. Then, any divisor d of mn can be expressed uniquely as $d = d_1 d_2$ where $d_1|m$, $d_2|n$ $\Big[$and $gcd(d_1 d_2) = 1 = gcd\Big(\frac{m}{d_1}, \frac{n}{d_2}\Big)\Big]$. Conversely, if $d_1|m$ and $d_2|n$, then $d_1 d_2|mn$. Thus,

$$\begin{aligned} (g \star h)(mn) &= \sum_{d|mn} g(d)h\Big(\frac{mn}{d}\Big) \\ &= \sum_{d_1|m,\, d_2|n} g(d_1 d_2)h\Big(\frac{mn}{d_1 d_2}\Big) \\ &= \sum_{d_1|m,\, d_2|n} g(d_1)g(d_2)h\Big(\frac{m}{d_1}\Big)h\Big(\frac{m}{d_2}\Big) \text{ (as } \mu, F \text{ are multiplicative)} \\ &= \Big[\sum_{d_1|m} g(d_1)h\Big(\frac{m}{d_1}\Big)\Big]\Big[\sum_{d_2|n} g(d_2)h\Big(\frac{n}{d_2}\Big)\Big] \\ &= (g \star h)(m)(g \star h)(n). \qquad \square \end{aligned}$$

The above proposition provides another way of proving the following result, which we established earlier.

COROLLARY 3.28. *If F and f are two arithmetic functions related by $F(n) = \sum_{d|n} f(d)$, then F is multiplicative if and only if f is multiplicative.*

Proof: We know that μ and u are multiplicative functions with $\mu \star u = u \star \mu = I$. Now, $F = f \star u$, hence if f multiplicative, so is $F \star u$ by the above proposition. For the converse,

$$F = f \star u \implies F \star \mu = (f \star u) \star \mu = f \star (u \star \mu) = f \star I = f.$$

If F is multiplicative, so is $F \star \mu$, hence f is multiplicative. □

3.7 Exercises

1. Determine all real numbers x for which

   (A) $\lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor = \lfloor 2x \rfloor$

   (B) $\lfloor x + \frac{1}{2} \rfloor + \lfloor x - \frac{1}{2} \rfloor = \lfloor 2x \rfloor$

   (C) $\lfloor 4x \rfloor = 4$

2. Find a counterexample to show that the statement

   $$\lfloor 3x + 3y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor + \lfloor 2x + 2y \rfloor$$

   is false.

3. For any two natural number m and n, show that

   $$\frac{(2m)!\,(2n)!}{m!\,n!\,(m+n)!}$$

   is an integer.

4. Show that $n!(n-1)!$ divides $(2n-2)!$ for any natural number n.

5. Show that $\frac{(2m)!}{m!\,m!}$ is an even integer for any natural number m.

6. Compute $\sigma(250)$, $\sigma_0(250)$, $\phi(250)$, $\mu(250)$, $\omega(250)$.

7. Find all integers n such that $\phi(n) = 12$.

8. Find all integers n such that $\phi(n) = 30$.

9. If d is a divisor of n, show that $\phi(d)$ divides $\phi(n)$.

10. Find all integers n such that $\phi(n) = \frac{n}{2}$.

11. Find all integers n such that $\phi(n) = \frac{n}{4}$.

12. Prove that $\phi(n^2) = n\phi(n)$.

13. Prove that $\phi(n) \mid n \implies n = 2^a 3^b$ for some non-negative integers a and b.

14. Show that $\phi(n) = 2k$ has no solution for $k = 7$. Show that 7 is the smallest value of k for which there is no solution.

15. Show that there are infinitely many integers n such that $\phi(n)$ divide n.

16. show that if $\phi(n)$ divides $n-1$, then n must be square-free.

17. Show that there are infinitely many integers for which $5\phi(n) = 4n$.

18. Prove that for any two positive integers,

$$\phi(m)\phi(n) = \phi(gcd(m,n))\phi(lcm(m,n)).$$

19. Prove that

$$\sum_{(a,n)=1,\ 1\leq a\leq n} a = \frac{n\phi(n)}{2}.$$

20. Let p be a prime number, and n be an integer satisfying $\phi(n) = 2p$. Find ten such pairs (p,n).

21. Prove that for every even positive integer n, n^2-1 divides $2^{n!}-1$.

22. If a number consists of a single digit with 2^n occurrences, then show that it has at least n distinct prime factors.

23. If p is a prime of the form $3k+2$ and p divides a^2+ab+b^2, then show that p divides both a and b.

24. Show that for integers $m \neq n$, and a odd, $a^{2^n}+2^{2^n}$ and $a^{2^m}+2^{2^m}$ are co-prime.

25. If n is an odd integer, show that n does not divide 3^n+1.

26. (A) Show that $m^{16}-n^{16}$ is divisible by 17 for integers m and n not divisible by 17.

    (B) Show that $m^{16}-n^{16}$ is divisible by 85 for integers m and n coprime to 85.

27. Show that

$$\prod_{d|n} d = n^{\sigma(n)}2.$$

28. Show that there are infinitely many positive integers such that $\sigma(n) > 2n$.

29. Show that there are infinitely many positive integers such that $\sigma(n) < 2n$.

30. If $\sigma(n) > 2n$ and p is a prime not dividing n, show that $\sigma(pn) > 2pn$.

31. Let n be an odd natural number. Prove that $\sigma(n)$ is odd if and only if n is a perfect square.

32. Let m be an even integer. We can write $m = 2^k n$ where n is odd. Show that $\sigma(m)$ is odd if and only if n is a perfect square.

33. If n is not a prime, show that $\sigma(n) > n + \sqrt{n}$.

34. Prove that
$$\sum_{d|n} \mid \mu(d) \mid = 2^{\omega(n)}.$$

35. Prove that
$$\sum_{d|n} \frac{\mu^2(d)}{\phi(d)} = \frac{n}{\phi(n)}.$$

36. Prove that
$$\sum_{d|n} \mu(d)\phi(d) = 0.$$

37. Prove that
$$\sum_{d|n} \mu(d)\sigma_0(d) = (-1)^{\omega(n)}.$$

38. Prove that
$$\sum_{d|n} \mu(d)\sigma(d) = \prod_{p|n}(-p).$$

39. Given any integer n_0, show that there can be only finitely many integers satisfying $\sigma(n) = n_0$.

40. Find the smallest integer n_0 for which $\sigma(n) = n_0$ has no solution, exactly one solution, exactly two solutions, exactly three solutions.

41. Prove that
$$\sum_{a=1}^{n}(a-1, n) = \sigma_0(n)\phi(n).$$

Module 4

Primitive Roots

4.1 Lecture 1

Preamble: In this lecture we will introduce primitive roots of an integer n. Powers of a primitive root gives all the positive integers less than and coprime to n.

Keywords: primitive root, order modulo n

4.1.1 Units Modulo an Integer

Let n be a positive integer. Consider the integers modulo n. If a is coprime to n, then by Euclid's algorithm we can find integers b and c such that

$$\begin{aligned} ab + nc &= 1 \\ \implies ab &\equiv 1 \bmod n. \end{aligned}$$

In other words, any iteger a which is coprime to n has an multiplicative inverse modulo n. Such an integer a is called a unit modulo n. The set of all units in $\mathbb{Z}_n$ is denoted by U_n. It is clear that if a is in U_n, so is its inverse. Moreover, if a and b are in U_n, so is their product modulo n. Thus, U_n is a group under multiplication. Clearly, U_n has $\phi(n)$ elements.

For example:

$$\begin{aligned} U_5 &= \{1,\ 2,\ 3,\ 4\}, \\ U_7 &= \{1,\ 2,\ 3,\ 4,\ 5,\ 6\}, \\ U_8 &= \{1,\ 3,\ 5,\ 7\}, \\ U_{15} &= \{1,\ 2,\ 4,\ 7,\ 8\ 11,\ 13,\ 14\}, \end{aligned}$$

Observe that each element in U_5 is a power of 2 modulo 5, and each element in U_7 is a power of 3 modulo 7. In other words U_5 and U_7 are cyclic groups under multiplication modulo 5 and 7 respectively, and 2 and 3 are their respective generators. On the other hand, we can not find such generating element in U_8, as square of each of its element is 1 modulo 8. We want to characterize the positive integers n such that U_n is cyclic.

4.1.2 Order of a Unit Modulo an Integer

Let $a \in U_n$. By Euler's theorem, we have $a^{\phi(n)} \equiv 1 \bmod n$.

DEFINITION 4.1. *Let h be the smallest positive integer such that $a^h \equiv 1$ mod n. Then h is called the order of a modulo n.*

PROPOSITION 4.2. *Let a be an integer co-prime to n, and let $a^k \equiv 1$ mod n. Then the order h of a modulo n divides k.*

Proof: By division algorithm, we can write $k = hq + r$ where $0 \leq r < h$. Our aim is to show that $r = 0$. We have

$$\begin{aligned} a^k &\equiv (a^h)^q a^r \bmod n \\ \implies 1 &\equiv a^r \bmod n \\ \implies r &= 0 \bmod n, \end{aligned}$$

otherwise there will be a positive integer r smaller than h such that $a^r \equiv 1 \bmod n$, contradicting the definition of the order of a. □

COROLLARY 4.3. *The order h of any element a in U_n divides $\phi(n)$.*

LEMMA 4.4. *Let a be an integer coprime to n. Then the order of a^i modulo n is*

$$d = \frac{h}{gcd(i,h)},$$

where h is the order of a modulo n

Proof: Let the order of a^i modulo n be m. We will show that $d|m$ and $m|d$. Observe that

$$(a^i)^m \equiv 1 \bmod n \implies h \mid im.$$

After canceling the gcd (h, i), we must have $d \mid m$. Conversely, it is clear from the definition of d that id is divisible by $d.gcd(i, h) = h$, hence

$$(a^i)^d \equiv a^{id} \equiv 1 \bmod n,$$

hence $m \mid d$. Thus, $m = d$. □

4.1.3 Primitive Roots

DEFINITION 4.5. *An integer g is called a primitive root modulo n if the order of g modulo n is $\phi(n)$.*

For example, 2 is a primitive root of $n = 5$. And so is 3. Similarly, 3 is a primitive root of 7. Primitive roots may not exist for certain integers n. For example, $U_{12} = \{1, 5, 7, 11\}$, and the order of 5, 7, 11 in U_{12} is 2, and the order of 1 is 1. Hence there are no primitive roots for 12. If one primitive root exists for an integer n, it is easy to prove that there are $\phi(\phi(n))$ of them. We will give a proof later.

PROPOSITION 4.6. *Let g be a primitive root of n. Then, $U_n = \{g^i \mid i = 1, 2, \cdots \phi(n)\}$.*

Proof: We know that U_n has $\phi(n)$ elements. Now for $1 \leq i, j \leq \phi(n)$,

$$\begin{aligned} g^i &\equiv g^j \bmod n \\ \implies g^{i-j} &\equiv 1 \bmod n \\ \implies \phi(n) &\mid (i-j) \\ \implies i &= j. \end{aligned}$$

Thus, $\{g^i \mid i = 1, 2, \cdots, \phi(n)\}$ is a subset of U_n with $\phi(n)$ elements. But $\phi(n)$ is the number of elements in U_n. Hence the proposition follows. □

PROPOSITION 4.7. *Suppose there exists a primitive root g of n. Then n has precisely $\phi(\phi(n))$ number of primitive roots.*

Proof: Any element of U_n is of the form g^i for some integer i. Suppose g^i is another primitive root of n. Then the order of g^i modulo n is $\phi(n)$, hence we must have

$gcd(i, \phi(n)) = 1$. Conversely, if $(i, \phi(n)) = 1$ then the order of g^i is $\phi(n)$. Hence there are precisely $\phi(\phi(n))$ primitive roots for n provided it has one. $\square$

For example, $U_{10} = \{1, 3, 7, 9\}$ and 3 is a primitive root. Hence so is $3^3 = 7$. But 1 and 9 are clearly of order ≤ 2, and they are not primitive roots. Hence the number of primitive roots is $2 = \phi(\phi(10))$.

4.2 Lecture 2

Preamble: We will show that each prime p has a primitive root.

Keywords: primitive roots

4.2.1 Existence of Primitive Roots for Primes

We have seen in the previous lecture the primes 5 and 7 have primitive roots. Now we will ascertain that any prime has a primitive root. We need to prove a result regarding the number of solutions to a polynomial congruence first. This result is known as Lagrange's theorem.

THEOREM 4.8. *Let p be a prime and*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

be a polynomial with integral coefficients such that
$nmida - n$. The the polynomial congruence

$$f(x) \equiv 0 \ mod \ p$$

has at most n distinct solutions modulo p.

Proof: We will use induction on degree of $f(x)$. If $n = 1$, then $a_1 x + a_0 \equiv 0 \bmod p$ clearly has a unique solution modulo p as $gcd(a_1, p) = 1$. Now assume that the theorem is true for all polynomials of degree $n = k \geq 1$. Consider a polynomial $f(x)$ of degree $k + 1$. Suppose α is a root of $f(x)$. Then, we can divide $f(x)$ by $x - \alpha$ and obtain

$$f(x) = (x - \alpha)g(x) + r,$$

where $g(x)$ also has integral coefficients and r is a constant. Substituting $x = \alpha$, we find that $r = 0$. Now, $g(x)$ has degree k and the coefficient of x^k must not be divisible by p, otherwise the coefficient of x^{k+1} in $f(x)$ will be divisible by p. If β us another root of $f(x)$ modulo p, then

$$f(\beta) \equiv 0 \bmod p \implies (\beta - \alpha)g(\beta) \equiv 0 \bmod p.$$

If $\beta \not\equiv \alpha \bmod p$, we must have $q(\beta) \equiv 0 \bmod p$. By induction hypothesis, there can be at most k such β's. Therefore, the number of roots of $f(x)$ modulo p is at most p. □

COROLLARY 4.9. *If p is a prime, and d is an integer dividing $p-1$, then the polynomial congruence*

$$x^d - 1 \equiv 0 \ mod\ p$$

has exactly d solutions.

Proof: We can write $p - 1 = dq$. Then,

$$x^{p-1} - 1 = (x^d - 1)(x^{d(q-1)} + x^{d(q-2)} + \cdots + x^d + 1) = (x^d - 1)f(x).$$

By Lagrange's theorem, $h(x)$ has at most $d(q-1) = p - 1 - d$ distinct solutions modulo p, and $x^d - 1$ has at most d distinct solutions modulo p. By Fermat's little theorem, $x^{p-1} - 1$ has exactly $p - 1$ distinct solutions modulo p. Any solution β of $x^{p-1} - 1$ that is not a solution of $f(x)$ must be a solution of $x^d - 1$:

$$(\beta^d - 1)(f(\beta)) \equiv \beta^{p-1} - 1 \equiv 0 \bmod p.$$
$$f(\beta) \not\equiv 0 \bmod p \implies \beta^d - 1 \equiv 0 \bmod p.$$

Therefore, $x^d - 1$ must have at least $p - 1 - (p - 1 - d) = d$ solutions. Combining with Lagrange's theorem, we can conclude that $x^d - 1$ has exactly d distinct solutions modulo p. □

THEOREM 4.10. *Let p be a prime. Then it has a primitive root, hence it has $\phi(p-1)$ primitive roots.*

Proof: The order d of any element of U_p must divided $\phi(p) = p - 1$. Moreover, let d be a divisor of $p - 1$, and $\psi(d)$ be the number of elements in U_p of order d, so that

$$\begin{aligned} \sum_{d|(p-1)} \psi(d) &= p - 1. \\ \sum_{d|(p-1)} \phi(d) &= p - 1 \\ \sum_{d|(p-1)} (\phi(d) - \psi(d)) &= 0. \end{aligned}$$

We claim that $\psi(d) \leq \phi(d)$ for each d. If $\psi(d)$ is 0, then it is obvious. Else, let a be an element of order d. Any element of order d is a root of $x^d - 1$ modulo p. But a, a^2, a^{d-1}, a^d are all distinct mod p, and they are roots of $x^d - 1$ modulo p. The number of solutions of $x^d - 1 = 0$ in $\mathbb{Z}_p$ is exactly d by the previous corollary. Hence, a, a^2, a^{d-1}, a^d are all the possible elements of order dividing d. Out of these, a^i has order d if and only if $gcd(d, i) = 1$. Hence, there are at most $\phi(d)$ elements of order d. Hence we must have $\psi(d) = \phi(d)$ for all $d \mid (p-1)$. In particular, $\psi(p-1) = \phi(p-1)$, and there are $\phi(p-1)$ elements of order $p - 1$. Thus there are $\phi(p-1)$ primitive roots for p. □

4.3 Lecture 3

Preamble: We have seen that every prime has a primitive root. Now we will investigate whether their powers have primitive roots. Finally, we will characterize all integers n which have primitive roots.

Keywords: primitive roots

4.3.1 Primitive Roots for Powers of 2

We begin by investigating whether powers of 2 have primitive roots. It is easy to note that 3 is a primitive root for 4. But 8 does not have a primitive root. The set U_8 of units modulo 8 is has four elements 1, 3, 5 and 7. But the order of 3, 5 and 7 modulo 8 is $2 < 4 = \#U_8$. We will now show that any higher power of 2 also does not have a primitive root.

PROPOSITION 4.11. *2^e does not have a primitive root for $e \geq 3$.*

Proof: We have already noticed that $a^2 \equiv 1 \bmod 8$ for any odd integer a:

$$\begin{aligned} a &= 2m+1 \\ \implies a^2 &= 4m(m+1)+1 \\ &\equiv 1 \bmod 8. \end{aligned}$$

Thus the order of any odd integer modulo 2^3 is at most $2 = 2^{3-2}$. We will show by induction on e that that the order of any odd integer a modulo 2^e is at most 2^{e-2}, i.e.,

$$a^{2^{e-2}} \equiv 1 \bmod 2^e.$$

Assume this is true for $e \geq 3$. Then

$$\begin{aligned} a^{2^{e-2}} &= 1 + k2^e \\ \implies a^{2^{e-1}} &= \left(1 + k2^e\right)^2 \\ &= 1 + 2^{e+1}(k + k^2 2^{e-1}) \\ &\equiv 1 \bmod 2^{e+1}. \end{aligned}$$

Therefore, the order of any odd integer a modulo 2^e is at most 2^{e-2}, which is strictly less that $\phi(2^e) = 2^{e-1}$. Thus, 2^e can not have a primitive root for any power of 2 other than 2 and 4. $\square$

4.3.2 Primitive Roots for Powers of Odd Primes

We will now show that the powers of odd primes always have a primitive root.

THEOREM 4.12. *Let p be an odd prime and e be any positive integer. Let g be a primitive root of p. Then either g or $g+p$ is a primitive root for p^e for all $e \geq 2$.*

Proof: First consider $e = 2$. Then $\phi(p^2) = p(p-1)$. By Euler's theorem, we have

$$g^{p(p-1)} \equiv 1 \bmod p^2.$$

Hence the order d of g modulo p^2 is either $(p-1)$ or $p(p-1)$. If $d = p(p-1)$, g is primitive root for p^2, so assume $d = p-1$. We claim that in this case $g+p$ is a primitive root for p^2. Let h be the order of $g+p$ mod p^2, so $h \mid p(p-1)$. Now,

$$\begin{aligned} (g+p)^h &\equiv 1 \bmod p^2 \\ \implies (g+p)^h &\equiv 1 \bmod p \\ \implies (p-1) &\mid h \\ \implies h &= (p-1)k. \end{aligned}$$

The only possibilities for h are $p-1$ or $p(p-1)$. But with $h = p-1$, we obtain

$$(g+p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}p \equiv 1 + (p-1)g^{p-2}p \not\equiv 1 \bmod p^2.$$

Hence $h = p(p-1)$ and $g+p$ is a primitive root for p^2.

Now let y be a primitive root mod p^e ($e \geq 2$). We claim that y is a primitive root for p^{e+1}. Let h be the order of y modulo p^{e+1}. Then, $h \mid \phi(p^{e+1})$, i.e., $h \mid p^e(p-1)$. Now,

$$\begin{aligned} y^h &\equiv 1 \bmod p^{e+1} \\ \implies y^h &\equiv 1 \bmod p^e \\ \implies \phi(p^e) = p^{e-1}(p-1) &\mid h, \end{aligned}$$

as y is a primitive root modulo p^e. Thus, either $h = p^{e-1}(p-1)$ or $h = p^e(p-1)$. It is now enough to rule out the former case.

We must have $y^{p^{e-2}(p-1)} \equiv 1 \bmod p^{e-1}$ by Euler's theorem. As y is a primitive root for p^e, we must have $y^{p^{e-2}(p-1)} \not\equiv 1 \bmod p^e$. Thus, $y^{p^{e-2}(p-1)} = 1 + kp^{e-1}$ for some integer k coprime to p. By binomial theorem,

$$y^{p^{e-1}(p-1)} = 1 + kp^e + \frac{p(p-1)}{2}k^2p^{2e-2}\cdots \equiv 1 + kp^e \not\equiv 1 \bmod p^{e+1}.$$

Thus, $h = p^e(p-1)$ and we are done. $\square$

4.3.3 Characterization of Integers with Primitive Roots

We have looked at existence of primitive roots for prime powers. Now we will investigate existence of primitive roots for integers which are not necessarily prime powers. The following lemma tells us that integers which are not prime powers in fact do not have a primitive root except for a few exceptional cases, which we will discuss in the theorem following the lemma.

LEMMA 4.13. *If $n = kl$ where $k > 2$ and $l > 2$ are two co-prime integers, then n does not have a primitive root.*

Proof: We will show that every integer co-prime to n has order strictly less that $\phi(n)$ modulo n. As ϕ is a multiplicative function, $\phi(n) = \phi(k)\phi(l)$. For $k,\ l > 2$, it is clear that $\phi(k)$ and $\phi(l)$ are both even. Hence $\phi(n)$ is divisible by 4, and $\frac{\phi(n)}{2}$ is divisible by both $\phi(k)$ and $\phi(l)$. If a is co-prime to n, it is also co-prime to both k and l. Applying Euler's theorem ot any integer coprime to n, we find that

$$\begin{aligned} a^{\phi(k)} \equiv 1 \bmod k \quad &\implies \quad a^{\frac{\phi(n)}{2}} \equiv 1 \bmod k \\ a^{\phi(l)} \equiv 1 \bmod l \quad &\implies \quad a^{\frac{\phi(n)}{2}} \equiv 1 \bmod l. \\ gcd(k,l) = 1 \quad &\implies \quad a^{\frac{\phi(n)}{2}} \equiv 1 \bmod n. \end{aligned}$$

Hence, the order of any integer coprime to n has order at most $\frac{\phi(n)}{2}$. Hence, n does not have a primitive root. $\square$

We can now identify all the natural numbers which have primitive roots.

THEOREM 4.14. *A natural number n has a primitive root if and only if n is one of the following: 1, 2, 4, p^e or $2p^e$ where p is an odd prime.*

Proof: Let p denote an odd prime. We have already seen that 1, 2, 4 and p^e have primitive roots. Let g be a primitive root of p^e. We want to exhibit a primitive root for $2p^e$ using g. Any primitive root of $2p^e$ must be odd. We will show that any odd primitive root of p^e will be a primitive root of $2p^e$. First we observe that p^e in deed has odd primitive roots. If g is a primitive root of p^e, so is $g + p^e$. As p^e is odd, one of g or $g+p^e$ is odd. Hence we can assume, without loss of generality, that g is an odd primitive root of p^e. Clearly, g coprime to $2p^e$. If the order of g modulo $2p^e$ is h, then $h \mid \phi(2p^e)$. Further,

$$g^h \equiv 1 \bmod 2p^e \implies g^h \equiv 1 \bmod p^e.$$

As g is a primitive root of p^e, we must have $\phi(p^e) \mid h$. But

$$\phi(2p^e) = \phi(2)\phi(p^e) = \phi(p^e).$$

As $h \mid \phi(p^{2e})$ and $\phi(2p^e) \mid h$, we conclude that $h = \phi(2p^e)$. Thus, $2p^e$ has a primitive root.

Conversely, suppose n has a primitive root. We want to show that n must be of one the above given forms. If n is not one of the above forms, then either (i) $n = 2^e$, $e \geq 3$ or (ii) $n = kl$ where $k > 2$ and $l > 2$ are two coprime integers. We have already seen that in each of the two cases n can not have a primitive root. □

4.3.4 Application of Primitive Roots

Consider a congruences of the form

$$x^m \equiv c \bmod n,$$

where c and n are coprime. If we have a primitive root g of n, we can find solutions to the above congruence as follows.

Suppose $c \equiv g^k \bmod n$. It is enough to find an integer i such that $1 \leq i \leq \phi(n)$ and $x \equiv g^i \bmod n$. Now

$$\begin{aligned} x^m &\equiv c \bmod n \\ \implies g^{im} &\equiv g^k \bmod n \\ \implies g^{im-k} &\equiv 1 \bmod n \\ \implies im &\equiv k \bmod \phi(n). \end{aligned}$$

So we need to solve only the linear congruence $im \equiv k \bmod \phi(n)$ for i to get solution $g^i = x$ for the non-linear congruence $x^m \equiv c \bmod n$.

Example: Solve the congruence $x^8 \equiv 5 \bmod 11$. We have

$$2^{\frac{11-1}{2}} \equiv -1 \bmod 11,$$

hence 2 is a primitive root for 11 by Euler's criterion. Now,

$$2^2 = 4, \;\; 2^3 = 8, \;\; 2^4 = 5.$$

Let $x = 2^i$. We need to find i such that

$$(2^i)^8 \equiv 2^4 \bmod 11.$$

We must have

$$8i \equiv 4 \bmod 10 \implies 2i \equiv 1 \bmod 5 \implies i \equiv 3 \bmod 5.$$

Hence $x \equiv 2^3 \equiv 8$ is a solution of $x^8 \equiv 5 \bmod 11$. $\square$

4.4 Exercises

1. (A) Find a primitive root for the following primes:

$$11,\ 13,\ 17,\ 19.$$

   (B) How many primitive roots does each prime above have?

   (C) List all the primitive roots for each of the primes above.

2. Find an element of

   (A) order 5 modulo 11

   (B) order 4 modulo 13

   (C) of order 8 modulo 17

   (D) of order 6 modulo 19.

3. Can you find a element of order 12 modulo 29?

4. If a is a primitive root of an odd prime p, show that

$$a^{\frac{p-1}{2}} \equiv -1 \bmod p.$$

5. If a and b are two primitive roots of an odd prime p, show that ab can not be a primitive root of p.

6. Show that the primitive roots of an odd prime p occur in pairs (a, a') where

$$aa' \equiv 1 \bmod p, \qquad a \not\equiv a' \bmod p.$$

7. Determine the product of all the primitive roots of an odd prime p modulo p.

8. let $p > 3$ be a prime, and a be a primitive root of p. Show that $-a$ is a primitive root of p if and only if $p \equiv 1 \bmod 4$.

9. Show that the congruence $x^2 \equiv 1 \bmod 24$ has 8 solutions. Conclude that Lagrange's theorem that the number of incongruent solutions of a polynomial congruence does not exceed the degree of the polynomial does not hold for composite moduli.

10. (A) Find a primitive root for the following prime powers:

$$5^2,\ 3^3,\ 7^2,\ 11^2,\ 11^3.$$

(B) How many primitive roots does each one of them have?

(C) Find the largest possible order of an element in U_n when n is

$$\begin{array}{llll} (i) & 25 & (ii) & 50 \\ (iii) & 75 & (iv) & 100. \end{array}$$

(D) List all the primitive roots for each one of them.

11. (A) List the composite numbers which have a primitive root in the following:

$$10,\ 12,\ 14,\ 15,\ 18,\ 21,\ 22,\ 28,\ 98.$$

(B) Find a primitive root for the composite numbers in the list found.

(C) Determine all the primitive roots in each case.

12. Find a solution of the following polynomial congruences

(A) $x^6 \equiv 2 \bmod 7$

(B) $x^8 \equiv 2 \bmod 11$

(C) $x^6 \equiv -1 \bmod 10$

13. Determine whether the polynomial congruence

$$x^6 \equiv 3 \bmod 10$$

has a solution.

14. Let g be a primitive root of an odd prime p. Show that

$$(p-1)! \equiv g.g^2.\cdots.g^{p-1} \bmod p.$$

Deduce Wilson's theorem from the above congruence.

15. Let p be an odd prime. Show that the elements $1^k,\ 2^k,\ \cdots,\ (p-1)^k$ form a reduced residue system if and only if k is coprime to p.

16. Let $a \geq 2$ be any integer coprime to n. Show that n divides $\phi\big(a^n - 1\big)$.

17. Show that 3is a primitive root of any prime of the form $2^n + 1$.

18. If $p$is any prime bigger than 3, show that the numerator of

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

is divisible by p^2.

19. (A) Compute $2^{30} \bmod 61$.

    (B) Is 2 a primitive root of 61?

    (C) Find all the elements of order 15 modulo 61.

    (D) Find all the solutions of $x^5 \equiv 83 \bmod 61$.

20. (A) Let g be a primitive root of an odd prime p such that $g^2 = g+1$ (for example, $g = 8$ and $p = 11$). Show that $g - 1$is also a primitive root.

    (B) If $p \equiv 3 \bmod 4$, prove that $(g-1)^{2k+3} \equiv g - 2 \bmod p$. Deduce that $g - 2$ is also a primitive root.

Module 5

Quadratic Residues

5.1 Lecture 1

Preamble: In this lecture, we will introduce quadratic residues of an integer n. The quadratic residues of n are the integers which are squares modulo n. We will particularly study quadratic residues of an odd prime p. We will discuss Euler's criterion, which specifies when an integer is a quadratic residue modulo p. Whether an integer a is a quadratic residue of p is indicated by a symbol called Legendre's symbol. We will also discuss properties of Legendre Symbol.

Keywords: Quadratic Residues, Legendre symbol, Euler's criterion

5.1.1 Definition and Examples

Let n be a positive integer. Recall that U_n denotes the set of positive integers which are not bigger than n and coprime to n.

Definition 5.1. *An integer a in U_n is called a quadratic residue of p if the equation $x^2 \equiv a \bmod n$ has a solution. In general, an integer a is called quadratic residue modulo n if it is coprime to n and is the square of an integer modulo n. If a is not a quadratic residue of n, we call it a quadratic non-residue.*

For example, 1 is a quadratic residue of p for any integer p. 2 is a quadratic non-residue of 3, as $1^2 \equiv 1 \equiv 2^2$ modulo 3. $5^2 \equiv 10 \bmod 15$ implies that 10 is a quadratic residue of 15, and 40 is also a quadratic residue modulo 15 as $5^2 \equiv 40 \bmod 15$.

PROPOSITION 5.2. *Let p be a prime. The number of quadratic residues of p is $\frac{p-1}{2}$.*

Proof: As $c^2 = (-c)^2$, the number of quadratic residues is at most $\frac{p-1}{2}$. On the other hand, if a be a quadratic residue of p, it follows easily that $x^2 \equiv a \bmod p$ has only two solutions modulo p as follows. Let $b \in U_p$ such that $b^2 \equiv a \bmod p$. Now

$$\begin{aligned} & x^2 \equiv a \bmod p \\ \implies \quad & x^2 \equiv b^2 \bmod p \\ \implies \quad & p \mid (x-b)(x+b) \\ \implies \quad & p \mid (x-b) \text{ or } p \mid (x+b) \\ \implies \quad & x \equiv b \text{ or } x \equiv -b \bmod p. \end{aligned}$$

As p is odd and b is coprime to p, $b \not\equiv -b \bmod p$. Hence $x^2 \equiv a \bmod p$ has precisely two solutions modulo p, namely b and $-b$. So there are exactly $\frac{p-1}{2}$ quadratic residues modulo p, and there are $\frac{p-1}{2}$ quadratic non-residues. □

5.1.2 Euler's Criterion

Euler's criterion tells us precisely when an integer a is a quadratic residue moduloan odd prime p. It is particularly useful in proving theoretical results concerning quadratic residues.

PROPOSITION 5.3. *Let p be an odd prime and $(a, p) = 1$. Then a is a quadratic residue modulo p if and only if $a^{\frac{p-1}{2}} \equiv 1$ mod p.*

Proof: Suppose a is a quadratic residue. Then there exists an integer b coprime to p such that

$$\begin{aligned} & a \equiv b^2 \bmod p \\ \implies \quad & a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \bmod p \end{aligned}$$

by Fermat's little theorem.

Conversely, suppose $a^{\frac{p-1}{2}} \equiv 1 \bmod p$. We know there exists a primitive g root for p, so that any integer in U_p can be expressed as $g^i \bmod p$ for some $1 \leq i \leq p-1$, and $g^m \equiv 1 \bmod p$ holds only when $(p-1) \mid m$. In particular, for some $1 \leq i \leq p-1$, we have

$$\begin{aligned} & a \equiv g^i \bmod p \\ \implies \quad & g^{i(\frac{p-1}{2})} \equiv a^{\frac{p-1}{2}} \equiv 1 \bmod p. \end{aligned}$$

By the property of the primitive root g mentioned above, $p-1$ must divide $i(\frac{p-1}{2})$. Therefore, i must be even, say $i = 2j$. Then, $a \equiv (g^j)^2 \bmod p$, and it follows that a is a quadratic residue. $\square$

5.1.3 The Legendre Symbol

The Legendre symbol is convenient notation to indicate whether an integer a is a quadratic residue modulo an odd prime p. The Legendre symbol of a modulo p is denoted by $\left(\frac{a}{p}\right)$.

DEFINITION 5.4. *Let p be an odd prime. If a is a non-zero quadratic residue modulo p, we denote it by $\left(\frac{a}{p}\right) = 1$. If a is a non-zero quadratic non-residue modulo p, we denote it by $\left(\frac{a}{p}\right) = -1$. If $p \mid a$, we write $\left(\frac{a}{p}\right) = 0$.*

For example, $\left(\frac{2}{7}\right) = 1$ as $3^2 \equiv 2 \bmod 7$. But $\left(\frac{2}{5}\right) = -1$ as the quadratic residues of 5 are precisely $(\pm 1)^2 = 1$ and $(\pm 2)^2 = 4$. Observe that as $a^{p-1} \equiv 1 \bmod p$ we must have $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$.

Using Legendre's symbol, we can now express Euler criterion as

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p. \tag{5.1}$$

PROPOSITION 5.5. *The Legendre symbol has the following properties:*

$$\begin{aligned}
&(i) \quad a \equiv b \ mod\ p \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).\\
&(ii) \quad \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ mod\ p.\\
&(iii) \quad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).
\end{aligned}$$

Proof: The first property is obvious, and the second is a restatement of (5.1). The third property is obvious when $p \mid ab$, as both sides of the equality are clearly zero. When p is coprime to ab, we have

$$\begin{aligned}
\left(\frac{ab}{p}\right) &\equiv (ab)^{\frac{p-1}{2}} \bmod p\\
&\equiv (a)^{\frac{p-1}{2}}(b)^{\frac{p-1}{2}} \bmod p\\
\implies \left(\frac{ab}{p}\right) &\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p
\end{aligned}$$

But both sides of the last congruence take values only ± 1. As the prime p is odd, one can conclude that both sides of the last congruence are either 1 or -1. Therefore the third property follows. $\square$

PROPOSITION 5.6. *Let p be an odd prime. Then $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1$ mod 4.*

Proof: By (5.1), we have $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \bmod p$. Since both sides of the congruence takes only ± 1 as values, and p is an odd prime, we have

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Now,

$$\begin{aligned} \left(\frac{-1}{p}\right) &= 1 \\ \Leftrightarrow (-1)^{\frac{p-1}{2}} &= 1 \\ \Leftrightarrow \frac{p-1}{2} &\in 2\mathbb{Z} \\ \Leftrightarrow p &\equiv 1 \bmod 4. \end{aligned}$$ $\square$

5.2 Lecture 2

Preamble: In this lecture we will prepare the groundwork for proving the law of quadratic reciprocity. We will prove a result known as Gauss lemma, which will play a crucial role in the proof of quadratic reciprocity.

Keywords: Gauss lemma

5.2.1 Gauss Lemma

Gauss lemma provides us with a method for computing the Legendre symbol. It will be crucial ingredient in our later results, in particular, in our discussions of quadratic reciprocity. As before, let p be an odd prime, and a be an integer coprime to p. Lets us consider the following sets of residues modulo p:

$$\begin{aligned} U_p &= \Big\{ \pm 1, \pm 2, \cdots, \pm\frac{p-1}{2} \Big\} \\ P &= \Big\{ 1,\ 2,\ \cdots,\ \frac{p-1}{2} \Big\}, \\ N &= \Big\{ -1,\ -2,\ \cdots,\ -\frac{p-1}{2} \Big\} \\ aP &= \Big\{ ax \bmod p | x \in P \Big\} \ = \ \{ a \bmod p,\ 2a \bmod p,\ \cdots,\ \Big(\frac{p-1}{2}\Big) a \bmod p \Big\}. \end{aligned}$$

Clearly, U_p forms a complete set of non-zero residues modulo p, and

$$U_p = P \cup N, \qquad aP \subset U_p.$$

Gauss lemma states that

LEMMA 5.7.

$$\Big(\frac{a}{p}\Big) = (-1)^{\mu},$$

where μ is the number of elements in the set $aP \cap N$.

Proof: Consider the following $\frac{p-1}{2}$ disjoint sets, each consisting of two elements:

$$\{\pm 1\},\ \ \{\pm 2\},\ \ \cdots \Big\{ \pm \Big(\frac{p-1}{2}\Big) \Big\}$$

For each i in P, ai modulo p lies in exactly one distinct set from the above sets:

$$\begin{aligned} & ai \equiv \pm aj \bmod p \\ \implies \quad & i \equiv \pm j \bmod p \qquad (\text{as } gcd(a,p) = 1) \\ \implies \quad & i \pm j \equiv 0 \bmod p \\ \implies \quad & i = j. \end{aligned}$$

Taking product of all the elements of the set aP, we have

$$a.2a.3a.\cdots.\frac{p-1}{2}a \equiv (-1)^{\mu} 1.2.\cdots.\frac{p-1}{2} \bmod p. \tag{5.2}$$

As the product $1.2.\cdots.\frac{p-1}{2}$ is coprime to p, (5.2) implies

$$a^{\frac{p-1}{2}} \equiv (-1)^{\mu} \bmod p.$$

By (5.1), we have

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

Hence,

$$\left(\frac{a}{p}\right) \equiv (-1)^{\mu} \bmod p.$$

As p is an odd prime, and both sides of the above congruence are ± 1, we must have

$$\left(\frac{a}{p}\right) = (-1)^{\mu}. \qquad \square$$

Example: Let us consider $p = 13$ and $a = 5$. Then,

$$P = \{1, 2, 3, 4, 5, 6\}, \qquad N = \{-1, -2, -3, -4, -5, -6\}.$$

We have $aP = \{5, -3, 2, -6, -1, 4\}$. So $aP \cap N$ has 3 elements. Hence,

$$\left(\frac{5}{13}\right) = (-1)^3 = -1,$$

and we can conclude that 5 is not a quadratic residue mod 13.

With $p = 13$ and $b = 3$, we obtain $bP = \{3, 6, -4, -1, 2, 5\}$, so that $bP \cap N$ has 2 elements. Hence $\left(\frac{3}{13}\right) = (-1)^2 = 1$, and 3 is a quadratic residue mod 13. We can verify that $4^2 \equiv 3 \bmod 13$. $\square$

5.2.2 An Application of Gauss Lemma

As an application of Gauss lemma, we will now characterize all odd primes p for which 2 is a quadratic residue.

PROPOSITION 5.8. *Let p be an odd prime. Then 2 is a quadratic residue of p if and only if $p \equiv 1$ or $p \equiv 7$ modulo 8. We can also restate this result as*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Proof: Consider

$$P = \left\{1,\ 2,\ \cdots,\ \frac{p-1}{2}\right\}, \qquad N = \left\{-1,\ -2,\ \cdots,\ -\frac{p-1}{2}\right\}.$$

Let i denote an element of P.

Case (1): Suppose $p \equiv 1 \bmod 4$. Then

$$2i \bmod p \in N \text{ for } \frac{p-1}{4} + 1 \leq i \leq \frac{p-1}{2}.$$

Thus,

$$|2P \cap N| = \frac{p-1}{2} - \frac{p-1}{4} = \frac{p-1}{4}.$$

By Gauss lemma, 2 is a quadratic residue modulo p if and only if $\frac{p-1}{4}$ is even. Thus 2 is a quadratic residue modulo for a prime $p \equiv 1 \bmod 4$ if $p \equiv 1 \bmod 8$ as well, and it is a quadratic non-residue if $p \equiv 1 \bmod 4$ but $p \equiv 5 \bmod 8$. Observe that $p^2 - 1$ is not divisible by 16 in the latter case.

Case (2): Suppose $p \equiv 3 \bmod 4$. Then

$$2i \bmod p \in N \text{ for } \frac{p-3}{4} + 1 \leq i \leq \frac{p-1}{2}.$$

Thus,

$$|2P \cap N| = \frac{p-1}{2} - \frac{p-3}{4} = \frac{p+1}{4}.$$

By Gauss lemma, 2 is a quadratic residue modulo p if and only if $\frac{p+1}{4}$ is even. Thus 2 is a quadratic residue modulo for a prime $p \equiv 3 \bmod 4$ if $p \equiv 7 \bmod 8$ as well, and it is a quadratic non-residue if $p \equiv 3 \bmod 4$ and $p \equiv 3 \bmod 8$, in which case $p^2 - 1$ is not divisible by 16. □

For example, 2 is not a quadratic residue of 5 or 11.

5.3 Lecture 3

Preamble: In this lecture we will prove a classical result known as the law of quadratic reciprocity, first established by Gauss. Let p and q be distinct odd primes. Quadratic reciprocity shows that if p is a quadratic residue modulo p, then p will also be a quadratic residue modulo q unless $p \equiv q \equiv 3 \bmod 4$. This simplifies the computation in determining whether a given integer is a quadratic residue modulo a prime, as we shall see.

Keywords: quadratic reciprocity, Gauss lemma

5.3.1 Quadratic Reciprocity

Observe that 13 is a quadratic residue modulo 3, and 3 is also a quadratic residue modulo 13. The former is easier to verify, as 3 is smaller than 13. Hence for a pair of odd primes p and q, it is useful to know whether p being a quadratic residue modulo q automatically implies q is a quadratic residue modulo p. The following example says that it can not be true for any two odd primes: let $p = 3$ and $q = 19$. Clearly, 19 is a quadratic residue modulo 3, but 3 is not a quadratic residue modulo 19: by Gauss lemma,

$$\left(\frac{3}{19}\right) = (-1)^{\mu}, \text{ where } \mu = |\{3, 6, 9, -7, -4, -1, 2, 5, 8\} \cap \{-1, -2, \cdots, -9\}| = 3.$$

The following theorem is known as the law of quadratic reciprocity.

THEOREM 5.9. *Let p and q be distinct odd primes. If p is a quadratic residue modulo p, then p will also be a quadratic residue modulo q unless $p \equiv q \equiv 3$ mod 4.*

Remark: we can express the above theorem also as

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \text{ unless } p \equiv q \equiv 3 \bmod 4,$$

or as

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Proof: We will use Gauss lemma to establish the theorem. Let us first consider whether p is a quadratic residue modulo q. Let us consider the two sets

$$P = \Big\{1,\ 2,\ \cdots,\ \frac{q-1}{2}\Big\}, \qquad N = \Big\{-1,\ -2,\ \cdots,\ -\frac{q-1}{2}\Big\}.$$

We know that $\left(\frac{p}{q}\right) = (-1)^{\mu}$, where μ is the number of x in P such that $px \equiv n \bmod q$ for some n in N. Thus μ is the number of elements x in P such that the inequality

$$-\frac{q-1}{2} \leq px - qy \leq -1$$

has a solution y in integers. We claim that such a solution y must lie in the set

$$Q = \Big\{1, 2, \cdots, \frac{p-1}{2}\Big\}.$$

We have

$$\begin{aligned} -\frac{q-1}{2} \leq px - qy \leq -1 \quad &\Longrightarrow \quad \frac{q-1}{2} \geq qy - px \geq 1 \\ \Longrightarrow \ \frac{q}{2} > qy - px > 0 \quad &\Longrightarrow \quad \frac{q}{2q} + \frac{p}{q}x > y > \frac{p}{q}x \\ \Longrightarrow \ \frac{1}{2} + \frac{p}{q}.\frac{q-1}{2} > y > 0 \quad &\Longrightarrow \quad \frac{p}{2} > y > 0, \end{aligned}$$

noting that y is an integer. Thus, μ is the number of pairs of integers (x, y) with

$$1 \leq x \leq \frac{q-1}{2}, \qquad 1 \leq y \leq \frac{p-1}{2}, \qquad 0 < qy - px < \frac{q}{2}.$$

Interchanging the roles of p and q, we obtain that $\left(\frac{q}{p}\right) = (-1)^{\nu}$ where ν is the number of pairs (x, y) with

$$1 \leq y \leq \frac{p-1}{2}, \qquad 1 \leq x \leq \frac{q-1}{2}, \qquad 0 > qy - px > -\frac{p}{2}.$$

Now,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu+\nu}.$$

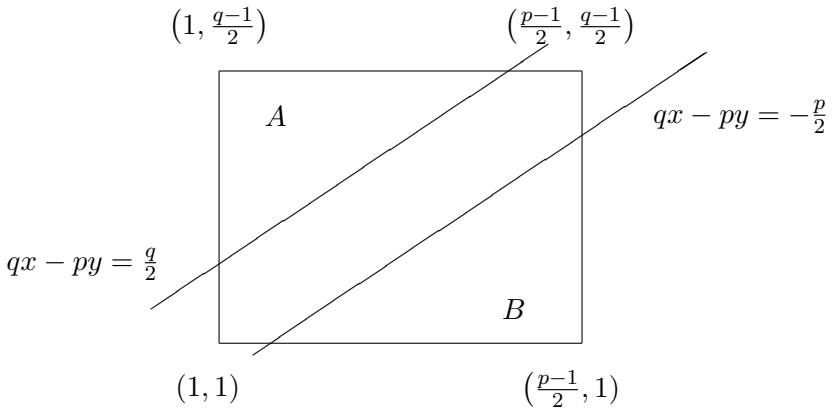
In order to prove quadratic reciprocity, we need to show that

$$\mu + \nu \equiv \Big(\frac{p-1}{2}\Big)\Big(\frac{q-1}{2}\Big) \bmod 2.$$

We now have

$$\mu + \nu = \#\Big\{(x, y) \in \mathbb{Z}^2 \mid 1 \leq x \leq \frac{q-1}{2}, \quad 1 \leq y \leq \frac{p-1}{2}, \quad -\frac{p}{2} < qy - px < \frac{q}{2}\Big\},$$

by combining the two conditions on $qy - px$, noting that $qy - px = 0$ is not possible for the given range for x and y).



Consider the number of integer points (x, y) inside the rectangle

$$R : 1 \leq x \leq \frac{q-1}{2}, \qquad 1 \leq y \leq \frac{p-1}{2}.$$

In total, there $\left(\frac{p-1}{2}\right).\left(\frac{q-1}{2}\right)$ such points in the rectangle. Out of these, $\mu + \nu$ points lie in the region bounded by the two lines $qy - px = -\frac{p}{2}$ and $qy - px = \frac{q}{2}$. But the number of remaining points in the rectangle is even by symmetry of the region A and B under

$$\begin{array}{rcl} A & \longrightarrow & B \\ (x, y) & \mapsto & \left(\frac{p+1}{2} - x, \frac{q+1}{2} - y\right) \\ 1 \leq x \leq \frac{p-1}{2},\ 1 \leq y \leq \frac{q-1}{2} & \Leftrightarrow & 1 \leq \left(\frac{p+1}{2} - x\right) \leq \frac{p-1}{2},\ 1 \leq \left(\frac{q+1}{2} - y\right) \leq \frac{q-1}{2}, \\ qx - py < \frac{q}{2} & \Leftrightarrow & q\left(\frac{p+1}{2} - x\right) - p\left(\frac{q+1}{2} - y\right) \\ & & = -\frac{p}{2} + \left[\frac{q}{2} - (qx - py)\right] > -\frac{p}{2}. \end{array}$$

Hence,

$$\left(\frac{p-1}{2}\right).\left(\frac{q-1}{2}\right) \equiv \mu + \nu \bmod 2. \qquad \square$$

For example, consider $p = 7$ and $p = 101$. Then,

$$\begin{array}{rcl} \left(\frac{7}{101}\right) & = & (-1)^{(\frac{7-1}{2}).(\frac{101-1}{2})}\left(\frac{101}{7}\right) \ = \ \left(\frac{3}{7}\right) \\ & = & (-1)^{(\frac{7-1}{2}).(\frac{3-1}{2})}\left(\frac{7}{3}\right) \ = \ -\left(\frac{1}{3}\right) \ = = -1. \end{array}$$

We can conclude that 5 is not a quadratic residue of the prime 101. Similarly, we find that

$$\begin{aligned}\left(\frac{11}{101}\right) &= (-1)^{(\frac{11-1}{2})\cdot(\frac{101-1}{2})}\left(\frac{101}{11}\right)\\ &= \left(\frac{2}{11}\right)\\ &= (-1)^{\frac{11^2-1}{8}}\\ &= -1.\end{aligned}$$

Hence, 11 is also not a quadratic reside of 101. Now, 35 will be a quadratic residue of 101 as

$$\begin{aligned}\left(\frac{35}{101}\right) &= \left(\frac{5}{101}\right)\left(\frac{7}{101}\right)\\ &= (-1)(-1) = 1. \qquad \square\end{aligned}$$

5.4 Lecture 4

Preamble: In this lecture we will first identify the quadratic residues of prime powers. Then, we will extend our discussion to quadratic residues of arbitrary integers.

Keywords: quadratic residues

5.4.1 Quadratic Residues of Powers of an Odd Prime

THEOREM 5.10. *Let p be an odd prime, and n be any positive integer. Then a is a quadratic residue of p^n if and only if it is a quadratic residue of p.*

Proof: If a is a quadratic residue of p^n for some $n \geq 1$, then there exists an integer x_0 such that

$$x_0^2 \equiv a \bmod p^n.$$

Then it trivially follows that

$$x_0^2 \equiv a \bmod p.$$

Conversely, let a be a quadratic residue of p. Then, there exists an integer x_0 such that

$$x_0^2 \equiv \bmod p.$$

We want to find an integer y_0 such that

$$y_0^2 \equiv a \bmod p^n.$$

We will proceed by induction on n. The existence is given for $n = 1$. Suppose such y_0 exists for $n = k \geq 1$. Then $y_0^2 = a + p^k b$ for some integer b. Let $z_0 = y_0 + p^k c$. Then,

$$\begin{aligned} z_0^2 &\equiv a \bmod p^{k+1} \\ \Leftrightarrow y_0^2 + 2p^k c y_0 + p^{2k} c^2 &\equiv a \bmod p^{k+1} \\ \Leftrightarrow a + p^k b + 2p^k c y_0 + p^{2k} c^2 &\equiv a \bmod p^{k+1} \\ \Leftrightarrow b + 2c y_0 &\equiv 0 \bmod p. \end{aligned}$$

As $2y_0$ is coprime to p, we can always find a solution $c = c_0$ for the linear congruence $b + 2cy_0 \equiv 0 \bmod p$. Going backwards, we can see that $z_0 = y_0 + p^k c_0$ is an integer with $z_0^2 \equiv a \bmod p^{k+1}$. □

Example: Determine whether 2 is a quadratic residue of 49. Then confirm by explicitly finding its square root modulo 49.

Solution: As 7 is a prime of the form $8k + 7$, 2 must be a quadratic residue of 7. The previous theorem tels us that 2 will be a quadratic residue of 7^2 as well. In order to determine the square root explicitly, first observe that $3^2 \equiv 2 \bmod 7$. Let $x_0 = 3 + 7c$. We want to find a valued of c such that

$$\begin{aligned} x_0^2 &\equiv 2 \bmod 49 \\ \Leftrightarrow 3^2 + 2.3.7c + 7^2c^2 &\equiv 2 \bmod 49 \\ \Leftrightarrow 9 + 2.3.7c &\equiv 2 \bmod 49 \\ \Leftrightarrow 1 + 6c &\equiv 0 \bmod 7 \\ \Leftrightarrow c &\equiv 1 \bmod 7 \end{aligned}$$

Thus, $3 + 7.1 = 10$ is a square root of 2 modulo 49. One can check that

$$10^2 = 100 \equiv 2 \bmod 49. \qquad \square$$

5.4.2 Quadratic Residues of Powers of 2

THEOREM 5.11. *(a) An integer a is a quadratic residue of 4 if and only if $a \equiv 1 \bmod 4$. (b) An integer a is a quadratic residue of 2^n for $n \geq 3$ if and only if $a \equiv 1 \bmod 8$.*

Proof: We can directly verify that 4 has only 1 as quadratic residue. Now, assume that $n \geq 3$. Let a be a quadratic residue of 2^n. Then there is an integer $b = 2l + 1$ such that $b^2 \equiv a \bmod 2^n$. It follows that

$$a \equiv 4l(l + 1) + 1 \bmod 2^n \implies a \equiv 1 \bmod 8.$$

Conversely, let a be an integer such that $a \equiv 1 \bmod 8$. we want to show that we can find an integer y_0 such that $y_0^2 \equiv a \bmod 2^n$. We will use induction on n. For $n = 3$, we can trivially verify that 1 is a quadratic residue of 8. Assume the statement is true for $k \geq 3$. Then, there exists an integer x_0 such that

$$x_0^2 \equiv a \bmod 2^k.$$

Then $x_0^2 = a + 2^k b$ for some integer b. We want to find an integer y_0 such that

$$y_0^2 \equiv a \bmod 2^{k+1}.$$

Let $y_0 = x_0 + 2^{k-1}c$. Then,

$$\begin{aligned} y_0^2 &\equiv a \bmod 2^{k+1} \\ \Leftrightarrow x_0^2 + 2.2^{k-1}cx_0 + 2^{2k-2}c^2 &\equiv a \bmod 2^{k+1} \\ \Leftrightarrow a + 2^k b + 2^k cx_0 + 2^{2k-2}c^2 &\equiv a \bmod 2^{k+1} \\ \Leftrightarrow b + cx_0 &\equiv 0 \bmod 2, \end{aligned}$$

as $k \geq 3$ implies $2k - 2 \geq k + 1$. But we can always solve the linear congruence $b + cx_0 \equiv 0 \bmod 2$ for c, as x_0 is odd. Choosing a solution $c = c_0$ for this linear congruence, and going backwards, we can see that

$$y_0 = x_0 + 2^{k-1}c_0$$

is an integer with $y_0^2 \equiv a \bmod 2^{k+1}$. □

Example: Determine whether 17 is a quadratic residue of 32. Then confirm by explicitly finding its square root modulo 32.

Solution: As $17 \equiv 1 \bmod 8$, it must be a quadratic residue of 2^5 by the previous theorem. In order to determine the square root explicitly, first observe that

$$1^2 \equiv 17 \bmod 16 = 2^{5-1}.$$

Let $x_0 = 1 + 8c$. We want to find a valued of c such that

$$\begin{aligned} x_0^2 &\equiv 17 \bmod 32 \\ \Leftrightarrow 1 + 2.8c + 64c^2 &\equiv 17 \bmod 32 \\ \Leftrightarrow -16 + 16c &\equiv 0 \bmod 32 \\ \Leftrightarrow -1 + c &\equiv 0 \bmod 2 \\ \Leftrightarrow c &\equiv 1 \bmod 2 \end{aligned}$$

Thus, $1 + 8.1 = 9$ is a square root of 17 modulo 32. One can check that

$$\begin{aligned} 9^2 - 17 &= 2.32 \\ \Longrightarrow 9^2 &\equiv 17 \bmod 32. \end{aligned}$$ □

5.4.3 Quadratic Residues of Arbitrary Moduli

THEOREM 5.12. *Let n be an arbitrary integer, and let*

$$n = 2^e.p_1^{e_1}.\cdots.p_r^{e_r}$$

be its factorization into prime powers. An integer a coprime to n is a quadratic residue if and only if

$$\begin{aligned} \left(\frac{a}{p_i}\right) &= 1 && \text{for } i = 1,\ 2,\ \cdots,\ r \\ a &\equiv 1 \ mod\ 4, && \text{if } 4 \mid n,\ \text{but } 8 \nmid n; \\ a &\equiv 1 \ mod\ 8 && \text{if } 8 \mid n. \end{aligned}$$

Proof: Consider the quadratic congruence

$$x^2 \equiv a \bmod n, \text{ where } gcd(a, n) = 1.$$

Solving this congruence is equivalent to solving the system of congruences

$$\begin{aligned} x^2 &\equiv a \bmod 2^e \\ x^2 &\equiv a \bmod p_1^{e_1} \\ x^2 &\equiv a \bmod p_2^{e_2} \\ &\vdots \quad \vdots \\ x^2 &\equiv a \bmod p^{e_r}. \end{aligned}$$

By the theorems is the previous two sections, we obtain our result. □

Example: 1. Determine whether 17 is a quadratic residue of $2^5.13^2.47^{100}$.

Solution: It is easy to check that $17 \equiv 2^2 \bmod 13$. Hence

$$\left(\frac{17}{13}\right) = 1.$$

Applying the law of quadratic reciprocity, we find that

$$\left(\frac{17}{47}\right) = \left(\frac{47}{17}\right) = \left(\frac{-4}{17}\right) = \left(\frac{-1}{17}\right) = 1.$$

As $17 \equiv 1 \bmod 8$ as well, 17 must be a quadratic residue of $2^5.13^2.47^{100}$ by the previous theorem. □

5.5 Lecture 5

Preamble: In this lecture, we will generalize the notion of Legendre symbol and introduce Jacobi symbol. In Jacobi symbol, the modulus can be composite as well. Jacobi symbol will also satisfy a reciprocity law. This property help us eventually in computing the Legendre symbol, as we shall see.

Keywords: Jacobi symbol, quadratic reciprocity

5.5.1 The Jacobi Symbol

Earlier in this chapter we talked about quadratic residues modulo an odd prime p. Now we will also look at quadratic residues modulo any odd natural number P. It is worthwhile to note that when we compute the Legendre symbol $\left(\frac{a}{p}\right)$ where a is relatively small compared to the prime p, we need to factorize a into primes and then use quadratic reciprocity so that knowing the Legendre symbol of p modulo prime factors of a are enough. We will see that we need not factorize a provided we have a reciprocity law for composite modulus as well. Hence, there is a need to extend the notion of Legendre symbol to composite moduli in a way that quadratic reciprocity holds as well. Note that while 9 is a quadratic residue modulo 5, 5 is not a quadratic residue modulo 9. Hence, if we simply extend the definition of Legendre symbol to a composite modulus P by assigning 1 as value for a quadratic residue modulo P and -1 for a quadratic non-residue modulo P, it will not result in quadratic reciprocity. Hence we Jacobi symbol is defined as follows:

DEFINITION 5.13. *Let P be an odd natural number, where*

$$P = p_1.\cdots.p_r,$$

where p_i's are odd primes, not necessarily distinct. Let A be any integer. The Jacobi symbol of A modulo P is denoted by $\left(\frac{A}{P}\right)$, and is defined as

$$\left(\frac{A}{P}\right) = \left(\frac{a}{p_1}\right).\left(\frac{a}{p_2}\right).\cdots.\left(\frac{a}{p_r}\right).$$

It is clear form the definition that $\left(\frac{A}{P}\right) = 0$ if and only if $\left(\frac{a}{p_i}\right) = 0$ for some prime p_i or equivalently $gcd(A, P) \neq 1$. The Jacobi symbol takes only three values: 0, 1 or -1. When P is an odd prime, the Jacobi symbol is nothing but the Legendre symbol. But the Jacobi symbol $\left(\frac{A}{P}\right)$ may be 1 even when A is not a quadratic residue modulo the

odd composite integer P. For example, $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = 1$. However, note that 2 is not a quadratic residue of 15. We have the following:

PROPOSITION 5.14. *Let P be an odd positive integer and A be any integer coprime to P. The Jacobi symbol $\left(\frac{A}{P}\right)$ is 1 if A is a quadratic residue modulo P.*

Proof: If A is a quadratic residue modulo P, then A is a quadratic residue modulo each prime factor p_i of P. Therefore, $\left(\frac{A}{p_i}\right) = 1$ for each $p - i$, and $\left(\frac{A}{P}\right)$ is just a product of 1. □

The converse of the above proposition does not hold, as we saw with $A = 2$ and $P = 15$.

PROPOSITION 5.15. *Let P and Q be odd positive integers, and A, B be integers. The Jacobi symbol has the following properties:*

$$
\begin{aligned}
&(i) \quad A \equiv B \ mod\ P \implies \left(\frac{A}{P}\right) = \left(\frac{B}{P}\right).\\
&(ii) \quad \left(\frac{AB}{P}\right) = \left(\frac{A}{P}\right)\left(\frac{B}{P}\right).\\
&(iii) \quad \left(\frac{A}{PQ}\right) = \left(\frac{A}{P}\right)\left(\frac{A}{Q}\right).\\
&(iv) \quad \left(\frac{Q^2}{P}\right) = \left(\frac{P}{Q^2}\right) = 1 \qquad when\ gcd(P,Q) = 1.\\
&(iv) \quad \left(\frac{AB^2}{PQ^2}\right) = \left(\frac{A}{P}\right) = 1 \qquad when\ gcd(AB,PQ) = 1.
\end{aligned}
$$

Proof: These properties follow easily from the definition of the Jacobi symbol and the corresponding properties of the Legendre symbols of the primes p_i dividing P. □

5.5.2 The Jacobi Symbol of -1 and 2

THEOREM 5.16. *If P is an odd positive integer, then*

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}.$$

We will use the following lemma in the proof of the above theorem.

LEMMA 5.17. *For odd integers m and n, we have*

$$\frac{mn-1}{2} \equiv \frac{m-1}{2} + \frac{n-1}{2} \ mod\ 2.$$

In particular, if we odd primes $p_1, \cdots, p_r$ (not necessarily distinct), we have

$$(-1)^{\frac{p_1.\cdots.p_r-1}{2}} = (-1)^{\frac{p_1-1}{2}+\cdots+\frac{p_r-1}{2}}.$$

Proof of the lemma: Observe that as $m-1$ and $n-1$ are even,

$$\begin{aligned} mn-1 &= (m-1)(n-1)+(m-1)+(n-1) \\ &\equiv (m-1)+(n-1) \bmod 4 \\ \implies \frac{mn-1}{2} &\equiv \frac{m-1}{2}+\frac{n-1}{2} \bmod 2. \\ \implies (-1)^{\frac{mn-1}{2}} &= (-1)^{\frac{m-1}{2}+\frac{n-1}{2}}. \end{aligned}$$

The last identity can be extended to the product of any r odd natual numbers. □

Proof of the theorem: We know that

$$\begin{aligned} P &= p_1.\cdots.p_r \\ \implies \left(\frac{-1}{P}\right) &= \left(\frac{-1}{p_1}\right).\cdots.\left(\frac{-1}{p_r}\right) \\ &= (-1)^{\frac{p_1-1}{2}+\cdots+\frac{p_r-1}{2}} \\ &= (-1)^{\frac{p_1p_2\cdots p_r-1}{2}} \\ &= (-1)^{\frac{P-1}{2}} \end{aligned}$$

by the previous lemma. □

THEOREM 5.18. *If P is an odd positive integer, then*

$$\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}.$$

Proof: We know that

$$\begin{aligned} P &= p_1.\cdots.p_r \\ \implies \left(\frac{2}{P}\right) &= \left(\frac{2}{p_1}\right).\cdots.\left(\frac{2}{p_r}\right) \\ &= (-1)^{\frac{p_1^2-1}{8}+\cdots+\frac{p_r^2-1}{8}} \end{aligned}$$

For odd integers m and n, observe that m^2-1 and n^2-1 are divisible by 8, and

$$\begin{aligned} m^2n^2-1 &= (m^2-1)(n^2-1)+(m^2-1)+(n^2-1) \\ &\equiv (m^2-1)+(n^2-1) \bmod 16 \\ \implies \frac{m^2n^2-1}{8} &\equiv \frac{m^2-1}{8}+\frac{n^2-1}{8} \bmod 2 \\ \implies (-1)^{\frac{m^2n^2-1}{8}} &= (-1)^{\frac{m^2-1}{8}+\frac{n^2-1}{8}} \end{aligned}$$

Using the last equality repeatedly, we find that

$$\left(\frac{2}{P}\right) = (-1)^{\frac{p_1^2 \cdots p_r^2 - 1}{8}} = (-1)^{\frac{P^2-1}{8}}. \qquad \square$$

5.5.3 Quadratic Reciprocity for the Jacobi Symbol

THEOREM 5.19. *Let P and Q be two relatively prime odd positive integers. Then,*

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}.$$

Proof: The proof relies on the quadratic reciprocity law for Legendre symbols involving the prime factors of P and Q and the lemma that we proved in this section.

$$\begin{aligned}
P &= p_1 \cdots p_r, \\
Q &= q_1 \cdots q_s, \\
\Longrightarrow \left(\frac{Q}{P}\right) &= \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right) \\
&= \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}}\left(\frac{p_i}{q_j}\right) \qquad \text{(by quadratic reciprocity for Legendre symbols)} \\
&= \left[\prod_{i=1}^{r}\left((-1)^{\sum_j \frac{q_j-1}{2}}\right)^{\frac{p_i-1}{2}}\right]\left[\prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)\right] \\
&= \prod_{i=1}^{r}\left((-1)^{\frac{Q-1}{2}}\right)^{\frac{p_i-1}{2}}\left(\frac{P}{Q}\right) \qquad \text{(by the previous lemma)} \\
&= \left((-1)^{\sum_i \frac{p_i-1}{2}}\right)^{\frac{Q-1}{2}}\left(\frac{P}{Q}\right) \\
&= \left((-1)^{\frac{P-1}{2}}\right)^{\frac{Q-1}{2}}\left(\frac{P}{Q}\right) \qquad \text{(by the previous lemma)} \\
&= (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right). \qquad \square
\end{aligned}$$

5.6 Exercises

1. Let p be an odd prime. Then show that

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 8 \quad \text{or } p \equiv 3 \bmod 8 \\ -1 & \text{if } p \equiv \pm 5 \bmod 8 \quad \text{or } p \equiv 7 \bmod 8 \end{cases}$$

2. Let p be an odd prime other than 3. Then show that

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 12 \\ -1 & \text{if } p \equiv \pm 5 \bmod 12 \end{cases}$$

3. Let p be an odd prime other than 3. Then show that

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 6 \\ -1 & \text{if } p \equiv 5 \bmod 6 \end{cases}$$

4. Determine all primes p such that $p-2$ is a quadratic residue of p.

5. Show that

$$\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) = 0.$$

6. If $p = 8k+7$ and $4k+3$ are both primes, show that -2 is a quadratic residue of p.

7. Prove that there are infinitely many primes of the form $6k+1$.

8. Prove that there are infinitely many primes of the form $8k+3$.

9. Determine all primes such that $\left(\frac{6}{p}\right) = 1$.

10. Determine all primes such that $\left(\frac{5}{p}\right) = -1$.

11. Show that the sum of all the quadratic residues of a prime $p > 3$ is divisible by p. What can you say about the sum of the non-residues?

12. Show that the product of all the quadratic residues of an odd prime p is congruent to either 1 or -1 according as $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$. What can you say about the product of the non-residues?

13. Determine whether the following quadratic congruences have a solution or not:

    (A) $x^2 \equiv 2 \bmod 71$

(B) $x^2 \equiv -2 \bmod 71$

(C) $x^2 \equiv 2 \bmod 73$

(D) $x^2 \equiv -2 \bmod 73$

14. Let p and q be twin primes. Show that $x^2 \equiv p \bmod q$ has a solution if and only if $x^2 \equiv p \bmod q$ has a solution.

15. Let p be an odd prime. Show that the product of two quadratic non-residues modulo p is a quadratic residue modulo p. Then show with an example that this need not hold for a composite number.

16. Show that a quadratic residue of an odd prime can not be a primitive root.

17. Count the number of solutions for the following congruences:

$$\begin{array}{llll} (i) & x^2 \equiv -1 \bmod 79 & (ii) & x^2 \equiv -1 \bmod 158 \\ (iii) & x^2 \equiv -2 \bmod 79 & (iv) & x^2 \equiv -2 \bmod 158 \\ (v) & x^2 \equiv -2 \bmod 205 & (vi) & x^2 \equiv 2 \bmod 205 \end{array}$$

18. Let n be a natural number not divisible by an odd prime p. Show that

$$\sum_{a=1}^{p-1} \Big(\frac{a(a+n)}{p}\Big) = -1.$$

19. Use Jacobi symbol to show that 2 is not a quadratic residue of 21, 85 and 123.

Module 6

Binary Quadratic Forms

6.1 Lecture 1

Preamble:: In this lecture, we will introduce binary quadratic forms. A binary quadratic form is a homogenous polynomial of degree 2 with integer coefficients. We will investigate which integers can be represented by such a form as x and y range over the set of integers.

Keywords: binary quadratic forms, unimodular substitution, equivalent forms

6.1.1 Definition and Examples

One of the simplest example of a binary quadratic form is $x^2 + y^2$. A form of degree d in n-variables over $\mathbb{Z}$ is a polynomial each of whose terms is of degree d with coefficients in $\mathbb{Z}$. A form of degree 2 is called a quadratic form. A quadratic form in two variables is called a binary quadratic form. Thus,

Definition 6.1. *A binary quadratic form is a homogenous polynomial of the second degree in two variables with integer coefficients, i.e.,*

$$q(x, y) = ax^2 + bxy + cy^2, \qquad a,\ b,\ c \in \mathbb{Z}.$$

For convenience, we will denote a binary quadratic form $ax^2 + bxy + cy^2$ by the ordered triple (a, b, c). Another useful observation is the fact that

$$q(x, y) = ax^2 + bxy + cy^2 = \begin{pmatrix} x \\ y \end{pmatrix}^t \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

where B^t denotes the transpose of a matrix B. We will denote the unique matrix

$$\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$$

associated with the quadratic form $q(x, y)$ by M_q. Given a form $ax^2 + bxy + cy^2$, an interesting question is to determine the set of integers it represents as x and y run over the set of integers.

6.1.2 Unimodular substitution

It is easy to see that the form $2x^2 + 5y^2$ will represent the same set of integers as the form $5x^2 + 2y^2$, and though it may be less obvious, the binary quadratic form $8x^2 + 6xy + 3y^2$ will represent the same set of integers as the form $3X^2 + 5Y^2$. Observe that $8x^2 + 6xy + 3y^2 = 5x^2 + 3(x + y)^2$, and as x, y run over the set of all integers, so do x and $x + y$. These two forms are related by a substitution $X = x$ and $Y = x + y$. This substitution takes a pair of integers to a pair of integers and is invertible, namely, $x = X,\ \ y = Y - X$. We will now examine all such substitutions.

Let us consider the substitution

$$X = px + qy, \qquad Y = rx + sy,$$

and assume that there is a one-to-one correspondence between integer pairs $x,\ y$ and $X,\ Y$. Clearly, $p,\ q,\ r$ and s have to be integers:

$$\begin{aligned} x = 1,\ y = 0 \quad &\Longrightarrow \quad X = p\ \ Y = r \\ x = 0,\ y = 1 \quad &\Longrightarrow \quad X = q\ \ Y = s. \end{aligned}$$

If Δ denotes $ps - qr$, then observe that

$$x = \frac{s}{\Delta}X - \frac{q}{\Delta}Y, \quad y = -\frac{r}{\Delta}X + \frac{p}{\Delta}Y.$$

If $x,\ y$ are integers for any integer pairs $X,\ Y$, we must have

$$\begin{aligned} \frac{s}{\Delta}, \frac{q}{\Delta}, \frac{r}{\Delta}, \frac{p}{\Delta} &\in \mathbb{Z} \\ \Longrightarrow \frac{s}{\Delta}\frac{p}{\Delta} - \frac{q}{\Delta}\frac{r}{\Delta} &\in \mathbb{Z} \\ \Longrightarrow \frac{\Delta}{\Delta^2} &\in \mathbb{Z} \\ \Longrightarrow \Delta &= \pm 1. \end{aligned}$$

Conversely, if $\Delta = \pm 1$, we will clearly have the one-to-one correspondence between integers pairs (x, y) and (X, Y).

It leads to a more fruitful theory if we consider substitution of the form

$$X = px + qy, \qquad Y = rx + sy \qquad \text{with} \qquad \Delta = ps - qr = 1.$$

Such a substitution will be called a *unimodular substitution.* For example,

$$X = x, \qquad Y = x + y$$

is a unimodular substitution. A unimodular substitution is given by an integer matrix

$$U = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

of determinant 1, and the substitution can be expressed as

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

It is clear from the above discussion that

COROLLARY 6.2. *A unimodular substitution is invertible and the inverse substitution is also unimodular.*

PROPOSITION 6.3. *A unimodular substitution takes a pair of relatively prime integers x, y to a relatively prime pair of integers X, Y.*

Proof: Any common divisor d of X and Y will be a common divisor of $x,\ y$ as x and y are integral combinations of X and Y given by the inverse of the unimodular substitution.

6.1.3 Equivalent Forms

DEFINITION 6.4. *Two binary quadratic forms are called equivalent if one can be obtained from the other by a unimodular substitution of the variables*

For example, the forms $g(x, y) = x^2 + 3y^2$ and $h(x, y) = 5x^2 + 26xy + 34y^2$ are equivalent, as the the unimodular substitution $X = 2x + 5y,\ Y = x + 3y$ yields

$$5x^2 + 26xy + 34y^2 = (2x + 5y)^2 + (x + 3y)^2 = X^2 + 5Y^2.$$

If the form $ax^2 + bxy + cy^2$ is equivalent to $\alpha x^2 + \beta xy + \gamma y^2$, we denote it by

$$(a, b, c) \sim (\alpha, \beta, \gamma).$$

PROPOSITION 6.5. *If $f(x,y)$ and $g(x,y)$ are equivalent quadratic forms through the unimodular substitution represented by a matrix U taking f to g, then*

$$M_g = U^t M_f U,$$

where M_g and M_f are the matrices associated with f and g respectively.

Proof:

$$\begin{aligned} g(x,y) &= \left[U\begin{pmatrix}x\\y\end{pmatrix}\right]^t M_g U\begin{pmatrix}x\\y\end{pmatrix} \\ \implies \begin{pmatrix}x\\y\end{pmatrix}^t M_g \begin{pmatrix}x\\y\end{pmatrix} &= \begin{pmatrix}x\\y\end{pmatrix}^t U^t M_g U\begin{pmatrix}x\\y\end{pmatrix} \qquad \forall x,y \\ \implies M_g &= U^t M_g U. \qquad \square \end{aligned}$$

PROPOSITION 6.6. *The relation $\sim$ on the set of all binary quadratic forms is an equivalence relation.*

Proof: We will show that the relation $\sim$ is reflexive, symmetric and transitive.

1. Clearly, $\sim$ is reflexive as $(a,b,c) \sim (a,b,c)$ by the unimodular substitution $X = x$, $Y = y$.
2. Secondly, $(a,b,c) \sim (\alpha,\beta,\gamma) \implies (\alpha,\beta,\gamma) \sim (a,b,c)$ as the inverse of a unimodular substitution is also unimodular: if the integer matrix $U = \begin{pmatrix}p & q\\ r & s\end{pmatrix}$ is of determinant 1, its inverse also has integer entries and is of determinant 1.
3. If $(a,b,c) \sim (\alpha,\beta,\gamma)$ and $(\alpha,\beta,\gamma) \sim (a',b',c')$, with the unimodular substitutions given by the matrices A and B respectively, then it is easy to check that the matrix AB has integer entries, is of determinant 1, and the unimodular substitution corresponding to the matrix AB yields $(a,b,c) \sim (a',b',c')$. $\square$

6.1.4 Proper Representation

DEFINITION 6.7. *An integer n is said to be properly represented by a quadratic form $ax^2 + bxy + cy^2$ if there exists a pair of relatively prime integers k and l such that $n = al^2 + bkl + cl^2$.*

For example, 65 is properly represented by the form $2x^2 + 5xy + 3y^2$ with $x = 2$ and $y = 3$. Once we know determine the set of integers S properly represented by a given

form, we can determine the set of all integers represented by the form as any such integer will be a square times some element of S.

We have seen that a unimodular substitution takes a pair of relatively prime integers x, y to a relatively prime pair of integers X, Y. Hence we have the following proposition.

PROPOSITION 6.8. *Two equivalent quadratic forms properly represent the same set of integers.*

6.2 Lecture 2

Preamble: In this lecture, we will discuss discuss an important invariant associated with an equivalence class of quadratic forms. This invariant is called the discriminant, and is crucial to our understanding of a quadratic form, in particular, in the study of its range.

Keywords: discriminant, principal forms, definite and indefinite forms

6.2.1 Discriminant of a Quadratic Form

DEFINITION 6.9. *The discriminant of a quadratic form $q(x,y) = ax^2 + bxy + cy^2$ is defined as the integer*

$$d_q = b^2 - 4ac.$$

For example, the discriminant of $3x^2+5xy+2y^2$ is $5^2-4.3.2 = 1$. Recall that a quadratic form $h(x,y) = ax^2 + bxy + cy^2$ can be expressed as

$$h(x,y) = \begin{pmatrix} x \\ y \end{pmatrix}^t \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}^t M_q \begin{pmatrix} x \\ y \end{pmatrix}.$$

Then, the discriminant of the quadratic from $h(x,y)$ is nothing but the $4\det(M_h)$.

PROPOSITION 6.10. *Equivalent forms have the same discriminant.*

Proof: If the two form $g(x,y)$ and $h(x,y)$ are equivalent, then there is a matrix U with integer entries of determinant 1 corresponding to the unimodular substitution taking h to g. Then, the matrices of g and h are are related by

$$\begin{aligned} M_g &= U^t M_h U \\ \implies d_g &= 4\det M_g \\ &= 4\det(U^t M_h U) \\ &= 4\det(U^t)\det(M_h)\det(U) \\ &= 4\det(M_h) = d_h. \qquad \square \end{aligned}$$

However, the converse is not true. Two inequivalent forms may have still the same discriminant. For example, the forms $6x^2 + y^2$ and $5x^2 + 4xy + 2y^2$ both have discriminant -24, but the latter forms properly represents 5 (with $x = 1,\ y = 0$), whereas the former

can not represent 5. Hence these two forms must be inequivalent.

PROPOSITION 6.11. *An integer d is the discriminant of a quadratic form if and only if $d \equiv 0$ or 1 mod 4.*

Proof: If d is the discriminant of (a, b, c), then

$$\begin{aligned} d = b^2 - 4ac \quad &\implies \quad d \equiv b^2 \bmod 4 \\ &\implies \quad d \equiv 0 \text{ or } 1 \bmod 4. \end{aligned}$$

If $d \equiv 4$, we clearly have a quadratic form $x^2 - \frac{d}{4}y^2$ of discriminant d. If $d \equiv 1 \bmod 4$, we have a quadratic form $x^2 + xy + \frac{1-d}{4}y^2$ of discriminant d. □

DEFINITION 6.12. *When $d \equiv 0$ mod 4, the form $x^2 - \frac{d}{4}y^2$ is called the principal form of discriminant d. When $d \equiv 1$ mod 4, the form $x^2 - \frac{d}{4}y^2$ is called the principal form of discriminant d.*

6.2.2 Definite and Indefinite Forms

DEFINITION 6.13. *A quadratic from $q(x, y)$ is called* **definite** *if it takes only positive or only negative values for $(x, y) \neq (0, 0)$. In the former case, $q(x, y)$ is called* **positive definite**, *and in the latter case $q(x, y)$ is called* **negative definite**. *The form is called* **positive semidefinite** *if $q(x, y) \geq 0$ for all x, y, and is called* **negative semidefinite** *if if $q(x, y) \leq 0$ for all x, y. A form $q(x, y)$ is called* **indefinite** *if takes both positive and negative values.*

It is obvious that we can convert a negative definite form to a positive definite form by changing each coefficient to its negative. Hence the negative definite forms need not be studies separately once we study the positive definite forms.

Consider the quadratic form $q(x, y) = ax^2 + bxy + cy^2$ with discriminant d. We can write

$$4aq(x, y) = (4a^2x^2 + 4ax.by + b^2y^2) - (b^2 - 4ac)y^2 = (2ax + by)^2 - dy^2.$$

1. If $d < 0$, it is clear that $4aq(x, y)$ always takes only positive values for any choice of x and y in integers other than $(x, y) \neq (0, 0)$.

   (A) If $d < 0$ and $a > 0$, then $q(x, y)$ always takes positive values for $(x, y) \neq (0, 0)$, and the form is *positive definite*.

(B) If $d < 0$ and $a < 0$, $q(x, y)$ always takes negative values for $(x, y) \neq (0, 0)$ and it is *negative definite*.

2. Now suppose $d > 0$. Then

$$q(1, 0) = a, \qquad q(b, -2a) = a(b^2 - 2b^2 + 4ac) = -ad.$$

(A) If $a \neq 0$, these two numbers are of opposite signs, and hence it is an *indefinite* form.

(B) If $a = 0$, then consider

$$q(0, 1) = c, \qquad q(-2c, b) = -cd.$$

They are of opposite signs unless $c = 0$. If $a = 0 = c$, then $q(x, y) = bxy$, and

$$q(1, 1) = b, \qquad q(1, -1) = -b.$$

Hence we can conclude that $q(x, y)$ is an *indefinite* form if $d < 0$.

3. If $d = 0$, then

$$4aq(x, y) = (2ax + by)^2.$$

If $a \neq 0$, then all the non-zero values of $q(x, y)$ are of the same sign, hence it is *semi-definite*. As

$$f(b, -2a) = -ad = 0,$$

$q(x, y)$ is not a definite form. If $d = 0$, $a = 0$ we must have $b = 0$, and $q(x, y) = cy^2$, and its non-zero values have same sign. Hence the form is *semidefinite*. As $q(1, 0) = 0$, the form is not definite in this case.

Thus, we have seen that the discriminant tells us completely whether a form is semidefinite, definite or indefinite.

6.3 Lecture 3

Preamble: In this lecture, we will describe a criterion for an integer to be properly represented by a given form. The we will introduce the reduced forms.

Keywords: proper representation, equivalent forms, reduced forms

6.3.1 Proper Representation and Equivalent Forms

Assume that n is a non-zero integer. Recall that a number n is said to be *properly represented* by a form (a, b, c) if there exist two relatively prime integers r and s such that $n = ar^2 + brs + cs^2$. We will now see that the question of proper representation of n by (a, b, c) can be reduced to a question about existence of a form (n, β, γ) (with n as the first coefficient) equivalent to (a, b, c):

PROPOSITION 6.14. *An integer n can be properly represented by (a, b, c) if and only if there exists a form (n, β, γ) with the first coefficient n which is equivalent to (a, b, c)*

Proof: If (n, β, γ) is equivalent to (a, b, c), they properly represent the same set of integers as we saw at the end of the previous lecture. But n is clearly properly represented by (n, β, γ) with $x = 1,\ y = 0$, hence n is properly represented by (a, b, c) as well.

Conversely, let $n = ap^2 + bpr + cr^2$ for relatively prime integers r and p. Then we have integers s and q such that $ps - rq = 1$. The substitution

$$X = px + qy, \quad Y = rx + sy$$

is unimodular, and it gives the equivalent form

$$\begin{aligned} & a(px + qy)^2 + b(px + qy)(rx + sy) + c(rx + sy)^2 \\ = \ & (ap^2 + bpr + cr^2)x^2 + (aq^2 + bqs + cs^2)y^2 + (b(ps + qr) + 2apq + 2crs)xy, \\ = \ & nx^2 + [b(ps + qr) + 2apq + 2crs]xy + (aq^2 + bqs + cs^2)y^2. \qquad \square \end{aligned}$$

PROPOSITION 6.15. *A non-zero integer n can be properly represented by a form of discriminant d if and only if the quadratic congruence*

$$\alpha^2 = d \ mod \ 4|n|$$

has a solution.

Proof: If n is properly represented by a form (a, b, c) of discriminant d, then there is a form (n, α, β) (for some integers α and β) which is equivalent to (a, b, c). As equivalent forms have the same discriminant, we must have $\alpha^2 - 4n\beta = d$. In other words, the congruence $\alpha^2 = d$ modulo $4|n|$ has a solution.

Conversely, suppose the congruence $\alpha^2 = d$ modulo $4|n|$ has a solution α_0, say $\alpha_0^2 - 4n\beta_0 = d$. Then the form (n, α_0, β_0) has discriminant $\alpha_0^2 - 4n\beta_0 = d$, and it represents n properly. □

The following proposition often helps us in determining whether a given integer n can be represented by a form of discriminant d.

PROPOSITION 6.16. *A non-zero integer n can be properly represented by a form of discriminant d if and only if $\alpha^2 = d$ modulo $4|n|$ has a solution for some $0 \leq \alpha < 2|n|$.*

Proof: If n is represented by a quadratic from of discriminant d, we know that there exists a form (n, α, β) of discriminant d. The substitution $X = x + uy$, $Y = y$ is unimodular for any integer u. Using this substitution, we find that n is also properly represented by $nx^2 + (\alpha + 2nu)xy + (nu^2 + \alpha\beta u + \beta)y^2$ [as in the proof of proposition 3.1], with the new middle coefficient being $\alpha + 2nu$. By a suitable choice of u, we can now find an equivalent form (n, α_0, β_0) with α_0 satisfying $0 \leq \alpha_0 < 2|n|$. □

6.3.2 Reduction of Binary Quadratic Forms

DEFINITION 6.17. *Let $q(x, y) = ax^2 + bxy + cy^2$ be a binary quadratic form whose discriminant d is a not a square. Then $q(x, y)$ is called a reduced form if*

1. $-|a| < b \leq |a| < |c|$, *or*
2. $0 \leq b \leq |a| = |c|$.

If $q(x, y) = ax^2 + bxy + cy^2$ is positive definite, we have $d < 0$ and $a > 0$ as well. So $q(x, y)$ will be a reduced form if

1. $-a < b \leq a < c$ or
2. $0 \leq b \leq a = c$.

For example, $-2x^2+xy+3y^2$ is a reduced form, and $3x^2+5xy+6y^2$ is not a reduced form.

THEOREM 6.18. *Any binary quadratic form whose discriminant is not a square is equivalent to some reduced form.*

Proof: Let $q(x,y) = ax^2 + bxy + cy^2$ be a positive definite quadratic form with discriminant $d = b^2 - 4ac$. As d is not a square, $a \neq 0$ implies $c \neq 0$. (i) If $\mid a \mid > \mid c \mid$ or $\mid a \mid = \mid c \mid$ and $\mid a \mid \leq b < 0$, then one can use the unimodular substitution $X = y$ and $Y = -x$ to obtain an equivalent form $cx^2 - bxy + ay^2$. Note that this substitution does not affect the absolute value of the second coefficient $|b|$.
(ii) If $|b| > a$, one can use the substitution $X = x + uy$, $Y = y$ to obtain

$$(a, b, c) \sim (a, b + 2ua, c + bu + au^2).$$

By choosing u appropriately, we have

$$|b + 2ua| \leq a.$$

Note that this substitution does not affect the first coefficient.

By performing the above two steps as many times as necessary, we can find (a, b, c) where $a \leq c$ and $|b| \leq a$ and is equivalent to $q(x, y)$. □

For example, consider the form $q(x,y) = 5x^2 + 3xy + 2y^2$. We have $(5, 3, 2) \sim (2, -3, 5)$. Now, we need to pick an integer u such that $|-3 + 2u.2| \leq 2$. Clearly, $u = 1$ will satisfy the inequality. Hence,

$$(2, -3, 5) \sim (2, -3 + 2.1.2, 5 + (-3)1. + 2.1^2) = (2, 1, 4).$$

Having known the first two coefficients of the equivalent form, we can find the third coefficient also from the discriminant:

$$-3^2 - 4.5.2 = 1^2 - 4.2.c \implies c = 4.$$

6.3.3 Reduced Forms of a Given Discriminant

THEOREM 6.19. *There are only finitely many reduced forms of any given discriminant d which is not a perfect square.*

Proof: Let (a, b, c) be a reduced form of discriminant d. We have $\mid a \mid \leq \mid c \mid$ and $-\mid a \mid b \leq \mid a \mid a$. Now, if $d < 0$ then a and c are of the same sign, and

$$\begin{aligned} d &= b^2 - 4ac = b^2 - 4 \mid a \mid \mid c \mid \leq a^2 - 4a^2 < 0, \\ &\Longrightarrow \mid a \mid \leq \sqrt{\frac{-d}{3}}. \end{aligned}$$

If $d > 0$, then a and c are of opposite signs, and

$$\begin{aligned} d &= b^2 - 4ac = b^2 + 4 \mid a \mid\mid c \mid \geq 4 \mid a \mid^2 . \\ &\Longrightarrow \mid a \mid \leq \frac{\sqrt{d}}{2}. \end{aligned}$$

Thus we have a bound for $\mid a \mid$ in terms of d in both the cases. Hence, there are only finitely many choices for a and the number of integers b such that $|b| \leq a$ is also finite. Given d, a and b, $d = b^2 - 4ac$ is satisfied by only finitely many integers c. □

Example: Find all the reduced forms of discriminant -19.

Solution: If (a, b, c) is a reduced form of discriminant -19, then

$$\begin{aligned} & 4ac - b^2 = 19, \ \ 0 < a \leq c, \ |b| \leq a, \\ \Longrightarrow \qquad & 4a^2 - a^2 \leq 19 \implies a = 1, \ 2. \end{aligned}$$

For $a = 1$, we have $|b| \leq 1$, hence $b = 0$ or $b = \pm 1$. Now, $-19 = b^2 - 4c$ can not have a integral solution for c if $b = 0$. Hence $b = \pm 1$, which yields

$$4c = (-1)^2 + 19 = 20 \implies c = 5.$$

Now $a < c$, hence we see that $(1, -1, 5) \sim (1, 1, 5)$ by the substitution $X = x + uy, Y = y$, where $\mid -1 + 2.u.1 \mid \leq 1$, i.e., $u = 1$. Now consider $a = 2$. Then $|b| \leq 2$, and $b = 0, \pm 1$ or ± 2. But then, $-19 = b^2 - 8c$ has no solution in integers for c. Hence there is only one reduced form of discriminant -19, and that is $x^2 + xy + 5y^2$.

6.4 Lecture 4

Preamble: In this lecture, we will show that each equivalence class of positive definite forms has a unique representative by a reduced form.

Keywords: reduced forms

6.4.1 Uniqueness of Equivalent Reduced Form

We will now show that each equivalence class of positive definite quadratic forms has exactly one reduced form. Recall that equivalent forms properly represent the same set of integers. We will first show that the first and the third coefficient of a reduced form in an equivalence class are uniquely determined by the set of integers properly represented by those equivalent forms. Then we will show that the middle coefficient of the reduced forms is also uniquely determined, so that each equivalence class can not have more than one reduced form.

PROPOSITION 6.20. *Let $f(x,y) = ax^2 + bxy + cy^2$ be a reduced form of discriminant $d < 0$, and S be the set of integers properly represented by f.*

1. *Then, a is the smallest integer in S.*
2. *If $c > a$, then c is the smallest integer in $S - \{a\}$.*
3. *Moreover, the number of proper representations of the integer a by f is*
   - *(A) 2 if $a < c$ (given by $f(\pm 1, 0) = a$)*
   - *(B) 4 if $0 \leq b < a = c$ (given by $f(\pm 1, 0) = f(0, \pm 1) = a$)*
   - *(C) 6 if $a = b = c$ (given by $f(\pm 1, 0) = f(0, \pm 1) = f(1, -1) = f(-1, 1) = a$).*

Proof: As $ax^2 + bxy + cy^2$ is reduced, we have

$$0 < a \leq c, \qquad |b| \leq a.$$

Clearly, $a,\ c \in S$. Let m and n be any two coprime integers such that $f(m,n) \leq c$. We claim that

$$|n|,\ |m| < 2, \qquad f(m,n) = a, \qquad f(m,n) = c.$$

Recall that

$$4af(x,y) = (2ax+by)^2 - dy^2.$$

$$\begin{aligned} |n| \geq 2 \quad &\implies 4af(m,n) \quad \geq -dn^2 \geq -4d = 16ac - 4b^2 \\ &\qquad\qquad\quad > 8ac - 4b^2 \geq 4ac + 4a^2 - 4b^2 \\ &\implies 4af(m,n) \quad > 4ac \\ &\implies f(m,n) \quad > c \qquad \forall m \end{aligned}$$

If $n = \pm 1$, then $|m| \geq 2$ would imply

$$|2am + bn| \geq |2am| - |bn| \geq 4a - |b| \geq 3a,$$

hence

$$4af(m,n) = (2am+bn)^2 - dn^2 \geq 9a^2 - b^2 + 4ac > a^2 - b^2 + 4ac \geq 4ac,$$

so that

$$f(m,n) > c.$$

Hence $f(m,n) \leq c$ and $n = \pm 1$ implies $|m| \leq 1$.

If $n = 0$, then $gcd(m,n) = 1$ forces $m = \pm 1$.

Hence if $f(m,n) \leq c$ and $gcd(m,n) = 1$, then (m,n) must be one of the six pairs $(\pm 1, 0)$, $(0, \pm 1)$, $(1,-1)$, $(-1,1)$. If $a < c$, then a can be properly represented by only the first two points. If $a = c$, and $0 \leq b < a$, then a can be properly represented exactly by the first four points. If $a = c = b$, all six points properly represent a. □

THEOREM 6.21. *Each binary quadratic form is equivalent to exactly one reduced form. In other words, if $f(x,y) = ax^2 + bxy + cy^2$ and $g(x,y) = Ax^2 + Bxy + Cy^2$ are both reduced forms, then $g \sim h$ implies $a = A$, $b = B$, $c = C$.*

Proof: The two equivalent forms $g(x,y)$ and $h(x,y)$ properly represent the same set S of integers. By the previous proposition, a is the least element of S, and so is A. Hence $a = A$.

Now suppose $a = c$. Then a has four proper representations by f, and hence A has four proper representations by g. So, $C = A$. For the reduced form f and g, we have

$0 \leq b \leq a$ and $0 \leq B \leq A$. But $B^2 - 4AC = b^2 - 4ac$ because equivalent forms have same discriminant. Hence $b^2 = B^2$, and both b and B are non-negative. It follows that $b = B$.

Now suppose $a < c$. As before $a = A$. Now a can be properly represented by f in precisely two ways, and hence $A = a$ can be represented in precisely two ways by the equivalent form g. By the previous proposition, it follows that $A < C$. By the same proposition, c is the smallest element of $S - \{a\}$, and C is the smallest element of $S - \{A\} = S - \{a\}$. Hence $c = C$. It only remains to show that $B = b$. Consider the matrix $M = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ taking f to g. Then, $ps - qr = 1$ and $gcd(p, r) = 1 = gcd(q, s)$. Now, $A = ap^2 + bpr + cr^2$ (see proposition 3.1 in the previous lecture), giving us a proper representation of $A = a$ by (p, r). Hence $(p, r) = (\pm 1, 0)$ by the previous proposition. Similarly $C = aq^2 + bqs + cs^2$, hence $c = C$ is properly represented by (q, s). Hence $(q, s) = (0, \pm 1)$. This limits the choice of M to either I or $-I$. In either case,

$$B = 2apr + b(ps + qr) + 2cqs = bps = b,$$

and we get the desired result. $\square$

6.5 Lecure 5

Preamble: In this lecture, we will show that there are only finitely many equivalence classes of positive definite quadratic forms of any given discriminant d. The number of equivalence classes of same discriminant d will be called the class-number of d.

Keywords: reduced forms, class number

6.5.1 Class Number

Let d be an integer. If $d \equiv 0, 1 \bmod 4$, we know that there is a quadratic form of discriminant d. If $d < 0$, the principal form of discriminant d is positive definite. It is clear that that there will be infinitely many positive definite quadratic forms of discriminant d, for example, the ones obtained from the principal form by unimodular substitutions. But all such positive definite forms belong to a finitely many equivalence classes. In other words, there will be only finitely many inequivalent positive definite forms of a given discriminant.

THEOREM 6.22. *Let $d \equiv 0, 1$ mod 4 be a negative integer. Then there are only finitely many inequivalent positive definite quadratic forms of discriminant d.*

Proof: We know that each equivalence class of a positive definite quadratic form contains a reduced form, and each class can not have more than one reduced forms. Hence it is enough to show that there are only finitely many reduced forms of discriminant d. But we have proved that already in previous lectures of this module. □

DEFINITION 6.23. *The number of inequivalent positive definite quadratic forms of discriminant d is called the class number of d. We denote it by $C(d)$*

Example: Consider $d = -3$. As $-3 \equiv 1 \bmod 4$, there will be at least one positive definite form of discriminant -3. If (a, b, c) is a reduced form of discriminant -3, we must have

$$\begin{aligned} & b^2 - 4ac = -3, && |b| \leq a \leq c \\ \implies \quad & -3 = b^2 - 4ac && \leq a^2 - 4a^2 \\ \implies \quad & a^2 && \leq 1 \\ \implies \quad & a = 1, && b = -1,\ 0 \text{ or } 1. \end{aligned}$$

Now, $4c = b^2 + 3$ will have a solution only if $b = \pm 1$, in which case $c = 1$. Now if $a = c$ for a reduced form, $0 \leq b \leq a$, hence $b = 1$. Thus, there is only one reduced form of discriminant -3, which is $x^2 + xy + y^2$, and $C(-3) = 1$.

Gauss conjectured that $C(d)$ approaches infinity as d approached $-\infty$. Much later, it was proved by Heilbronn in 1934. There is an interesting formula for the class number of d, and the formula is simplest to express when $d = -p$, where p is a prime number. Note that p has to be of the form $4k + 3$ as $d \equiv 0, 1 \bmod 4$. We further assume that $p > 3$. Let A be the sum of all the quadratic residues modulo p, and B be the sum of quadratic non-residues modulo p. Then,

$$C(-p) = \frac{B - A}{p}.$$

For example, consider $d = -7$ for the prime $7 \equiv 3 \bmod 4$. The quadratic residues modulo 7 are $(\pm)^1 = 1, (\pm 2)^2 = 4$ and $(\pm 3)^2 = 2$. The quadratic residues add up to $A = 7$. The quadratic non-residues of 7 add up to $B = 3 + 5 + 6 = 14$. Hence $C(-7)$ should be 1. We next verify this directly by computing the number of reduced forms of discriminant -7 as follows.

If (a, b, c) is a reduced form of discriminant -7, then $|b| \leq a \leq c$ and

$$\begin{aligned} -7 = b^2 - 4ac &\leq a^2 - 4a^2 \\ \implies a^2 &\leq 1, \\ \implies a &= 1 \\ \implies |b| &\leq a \\ \implies b &= 0 \text{ or } \pm 1. \end{aligned}$$

But $-7 = b^2 - 4c$ will have a solution in integers for c only if $b = \pm 1$, and then $c = 2$. As $a < c$, we can choose b in $-a < b \leq a$, and hence $b = 1$. Thus, there is only one reduced form of discriminant -7 and that is $x^2 + xy + 2y^2$.

The above formula for class number was discovered by Jacobi, and proved later by Dirichlet. This formula is part of what is known as Dirichlet's class number formula.

6.6 Exercises

1. Classify the following quadratic forms as positive definite, negative definite or indefinite

$$(i)\ \ 3x^2 - 5y^2 \qquad (ii)\ \ 3x^2 + 5y^2$$
$$(iii)\ \ x^2 - xy + y^2 \quad (iv)\ \ x^2 - 3xy + y^2$$

2. Find the reduced form equivalent to

$$22x^2 - 20xy + 5y^2.$$

3. Determine all the reduced forms of discriminant -20. Hence deduce the class number of -20.

4. Characterize all the integers that can be represented by a quadratic form of discriminant -20.

5. Determine whether the following pairs of quadratic forms are equivalent:

   (A) $3x^2 + 5xy + 4y^2$ and $6x^2 - xy + y^2$.

   (B) $17x^2 - 7xy + y^2$ and $35x^2 - 11xy + y^2$.

   (C) $2x^2 - 9xy + 11y^2$ and $2x^2 - 5xy + 4y^2$.

6. Characterize all primes that can be expressed as $x^2 + y^2$.

7. Determine whether the primes 97 and 101 can represented by the form $x^2 - xy + 3y^2$.

8. Determine whether the primes 41 and 43 can be represented by $q(x, y) = 13x^2 + 7xy + y^2$. Characterize all primes which can be represented by $q(x, y)$.

9. Show that an odd prime p can be represented by the form $x^2 + 2y^2$ if and only if p is of the form $8k + 1$ or $8k + 3$.

10. Show that an odd prime p can be represented by the form $x^2 - 2y^2$ if and only if p is of the form $8k \pm 1$.

11. Determine all the reduced forms of discriminant -23, and deduce that the class number of -23 is 3.

Module 7

Integers of Special Form

7.1 Lecture 1

Preamble: In this lecture, we will introduce Fermat numbers and Mersenne numbers. All Fermat numbers were thought to be prime, but hat turned out to be incorrect.

Keywords: Fermat numbers, Fermat primes, Mersenne numbers, Mersenne primes

7.1.1 Fermat Primes

For any non-negative integer n, consider the natural number

$$F_n = 2^{2^n} + 1.$$

Observe that

$$\begin{aligned} F_0 &= 3, \\ F_1 &= 5, \\ F_2 &= 17, \\ F_3 &= 257, \\ F_5 &= 65537 \end{aligned}$$

are prime numbers. This observation led Fermat to conjecture that F_n is prime for any $n \geq 0$. However, Euler showed that

$$F_5 = 2^{2^5} + 1 = 641 \times 6700417.$$

DEFINITION 7.1. *The numbers $F_n = 2^{2^n} + 1$ are called Fermat numbers and in particular, a prime of the form $F_n = 2^{2^n} + 1$ are called Fermat primes.*

Though a large number of Fermat numbers are calculated, all others except the first 5 are found to be composite. However, it is still an open question whether there are any other Fermat prime. In fact, it is still a possibility that there may be infinitely many Fermat primes. The Fermat primes have a geometric significance as discovered by Gauss in 1801. Gauss showed that a regular polygon with n sides can be constructed by ruler-and-compass methods of and only if $n = 2^e p_1 \cdots .p_k$ where $p_1, \cdots, p_k$ are Fermat primes.

While it is still not known whether there exist infinitely many Fermat primes, one can easily show that that factors of Fermat numbers give infinitely many distinct primes.

PROPOSITION 7.2. *Any two distinct Fermat numbers are relatively prime.*

Proof: Consider tow Fermat numbers F_n and F_{n+k} where $k \in \mathbb{N}$. Observe that

$$\begin{aligned} F_0.F_1.\cdots.F_{n+k-1} &= \left[\left(2^{2^0}-1\right)\left(2^{2^0}+1\right)\right]\left(2^{2^1}+1\right)\cdots\left(2^{2^{n+k-1}}+1\right) \\ &= \left[\left(2^{2^1}-1\right)\left(2^{2^1}+1\right)\right]\cdots\left(2^{2^{n+k-1}}+1\right) \\ &\vdots \quad \vdots \\ &= \left(2^{2^{n+k-1}}\right)^2 - (1)^2 \\ &= F_{n+k} - 2. \end{aligned}$$

Let, if possible, p be a prime that divides both F_n and F_{n+k}. Then

$$p \mid \left(F_{n+k} - F_0.F_1.\cdots.F_{n+k-1}\right) \implies p = 2.$$

But then F_n must be even, which clearly is not true. Hence, these numbers must be coprime. □

7.1.2 Mersenne Primes

PROPOSITION 7.3. *If $m > 1$ and $a^m - 1$ is prime, then $a = 2$ and m is prime.*

Proof: If $m = kl$, then clearly $a^k - 1$ and $a^l - 1$ are factors of $a^m - 1$. Moreover, if $a = b + 1$ then b is a factor of

$$a^m - 1 = (b+1)^m - 1 = b(b^{m-1} + \cdots + 1).$$

Therefore, if $a^m - 1$ is a prime, then m must be prime and a must be 2. □

DEFINITION 7.4. *Integers of the form $2^p - 1$ are called Mersenne numbers. A Mersenne number which is also a prime is called Mersenne prime.*

For example, 3, 7, 31 etc are Mersenne primes. Mersenne studies these numbers in 1644. Note that

$$M_{11} = 2047 = 23 \times 89,$$

so there are Mersenne numbers which are not prime. In fact, only 35 Mersenne primes have been found so far. It is still an open question whether there exist infinitely many Mersenne primes. Distinct Mersenne numbers can be shown to be pair-wise co-prime, so we can show infinitude of prime numbers using Mersenne numbers as well.

PROPOSITION 7.5. *Any two distinct Mersenne numbers are coprime.*

Proof: Let p and q be two distinct primes, say $q > p$. If we apply Euclid's algorithm to obtain the gcd of p and q which must be 1, then

$$\begin{aligned} q &= pk_1 + r_1, \\ p &= r_1k_2 + r_2, \\ &\vdots \quad\quad \vdots \\ r_{n-2} &= r_{n-1}k_{n-1} + r_n \\ &= r_{n-1}k_{n-1} + 1. \end{aligned}$$

Suppose l is a common divisor of $M_p = 2^p - 1$ and $M_q = 2^q - 1$. But

$$\begin{aligned} & l \mid \big(2^p - 1\big),\ l \mid \big(2^q - 1\big) \\ \Longrightarrow\ & l \mid \big[(2^q - 1) - 2^{q-p}(2^p - 1)\big] \\ \Longrightarrow\ & l \mid \big(2^{q-p} - 1\big). \\ \Longrightarrow\ & l \mid \big[(2^{q-p} - 1) - 2^{q-2p}(2^p - 1)\big]. \\ \Longrightarrow\ & l \mid \big(2^{q-2p} - 1\big) \\ & \vdots \quad\quad \vdots \\ \Longrightarrow\ & l \mid \big(2^{q-kp} - 1\big) \\ \Longrightarrow\ & l \mid 2^{r_1} - 1 \\ & \vdots \quad\quad \vdots \\ \Longrightarrow\ & l \mid \big(2^{r_n} - 1\big) \\ \Longrightarrow\ & l = 1. \\ \Longrightarrow\ & gcd(M_q, M_p) = 1. \qquad \square \end{aligned}$$

7.2 Lecture 2

Preamble: In this lecture we will first identify the prime numbers which can be expressed as the sum of two squares of integers. Then we will characterize all the positive integers which can be expressed as the sum of two squares.

Keywords: Thue's lemma, sum of two squares

7.2.1 Primes Expressible as a Sum of Two Squares

It is clear that $2 = 1^2 + 1^2$. Amongst the first few primes, observe that:

$$5 = 2^2 + 1^2, \;\; 13 = 3^2 + 2^2, \;\; 17 = 4^2 + 1^2, \;\; \cdots .$$

But we can not express 7 or 11 as sum of two squares. It is now natural to ask whether congruence modulo 4 determines whether a prime can be expressed as sum of two squares. In other words, we would like to establish whether an odd prime can be expressed as sum of squares if and only if it is of the form $4k + 1$.

PROPOSITION 7.6. *Let p be a prime of the form $4k + 3$. Then we can not express p as the sum of two squares.*

Proof: Suppose, if possible, $p = a^2 + b^2$. As p is odd, exactly one of a and b must be odd. Say $a = 2q$ and $b = 2l + 1$. Then

$$\begin{aligned} a^2 + b^2 &= 4(q^2 + l^2 + l) + 1 \\ \implies p &\equiv 1 \bmod 4. \qquad \square \end{aligned}$$

Next, let us show that any prime of the form $4k + 1$ can be expressed as sum of two squares.

THEOREM 7.7. *Let p be a prime of the form $4k + 1$. Then p can be expressed as the sum of two squares.*

Proof: If $p \equiv 1 \bmod 4$, we know that -1 is a quadratic residue modulo p. Hence, there is an integer a such that $a^2 \equiv -1 \bmod p$. Clearly, $(a, p) = 1$. The following result of Thue will show that if $(a, p) = 1$, then the linear congruence $ax \equiv y \bmod p$ has a solution

(x_0, y_0) such that $0 < |x_0| < \sqrt{p}$ and $0 < |y_0| < \sqrt{p}$. Given this result, we have

$$\begin{aligned} a^2x_0^2 &\equiv y_0^2 \bmod p \\ \implies -x_0^2 &\equiv y_0^2 \bmod p \\ \implies x_0^2 + y_0^2 &= kp \end{aligned}$$

for some integer k. But due to the bounds on x_0 and y_0, we have

$$\begin{aligned} 0 < x_0^2 + y_0^2 = kp &< p + p \\ \implies x_0^2 + y_0^2 &= p. \qquad \square \end{aligned}$$

Now we need only prove the following lemma to complete the proof the above theorem.

LEMMA 7.8. *(***Thue's lemma***) If p is a prime such that $(a, p) = 1$, then the linear congruence*

$$ax \equiv y \ mod \ p$$

has a solution (x_0, y_0) such that $0 < x_0 < \sqrt{p}$ and $0 < y_0 < \sqrt{p}$.

Proof: Let $m = \lfloor \sqrt{p} \rfloor$, where $\lfloor \sqrt{p} \rfloor$ denotes the largest integer less than $\sqrt{p}$. Consider the set

$$T = \{ax - y \mid 0 \le x \le m, \ \ 0 \le y \le m\}.$$

The set T has $(m+1)^2$ distinct elements. Since there are exactly p distinct equivalent classes modulo p, and $(m+1)^2 > p$, the set T contains at least two elements which are congruent modulo p. Suppose $(x_1, y_1) \neq (x_2, y_2)$ are two pairs for which

$$\begin{aligned} ax_1 - y_1 &\equiv ax_2 - y_2 \bmod p \\ \implies a(x_1 - x_2) &\equiv (y_1 - y_2) \bmod p, \\ \text{But } x_1 - x_2 = 0 &\Leftrightarrow y_1 - y_2 = 0 \\ \implies 0 < |x_1 - x_2| \le m < \sqrt{p}, & \quad 0 < |y_1 - y_2| \le m < \sqrt{p}. \\ \text{Taking } x_0 = x_1 - x_2, & \quad y_0 = y_1 - y_2 \\ \implies 0 < |x_0|, \ \ |y_0| &< \sqrt{p}, \text{ and} \\ ax_0 &\equiv y_0 \bmod p. \qquad \square \end{aligned}$$

Thus, we have completely characterized the primes that can be expressed as sum of two squares.

7.2.2 Integers Expressible as a Sum of Two Squares

In this section, our goal is to characterize the integers which are some of two squares. First we observe that of two integers are sum of two squares, so is their product.

LEMMA 7.9. *If two integers k and l are sum of two squares, so is kl.*

Proof:

$$\begin{aligned} k = & \quad a^2 + b^2, \qquad l = c^2 + d^2 \\ \implies kl = & \quad \big(a^2 + b^2\big).\big(c^2 + d^2\big) \\ = & \quad a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\ = & \quad (ac - bd)^2 + (ad + bc)^2. \qquad \square \end{aligned}$$

The above lemma also indicates that it is the square-free part of an integer that decides its expressibility as sum of two squares. In the following theorem, we look more closely at the square-free part of an integer.

THEOREM 7.10. *Let $n = m^2k$, where k is square-free (i.e., $p^2 \nmid k$ for any prime p). Then n can be expressed as sum of two squares if and only if k has no prime factor of the form $4l + 3$.*

Proof: If k has no prime factor of the form $4l + 3$, then each prime factor of k is sum of two squares. Hence their product k is also a sum of two squares by the previous lemma. Therefore,

$$n = m^2k = (mr)^2 + (ms)^2 \text{ where } k = r^2 + s^2.$$

Conversely, let $n = a^2 + b^2$ and p be an odd prime dividing k. We want to show that p must be of the form $4k + 1$. Equivalently, it is enough to show that -1 is a quadratic residue modulo p. We have

$$a^2 + b^2 = n = m^2k \equiv 0 \bmod p,$$

as p divides k. If p does not divide a, then we have an integer a' such that $aa' \equiv 1$ modulo p. Then,

$$a^2 + b^2 \equiv 0 \bmod p \implies 1 + (a'b)^2 \equiv 0 \bmod p,$$

and we have -1 as a quadratic residue of p.

If p divides a, then we need to take an extra step to show that -1 is a quadratic residue modulo p. Let $d = gcd(a, b)$, say $a = dx,\ b = dy$. Then $gcd(x, y) = 1$, and $d^2(x^2 + y^2) = m^2k$. As k is square-free, d must divide m, and we have

$$\begin{aligned} x^2 + y^2 &= \left(\frac{m}{d}\right)^2 k \\ \implies x^2 + y^2 &\equiv 0 \bmod p. \end{aligned}$$

As $gcd(x, y) = 1$, one of them, say x is coprime to p. Then, we have an integer x' such that $xx' \equiv 1 \bmod p$. This yields

$$\begin{aligned} x^2x'^2 + y^2x'^2 &\equiv 0 \bmod p \\ \implies (yx')^2 &\equiv -1 \bmod p \\ \implies p &\equiv 1 \bmod 4. \qquad \square \end{aligned}$$

The following corollary is just a restatement of the previous theorem.

COROLLARY 7.11. *An integer n is sum of two squares if and only if its prime factors of the form $4l + 3$ occur with an even exponent.*

For example, $n = 19^2.29.53$ will be a sum of two squares. We have $29 \equiv 1$ and $53 \equiv 1$ modulo 4. Though $19 \equiv 3$ modulo 4, its exponent is even. Explicitly,

$$29 = 5^2{+}2^2,\ \ 53 = 7^2{+}2^2,\ \ 29.57 = (5.7{-}2.2)^2{+}(2.7{-}5.2)^2 \implies 19^2.29.5 = (19.31)^2{+}(19.4)^2.$$

We can immediately say $n = 31.37.43^2$ can not be expressed as the sum of two squares, as the prime $31 = 4.7 + 3$ has odd exponent.

7.3 Lecture 3

Preamble: In this lecture, we will discuss whether we can express any positive integer as sum of three or four squares. We will first establish a necessary condition for a integer to be sum of three squares. We will then show that any prime number can be expressed as the sum of four squares of integers. Consequently, we will conclude that any positive integer can be expressed as the sum of four squares.

Keywords: sum of three squares, sum of four squares, Waring's problem

7.3.1 Sum of Three Squares

In the previous lecture, we have seen that we can not express certain integers as the sum of two squares. A natural question at this point is whether we can express every integer n as the sum of three squares or four squares. Three squares are also not enough, as the following proposition shows.

PROPOSITION 7.12. *An integer n can not be expressed as the sum of three squares if n is of the form $8k + 7$.*

Proof: Let $n = a^2+b^2+c^2$. If m is an even integer then $m = 4l$ or $4l+2$, so $m^2 = 16l^2$ or $m^2 = 16(l^2+l)+4$ and $m^2 \equiv 0$ or $4 \bmod 8$. If $m = 2l+1$ is odd, then $m^2 = 4l(l+1)+1$ is 1 modulo 8. Hence, the only possibilities for $a^2+b^2+c^2$ modulo 8 are $0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6$. □

COROLLARY 7.13. *An integer n can not be expressed as the sum of three squares if n is of the form $4^m(8k + 7)$ for any non-negative integer m.*

Proof: If possible, suppose there exists $m \geq 1$ such that

$$4^m(8k + 7) = a^2 + b^2 + c^2.$$

If exactly two of them are odd, then $a^2 + b^2 + c^2$ will be $2 \bmod 4$. The only option is that a, b, c are even when $m \geq 1$. Letting $a = 2a_1$, $b = 2b_1$, $c_1 = 2c_1$, we then have

$$4^{m-1}(8m + 7) = a_1^2 + b_1^2 + c_1^2.$$

Repeating this argument, we will eventually obtain $8k + 7$ as the sum of three squares, which will contradict the above proposition. □

The converse part of the above corollary is also true, i.e., any integer which is not of the form $4^m(8k+7)$ can be expressed as the sum of three squares, but we will not include the proof in these notes.

7.3.2 Sum of Four Squares

In this section we will investigate which integers can be expressed as sum of four squares. First, we will show that of two integers are sum of four squares, so is their product.

PROPOSITION 7.14. *If m, and n can be expressed as sum of four squares, then mn can also be expressed the sum of four squares.*

Proof: Let

$$m = a^2 + b^2 + c^2 + d^2 \text{ and } n = x^2 + y^2 + z^2 + w^2.$$

Then, one can directly verify that

$$\begin{aligned} mn &= (a^2+b^2+c^2+d^2)(x^2+y^2+z^2+w^2) \\ &= (ax+by+cz+dw)^2 + (ay-bx+cw-dz)^2 \\ &\quad +(az-bw-cx+dy)^2 + (aw+bz-cy-dx)^2. \qquad \square \end{aligned}$$

Our aim now is to show that every prime can be expressed as sum of four squares. Then, any positive integer is a sum of four squares in view of the above lemma. We will first prove that for any prime p, there exists a positive integer $k < p$ such that kp is sum of four squares. Then we will show that the smallest such k must be 1. We begin with the following lemma.

LEMMA 7.15. *Let p be an odd prime. Then the congruence*

$$x^2 + y^2 + 1 \equiv 0 \ mod\ p$$

has a solution $x_0,\ y_o$ where $0 \le x_0,\ y_0 \le \frac{p-1}{2}$.

Proof: We will apply pigeon-hole principle. Consider the two sets

$$S = \Big\{1+0^2,\ 1+1^2,\ \ldots,\ 1+\Big(\frac{p-1}{2}\Big)^2\Big\}, \qquad T = \Big\{-0^2,\ -1^2,\ \ldots,\ -\Big(\frac{p-1}{2}\Big)^2\Big\}.$$

Two distinct elements of S can not be congruent modulo p:

$$\begin{aligned} 1+x_1^2 &\equiv 1+x_2^2 \bmod p \\ \Longrightarrow\ x_1 &\equiv \pm x_2 \bmod p \end{aligned}$$

As $0 \leq x_1 + x_2 \leq 2.\left(\frac{p-1}{2}\right) = p-1$, we must have $x_1 = x_2$. Similarly, no two elements of T are congruent modulo p. Now the set $S \cup T$ has $2(1 + \frac{p-1}{2}) = p+1$ elements. There are only p distinct congruence classes modulo p, hence SUT must have two elements in the same congruence class modulo p. Neither S nor T can contain both these elements as shown in the above paragraph. Thus, one of these elements is in S, sat $1 + x_0^2$, and the other is in T, say $-y_0^2$. Then,

$$\begin{aligned} 0 \leq x_0,\, y_0 &\leq \frac{p-1}{2}, \\ 1 + x_0^2 &\equiv -y_0^2 \bmod p. \qquad \square \end{aligned}$$

COROLLARY 7.16. *Given an odd prime p, there exists a positive integer $k < p$ such that kp is the sum of four squares.*

Proof: By the previous lemma, there is an integer k and $x_0, y_o < \frac{p}{2}$ with

$$\begin{aligned} kp &= 1 + x_0^2 + y_0^2 + 0^2 \\ &< 1 + \frac{p^2}{4} + \frac{p^2}{4} \\ &< p^2 \\ \implies k &< p. \qquad \square \end{aligned}$$

Now we have the necessary ingredients to show that any prime p is a sum of four squares. We will show that the smallest positive integer k satisfying the above lemma must be 1.

THEOREM 7.17. *Any prime p can be expressed as the sum of four squares.*

Proof: Clearly, $2 = 1^2+1^2+0^2+0^2$. Assume that p is an odd prime. Let k be the smallest positive integer such that kp is the sum of four squares. By the previous corollary, $k < p$. It is enough to show that $k = 1$. First, we will show that k is odd.

Suppose $kp = a^2 + b^2 + c^2 + d^2$. If k is even, then amongst a, b, c and d we must have exactly four odd, or two odd, or no odd integers. Without loss of generality, we may assume that $a \equiv b$, $c \equiv d \bmod 2$. Then,

$$\begin{aligned} & \left(\frac{a-b}{2}\right)^2 + \left(\frac{a+b}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 \\ = \;& \frac{2(a^2+b^2)}{4} + \frac{2(c^2+d^2)}{4} \\ = \;& \frac{a^2+b^2+c^2+d^2}{2} \\ = \;& \frac{kp}{2} = \frac{k}{2}.p. \end{aligned}$$

Then, we get a contradiction for the minimality of k. Hence k must be odd.

Now, suppose k is an odd integer, and $k \leq 3$. We can find

$$x \equiv a,\ y \equiv b,\ z \equiv c,\ w \equiv d \bmod k, \qquad |x|, |y|, |z|, |w| < \frac{k}{2}$$

as follows. By division algorithm, we have $a = kq + r$ for some $0 \leq r < k$. If $r < \frac{k}{2}$ then we can take $x = r$. If $r > \frac{k}{2}$, we observe that $a = k(q+1) + r - k \equiv r - k \bmod k$. Hence we can can take x to be $r - k$ which is bigger than $\frac{k}{2} - k = -\frac{k}{2}$ and smaller than $k - k = 0$. Now,

$$\begin{aligned} x^2 + y^2 + z^2 + w^2 &\equiv a^2 + b^2 + c^2 + d^2 = kp \equiv 0 \bmod k \\ \implies \exists l \geq 0 \text{ such that } lk &= x^2 + y^2 + z^2 + w^2 < 4.\frac{k^2}{4} = k^2. \end{aligned}$$

Thus, $0 \leq l < k$. But $l = 0$ would imply that

$$x^2 + y^2 + z^2 + w^2 = lk = 0 \implies x = y = z = w = 0 \implies a \equiv 0 \equiv b \equiv c \equiv d \bmod k.$$

Hence, k^2 divides $a^2 + b^2 + c^2 + d^2 = kp$ and $k|p$. But $1 < k < p$, and p is a prime, so it is not possible. Hence $0 < l < k$. Now,

$$\begin{aligned} k^2lp &= kp.lk = (a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + w^2) \\ &= r^2 + s^2 + t^2 + u^2, \end{aligned}$$

where

$$r = ax + by + cz + dw \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \bmod k.$$

Similarly, k divides s, t, and u, and we have

$$lp = \left(\frac{r}{k}\right)^2 + \left(\frac{r}{k}\right)^2 + \left(\frac{r}{k}\right)^2 + \left(\frac{r}{k}\right)^2,$$

which again contradicts the minimality of k. Hence $k = 1$, and $k.p = p$ can be expressed as sum of four squares. □

As the product of sum of four squares is again a sum of four squares, we have now shown that any positive inetger can be expressed as sum of four squares.

7.3.3 Waring's Problem

We have shown that four squares are sufficient to express any positive integer as sum. Can such a result be generalized to any power? For a given natural number k, does there exist an integer $g(k)$ such that every positive integer n can be expressed as

$$n = a_1^k + a_2^k + \ \ldots\ + a_{g(k)}^k,$$

where a_is are non-negative integers, not necessarily distinct? This question is known as Waring's problem. Dickson showed that $g(3) = 9$. It was proved later that only a finite number of integers need 9 cubes, all except finitely many integers can be expressed as the sum of seven cubes,. Whether 6 cubes suffice or not is still an open question. The existence of $g(k)$ for each k was established by Hilbert, but his proof is not constructive. A relevant question is as follows: let $G(k)$ be the smallest integer r with the property that all except finitely many integers can be expressed as the sum of at most r k-th powers. Clearly, $G(k) \leq g(k)$. The exact values of $G(k)$ are known only for $k = 2$ and $k = 4$.

7.4 Exercises

1. Show that the n-th Fermat number must be of the form $9k + 5$ if n is odd, and of the form $9k + 8$ if it is even.

2. Show that the last digit of any Fermat's number except 5 must be 7. Deduce that a Fermat's number can never be a square.

3. Prove that $F_n \mid \left(2^{F_n} - 2\right)$, i.e., F_n is a pseudoprime if it is not a prime.

4. Show that there are infinitely many primes by proving that $2^{2^n} - 1$ has at least n distinct prime divisors.

5. Let n be a perfect number. Show that

$$\sum_{d|n} \frac{1}{d} = 2.$$

6. If the last digit of an integer is 0 or 2 or 4, then show that it can not be perfect.

7. If n is a perfect number, show that any proper divisor of n can not be a perfect number.

8. Show that any Fermat's number can be written as the difference of two squares.

9. Let p be a prime number and M_p be the p-th Mersenne number. Show that any prime divisor of M_p must be of the form $2kp + 1$.

10. Show that any prime divisor of M_p must be of the form $8k \pm 1$.

11. Show that an integer of the form $9k + 5$ can not be expressed as the sum of three cubes.

12. If a prime number is the sum of squares of three primes, the one of these primes must be 3.

13. Show that an integer of the form $4k + 2$ can not be expressed as the difference of two squares.

14. Show that any odd integer can be expressed as he difference of two squares.

15. If n is divisible by 4 then n can be expressed as the difference of two squares.

16. Show that any prime number p of the form $8k + 1$ or $8k + 3$ can be written as

$$p = a^2 + 2b^2$$

for some integers a and b.

17. Show that the product of two sums of three squares need not be a sum of three squares.

18. If n is a sum of two relatively prime squares, then show that any divisor of n is also sum of two squares.

19. If n is a sum of two squares of rational numbers, then show that n is a sum of two squares of integers as well.

Module 8

Continued Fractions

8.1 Lecture 1

Preamble: In this lecture, we will introduce finite continued fractions. We will show that a finite continued fraction represents a rational number, and every rational number can be expressed by a finite continued fraction in a unique way. Continued fractions provide an important approach for solving Diophantine equations.

Keywords: continued fractions, Euler's rule, convergents.

8.1.1 Finite Continued Fractions

Definition 8.1. *A finite continued fraction is an expression of the form*

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}, \tag{8.1}$$

where $q_i \in \mathbb{Z}$, $q_i \geq 1$ for all $i > 1$, and $q_n > 1$, where n is some positive integer.

Clearly, such an expression represents a rational number. For example,

$$-2+\cfrac{1}{3+\cfrac{1}{4+\cfrac{1}{5+\cfrac{1}{6}}}} = -2+\cfrac{1}{3+\cfrac{1}{4+\cfrac{6}{31}}} = -2+\cfrac{1}{3+\cfrac{31}{130}} = -2+\frac{130}{421} = \frac{-712}{421}.$$

Conversely, given any rational number $\frac{a}{b}$ we can apply Euclid's algorithm to express it as a finite continued fraction. We may assume, without loss of generality, that b is a natural number. Then,

$$\begin{aligned} a &= q_0 b + r_1, & 0 < r_1 < b \\ b &= q_1 r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 &= q_2 r_2 + r_3 & 0 < r_3 < r_2 \\ \vdots &= \vdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} &= q_n r_n \end{aligned}$$

Then, we obtain

$$\frac{a}{b} = q_0 + \cfrac{1}{\cfrac{b}{r_1}} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{\cfrac{r_1}{r_2}}} = \cdots = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}.$$

For example, consider $-\frac{65}{23}$.

$$\begin{aligned} -65 &= -3 \times 23 + 4 \\ 23 &= 5 \times 4 + 3 \\ 4 &= 1 \times 3 + 1 \\ 3 &= 3 \times 1. \end{aligned}$$

Then, we can obtain

$$-\frac{65}{23} = -3 + \frac{4}{23} = -3 + \cfrac{1}{\cfrac{23}{4}} == -3 + \cfrac{1}{5 + \cfrac{3}{4}} = -3 + \cfrac{1}{5 + \cfrac{\cfrac{1}{4}}{3}} = -3 + \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{3}}}.$$

For brevity, we will denote the continued fraction (8.1) by

$$q_0 + \frac{1}{q_1+}\frac{1}{q_2+}\frac{1}{q_3+}\cdots\frac{1}{q_{n-1}+}\frac{1}{q_n}.$$

THEOREM 8.2. *Every rational number is uniquely represented by a finite continued fraction.*

Proof: We have already shown above the existence of such a representation by Euclid's algorithm. We need to show that two such expressions for the same rational number must be identical. So assume that a rational number r is represented by

$$r = q_0 + \frac{1}{q_1+}\frac{1}{q_2+}\frac{1}{q_3+}\cdots\frac{1}{q_{n-1}+}\frac{1}{q_n}, \qquad r = p_0 + \frac{1}{p_1+}\frac{1}{p_2+}\frac{1}{p_3+}\cdots\frac{1}{p_{m-1}+}\frac{1}{p_m}.$$

Observe that $\frac{1}{q_1+}\frac{1}{q_2+}\frac{1}{q_3+}\cdots\frac{1}{q_{n-1}+}\frac{1}{n}$ and $\frac{1}{p_1+}\frac{1}{p_2+}\frac{1}{p_3+}\cdots\frac{1}{p_{m-1}+}\frac{1}{p_m}$ are stricyly less than 1, hence q_0 and p_0 both represent the greatest integer less than or equal to r, hence $q_0 = p_0$. Canceling these, we obtain,

$$q_1 + \frac{1}{q_2+}\frac{1}{q_3+}\cdots\frac{1}{q_{n-1}+}\frac{1}{q_n} = p_1 + \frac{1}{p_2+}\frac{1}{p_3+}\cdots\frac{1}{p_{m-1}+}\frac{1}{p_m},$$

and repeating the argument we get $q_1 = p_1$. Continuing this way, we have $q_i = p_i$ for all $0 \le i \le n$ and $n = m$. $\square$

8.1.2 General Continued Fraction

The relation amongst the coefficients q_i in a continued fraction

$$q_0 + \frac{1}{q_1+}\frac{1}{q_2+}\frac{1}{q_3+}\cdots\frac{1}{q_{n-1}+}\frac{1}{q_n},$$

can be studied without using the actual values of the q_i's or even without consideration of the fact that q_i's are integers. We will now treat the q_i's as variables and deduce interesting algebraic identities involving the coefficients. The following proposition is very useful in the study of continued fractions.

Let us define

$$\begin{aligned}
\big[q_0\big] &= q_0, \\
\big[q_0, q_1\big] &= q_0q_1 + 1, \\
\big[q_0, q_1, q_2\big] &= q_0q_1q_2 + q_0 + q_2 = q_0[q_1, q_2] + [q_2] \\
\big[q_0, q_1, q_2, q_3\big] &= q_0q_1q_2q_3 + q_0q_1 + q_0q_3 + q_2q_3 + 1 = q_0\big[q_1, q_2, q_3\big] + \big[q_2, q_3\big] \\
\vdots &= \vdots \\
\big[q_0, q_1, q_2, \cdots, q_n\big] &= q_0\big[q_1, q_2, \cdots, q_n\big] + \big[q_2, q_2, \cdots, q_n\big]
\end{aligned}$$

PROPOSITION 8.3.

$$q_0 + \frac{1}{q_1+}\frac{1}{q_2+}\frac{1}{q_3+}\cdots\frac{1}{q_{n-1}+}\frac{1}{q_n} = \frac{[q_0, q_1, q_2, \cdots, q_n]}{[q_1, q_2, \cdots, q_n]}.$$

Proof: Let us use induction on n. Thee is nothing to prove if $n = 0$. For $n = 1$,

$$q_0 + \frac{1}{q_1} = \frac{q_0q_1 + 1}{q_1} = \frac{\big[q_0, q_1\big]}{\big[q_1\big]}.$$

For $n = 2$,

$$q_0 + \frac{1}{q_1+}\frac{1}{q_2} = q_0 + \frac{q_2}{q_1q_2 + 1} = \frac{q_0q_1q_2 + q_1 + q_2}{q_1q_2 + 1} = \frac{\big[q_0, q_1, q_2\big]}{\big[q_1, q_2\big]}.$$

Assume the result is true for $n - 1 \geq 2$. Now,

$$\begin{aligned}
& q_0 + \frac{1}{q_1+}\frac{1}{q_2+}\frac{1}{q_3+}\cdots\frac{1}{q_{n-1}+}\frac{1}{q_n} \\
= \; & q_o + \cfrac{1}{q_1 + \frac{1}{q_2+}\frac{1}{q_3+}\cdots\frac{1}{q_{n-1}+}\frac{1}{q_n}} \\
= \; & q_0 + \cfrac{1}{\cfrac{\big[q_1, q_2, \cdots, q_n\big]}{\big[q_2, \cdots, q_n\big]}} \\
= \; & \frac{q_0\big[q_1, q_2, \cdots, q_n\big] + \big[q_2, \cdots, q_n\big]}{\big[q_1, q_2, \cdots, q_n\big]} \\
= \; & \frac{\big[q_0, q_1, q_2, \cdots, q_n\big]}{\big[q_1, q_2, \cdots, q_n\big]}. \qquad \square
\end{aligned}$$

8.2 Lecture 2

Preamble: In this lecture, we will discuss Euler's rule, which provides a way of computing the denominator and the numerator of the convergents. Then we will show how continued fractions can be used to find solutions for linear Diophantine equations.

Keywords: Euler's rule, convergents, linear Diophantine equations

8.2.1 Euler's Rule

Consider a continued fractions

$$q_0 + \frac{1}{q_1+}\frac{1}{q_2+}\frac{1}{q_3+}\cdots\frac{1}{q_{n-1}+}\frac{1}{q_n}.$$

We know that it can be evaluated as

$$\frac{\big[q_0, q_1, q_2, \cdots, q_n\big]}{\big[q_1, q_2, \cdots, q_n\big]},$$

where we recall that

$$\begin{aligned}
\big[q_0\big] &= q_0, \\
\big[q_0, q_1\big] &= q_0q_1 + 1, \\
\big[q_0, q_1, q_2, \cdots, q_n\big] &= q_0\big[q_1, q_2, \cdots, q_n\big] + \big[q_2, q_2, \cdots, q_n\big]
\end{aligned}$$

Euler's rule describes how one can evaluate the expression $\big[q_0, q_1, q_2, \cdots, q_n\big]$ directly without the recurrence relation. It says that *the expression* $\big[q_0, q_1, q_2, \cdots, q_n\big]$ *can be evaluated by taking the product of all* q_i*'s, then taking all products by omitting a pair of consecutive* q_i*'s, then taking all products by omitting two separate pairs of consecutive* q_i*'s, and so on and then taking the sum of all such products. The convention is to take* 1 *as the product when no* q_i*'s are left, which happens when* $n+1$ *is even.* One can directly see this for $n = 1, 2, 3$ etc. In general, one can prove the rule by induction. Assume the rule holds for $n-1$. Now,

$$\big[q_0, q_1, q_2, \cdots, q_n\big] = q_0\big[q_1, q_2, \cdots, q_n\big] + \big[q_2, \cdots, q_n\big].$$

By induction, the latter summand on the right above contains all products where the pair q_0, q_1 is not present, and the former summand on the RHS contains all products where the pair q_0q_1 are present. Thus, the rule hold for n as well.

COROLLARY 8.4.

$$\big[q_0, q_1, q_2, \cdots, q_n\big] = \big[q_n, q_{n-1}, q_{n-2}, \cdots, q_0\big].$$

This corollary is an immediate consequence of Euler's rule.

COROLLARY 8.5.

$$\big[q_0, q_1, q_2, \cdots, q_n\big] = q_n\big[q_0, q_1, q_2, \cdots, q_{n-1}\big] + \big[q_0, q_1, q_2, \cdots, q_{n-2}\big] \tag{8.2}$$

Proof: We have

$$\begin{aligned}\big[q_0, q_1, q_2, \cdots, q_n\big] &= \big[q_n, q_{n-1}, q_{n-2}, \cdots, q_0\big] \\ &= q_n\big[q_{n-1}, q_{n-2}, \cdots, q_0\big] + \big[q_{n-2}, \cdots, q_0\big] \\ &= q_n\big[q_0, q_1, \cdots, q_{n-1}\big] + \big[q_0, \cdots, q_{n-2}\big] \qquad \square\end{aligned}$$

8.2.2 Convergents

Consider a continued fractions

$$q_0 + \frac{1}{q_1+}\frac{1}{q_2+}\frac{1}{q_3+}\cdots\frac{1}{q_{n-1}+}\frac{1}{q_n},$$

where q_i's are natural numbers. The q_i's are called **partial quotients** of the continued fraction. The various continued fractions obtained by considering only the first partial quotient, then the first two, then the first three, etc , upto the first n (i.e, all of them) are called **convergents** of the given continued fractions. In other words, the convergents to the above continued fraction are

$$q_0,\ q_0+\frac{1}{q_1},\ q_0+\frac{1}{q_1+}\frac{1}{q_2},\ \cdots\ q_0+\frac{1}{q_1+}\frac{1}{q_2+}\frac{1}{q_3+}\cdots\frac{1}{q_{n-1}},\ q_0+\frac{1}{q_1+}\frac{1}{q_2+}\frac{1}{q_3+}\cdots\frac{1}{q_{n-1}+}\frac{1}{q_n}.$$

The value of the m-th $(0 \le m \le n)$convergent is

$$q_0 + \frac{1}{q_1+}\frac{1}{q_2+}\frac{1}{q_3+}\cdots\frac{1}{q_{m-1}+}\frac{1}{q_m} = \frac{\big[q_0, q_1, q_2, \cdots, q_m\big]}{\big[q_1, q_2, \cdots, q_m\big]}.$$

In order to obtain simpler expressions, let is write

$$A_m = \big[q_0, q_1, q_2, \cdots, q_m\big], \quad B_m = \big[q_1, q_2, \cdots, q_m\big],$$

so that the m-th convergent can be written as $\frac{A_m}{B_m}$. The first few convergents are then

$$\frac{A_0}{B_0} = q_0, \quad \frac{A_1}{B_1} = \frac{q_0q_1+1}{q_1}, \quad \frac{A_2}{B_2} = \frac{q_0q_1q_2+q_0+q_2}{q_1q_2+1}, \cdots$$

In view of (8.2), we have

$$A_m = q_m A_{m-1} + A_{m-2}, \qquad B_m = q_m B_{m-1} + B_{m-2}. \tag{8.3}$$

The following identity is very useful:

PROPOSITION 8.6. *For $m \geq 1$,*

$$A_m B_{m-1} - A_{m-1} B_m = (-1)^{m-1}$$

Proof: We will use induction on m. Clearly, the result holds for $m = 1$:

$$\begin{aligned} & A_0 = q_0, \;\; B_0 = 1, \;\; A_1 = q_0 q_1 + 1, \;\; B_1 = q_1 \\ \Longrightarrow \qquad & A_1 B_0 - A_0 B_1 = q_0 q_1 + 1 - q_0 q_1 = 1. \end{aligned}$$

Let $m \geq 2$ and assume the result hold for $m - 1$. Then, in view of (8.3)

$$\begin{aligned} A_m B_{m-1} - A_{m-1} B_m &= \big(q_m A_{m-1} + A_{m-2}\big) B_{m-1} - A_{m-1}\big(q_m B_{m-1} + B_{m-2}\big) \\ &= -\big(A_{m-1} B_{m-2} - A_{m-2} B_{m-1}\big) \\ &= -(-1)^{m-2} \quad \text{(by induction hypothesis)} \\ &= (-1)^{m-1}. \quad \square \end{aligned}$$

COROLLARY 8.7. *A_m and B_m are always relatively prime.*

COROLLARY 8.8.

$$\frac{A_m}{B_m} - \frac{A_{m-1}}{B_{m-1}} = \frac{(-1)^{m-1}}{B_m B_{m-1}}.$$

When we develop a rational number $\frac{a}{b}$ as a continued fraction, the convergents give us a finite sequence with $\frac{a}{b}$ as the final term.

COROLLARY 8.9. *We have the following inequalities for the convergents:*

$$\frac{A_0}{B_0} < \frac{A_2}{B_2} < \cdots < \frac{A_{2m-2}}{B_{2m-2}} < \frac{A_{2m}}{B_{2m}} < \cdots \leq \frac{a}{b} \leq \cdots < \frac{A_{2m-1}}{B_{2m-1}} < \frac{A_{2m-3}}{B_{2m-3}} < \cdots < \frac{A_3}{B_3} < \frac{A_1}{B_1}.$$

Proof: Recall that B_i form an increasing sequence of positive integers. It is clear from

the previous corollary that

$$\begin{aligned}
\frac{A_{2m}}{B_{2m}} - \frac{A_{2m-1}}{B_{2m-1}} &= \frac{-1}{B_{2m}B_{2m-1}} < 0 \\
\frac{A_{2m-1}}{B_{2m-1}} - \frac{A_{2m-2}}{B_{2m-2}} &= \frac{1}{B_{2m-1}B_{2m-2}} > 0 \\
\frac{A_{2m-2}}{B_{2m-2}} - \frac{A_{2m-3}}{B_{2m-3}} &= \frac{-1}{B_{2m-2}B_{2m-3}} < 0 \\
\implies \quad \frac{A_{2m}}{B_{2m}} - \frac{A_{2m-2}}{B_{2m-2}} &= -\frac{1}{B_{2m}B_{2m-1}} + \frac{1}{B_{2m-1}B_{2m-2}} > 0, \\
\frac{A_{2m-1}}{B_{2m-1}} - \frac{A_{2m-3}}{B_{2m-3}} &= \frac{1}{B_{2m-1}B_{2m-2}} - \frac{1}{B_{2m-2}B_{2m-3}} < 0,
\end{aligned}$$

noting that

$$B_{2m-2}B_{2m-3} < B_{2m-1}B_{2m-2} < B_{2m}B_{2m-1}$$

as B_i's form an increasing sequence. Thus, the even convergents form an increasing sequence approaching $\frac{a}{b}$ from below, and the odd convergents form a decreasing sequence, approaching $\frac{a}{b}$ from above. □

8.2.3 Application in Solving Linear Diophantine Equations

We can use continued fractions to find solutions of linear Diophantine equation of the form

$$ax - by = 1.$$

PROPOSITION 8.10. *Let $\frac{A_m}{B_m}$ denote the convergents when we express $\frac{a}{b}$ as a continued fraction. If $\frac{A_n}{B_n} = \frac{a}{b}$, then $x = B_{n-1}$, $y = A_{n-1}$ is a solution if n is odd, and $x = b - B_{n-1}$, $y = a - A_{n-1}$ is a solutin if n is even.*

Proof: We have

$$\begin{aligned}
A_nB_{n-1} - A_{n-1}B_n &= (-1)^{n-1} \\
\implies aB_{n-1} - bB_{n-1} &= (-1)^{n-1}.
\end{aligned}$$

If n is odd, clearly we have $x = B_{n-1}$, $y = A_{n-1}$ as a solution. If n id even, then

$$a(b - B_{n-1}) - b(a - A_{n-1}) = -\big(A_nB_{n-1} - A_{n-1}B_n\big) = -(-1)^{n-1} = 1. \ \square$$

8.3 Lecture 3

Preamble: In this lecture, we will introduce infinite continued fractions. We will show that any irrational number can be expressed uniquely as an infinite continued fraction. We will also discuss continued fraction which are periodic.

Keywords: Infinite continued fractions

8.3.1 Infinite Continued Fractions

We have seen before that any rational number can be expressed as a continued fraction using finitely many partial quotients q_0, q_1, $\cdots$, q_n, where q_i's are natural numbers for $i \geq 1$, and q_0 is an integer, which can be negative or zero. A natural question is whether we can express irrational numbers as a continued fraction. We will show that this is always possible, if we allow the final partial quotient to be irrational. If we want to involves only natural numbers, we can still express a irrational number as a continued fraction, but we will soon see that we have to allow for infinitely many partial quotients.

Let α be an irrational number. We can develop its continued fractions as follows. Let q_0 be the integral part of α, i.e., $\alpha = q_0 + \theta_0$, where $0 < \theta_0 < 1$. Note that q_0 is an integer, which can be positive, negative or zero. If $\theta_0 = 0$, then α would be rational. Now, $\alpha_1 = \frac{1}{\theta_0}$ is an irrational number bigger than 1. Let q_1 be the integral part of α_1, i.e., $\alpha_1 = q_1 + \theta_2$, where $0 < \theta_2 < 1$. In the next step, $\alpha_2 := \frac{1}{\theta_1} = q_2 + \theta_3$ where $0 < \theta_3 < 1$ is irrational, and continue. Then,

$$\alpha = q_0 + \theta_0 = q_0 + \frac{1}{\alpha_1} = q_0 + \frac{1}{q_1 + \theta_2} = q_0 + \frac{1}{q_1 + \dfrac{1}{\alpha_2}} = q_0 + \frac{1}{q_1 + \dfrac{1}{q_2 + \theta_3}}.$$

Continuing this way, we obtain at the n-the step

$$\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots + \cfrac{1}{q_n + \cfrac{1}{\alpha_{n+1}}}}}}.$$

As before, we can define the m-th convergent $\frac{A_m}{B_m}$ to α by stopping at the m-th partial quotient q_m, i.e.,

$$\frac{A_m}{B_m} = q_0 + \frac{1}{q_1+}\frac{1}{q_2+}\frac{1}{q_3+}\cdots\frac{1}{q_{n-1}+}\frac{1}{q_m} = \frac{\left[q_0, q_1, q_2, \cdots, q_m\right]}{\left[q_1, q_2, \cdots, q_m\right]}. \tag{8.4}$$

As in the previous lectures, we will have

$$\begin{aligned} A_m &= q_m A_{m-1} + A_{m-2}, \\ B_m &= q_m B_{m-1} + B_{m-2} \end{aligned}$$

and

$$\begin{aligned} \alpha &= \frac{\left[q_0, q_1, q_2, \cdots, q_n, \alpha_{n+1}\right]}{\left[q_1, q_2, \cdots, q_n, \alpha_{n+1}\right]} \\ &= \frac{\alpha_{n+1}\left[q_0, q_1, q_2, \cdots, q_n\right] + \left[q_1, q_2, \cdots, q_n\right]}{\alpha_{n+1}\left[q_1, q_2, \cdots, q_n\right] + \left[q_2, \cdots, q_n\right]} \\ &= \frac{\alpha_{n+1}A_n + A_{n-1}}{\alpha_{n+1}B_n + B_{n-1}}. \end{aligned}$$

We will now show that the sequence $\frac{A_m}{B_m}$ actually converges to α, so that we can represent any irrational number α as a limit of continued fractions involving only natural numbers (with the possible exception of the 0-th quotient). We will express this as

$$\alpha = q_o + \frac{1}{q_1+}\frac{1}{q_2+}\frac{1}{q_3+}\cdots\frac{1}{q_n+\cdots}.$$

The expression on the RHS above is called an **infinite continued fraction**. We will further show that any infinite continued fraction as above always represents some irrational number β, and the partial quotients that can be obtained from β coincides with the q_i's. Thus, we will show that any irrational number can be uniquely expressed as an infinite continued fraction involving only natural numbers except possibly for a non-positive integer for the zero-th partial quotient.

THEOREM 8.11. *Let $\frac{A_m}{B_m}$ be the convergents obtained from an irrational number α. Then, the sequence $(\frac{A_m}{B_m})$ converges to α.*

Proof:

$$\begin{aligned}\alpha - \frac{A_m}{B_m} &= \frac{\alpha_{m+1}A_m + A_{m-1}}{\alpha_{m+1}B_m + B_{m-1}} - \frac{A_m}{B_m} \\ &= \frac{\alpha_{m+1}A_mB_m + A_{m-1}B_m - \alpha_{m+1}B_mA_m - A_mB_{m-1}}{\big(\alpha_{m+1}B_m + B_{m-1}\big)B_m} \\ &= \frac{-(-1)^{m-1}}{\big(\alpha_{m+1}B_m + B_{m-1}\big)B_m}.\end{aligned}$$

Observe that $\alpha_{m+1} > q_{m+1}$. Thus,

$$|\ \alpha - \frac{A_m}{B_m}\ | = \frac{1}{\big(\alpha_{m+1}B_m + B_{m-1}\big)B_m} < \frac{1}{\big(q_{m+1}B_m + B_{m-1}\big)B_m} = \frac{1}{B_{m+1}B_m}. \qquad (8.5)$$

As the sequence B_m is a strictly increasing sequence of integers, we can conclude that $\frac{A_m}{B_m}$ converges to α as m goes to infinity. □

THEOREM 8.12. *Let $\frac{A_m}{B_m}$ be the convergents obtained from an infinite continued fraction*

$$q_0 + \frac{1}{q_1+}\frac{1}{q_2+}\frac{1}{q_3+}\cdots\frac{1}{q_n+}\cdots.$$

Then, the sequence $(\frac{A_m}{B_m})$ converges.

Proof: From corollary 2.4 of the previous lecture, it follows that the subsequence of even terms in the sequence $(\frac{A_m}{B_m})$ is an increasing sequence bounded above by $\frac{A_1}{B_1}$, and the subsequence of odd terms is decreasing sequence bounded below by $\frac{A_0}{B_0}$. Thus both subsequences are convergent by monotone convergence theorem. Corollary 2.3 from the previous lecture implies that the even and odd subsequences of the sequence $(\frac{A_m}{B_m})$ must converge to the same limit, as B_m is a strictly increasing sequence of integers. Hence the theorem follows. □

Remark: If α denotes the limits of the infinite continued fraction

$$q_0 + \frac{1}{q_1+}\frac{1}{q_2+}\frac{1}{q_3+}\cdots\frac{1}{q_n+}\cdots,$$

then we can easily show that the q_i's in the continued fraction are uniquely determined by the limit α:

As the infinite continued fraction $\frac{1}{q_1+}\frac{1}{q_2+}\frac{1}{q_3+}\cdots\frac{1}{q_n}+\cdots$ lies strictly between 0 and 1, q_0 must be the integral part of α. If we write $\alpha = q_0 + \frac{1}{\alpha_1}$, then

$$\alpha_1 = q_1 + \frac{1}{q_2+}\frac{1}{q_3+}\cdots\frac{1}{q_n} + \cdots,$$

and q_1 must be the integral part of α_1, which is uniquely determined by α. Proceeding in this way, we see that each q_i get uniquely determined by the limit α. We can conclude that an irrational number uniquely determines the infinite continued fraction representing it.

8.4 Lecture 4

Preamble: In this lecture we will discuss infinite continued fractions which are periodic. We will show that a periodic continued fractions represent a quadratic irrational number, and conversely, the infinite continued fraction of a quadratic irrational is periodic.

Keywords: periodic continued fraction, quadratic irrational

8.4.1 Periodic Continued Fractions

Consider the representation of $\sqrt{2}$ by continued fraction:

$$\sqrt{2} = 1 + \sqrt{2} - 1 = 1 + \frac{1}{\sqrt{2}+1} = 1 + \frac{1}{2+\sqrt{2}-1} = 1 + \frac{1}{2+}\frac{1}{2+}\cdots,$$

i.e., we have an infinite continued fraction which is repeated. We express this as

$$2 = 1, \overline{2}.$$

Similarly,

$$\begin{aligned}
\sqrt{3} &= 1 + \sqrt{3} - 1 = 1 + \frac{1}{\dfrac{1}{\sqrt{3}-1}} = 1 + \frac{1}{\dfrac{\sqrt{3}+1}{2}} \\
&= 1 + \frac{1}{1 + \dfrac{\sqrt{3}-1}{2}} = 1 + \frac{1}{1 + \dfrac{1}{\sqrt{3}+1}} \\
&= 1 + \frac{1}{1 + \dfrac{1}{2+\sqrt{3}-1}} \\
&= 1, \overline{1, 2}
\end{aligned}$$

DEFINITION 8.13. *An infinite continued fraction in which the partial quotients are repeated after a few initial terms is called* **periodic**. *It is called* **purely periodic** *if its partial quotient are repeated from the zero-th term onwards.*

8.4.2 Quadratic Irrationals and Their Continued Fractions

We have seen above that the continued fractions representing $\sqrt{2}$ and $\sqrt{3}$ are periodic. We may wonder whether an irrational number of the form $\sqrt{d}$ is always represented by

a periodic infinite continued fractions, and conversely, whether any periodic continued fraction always represents an irrational number of the form $\sqrt{d}$.

DEFINITION 8.14. *An irrational number is called quadratic irrational if it is the root of a quadratic equation with integral coefficients.*

For example, $\sqrt{2}$, $1+\sqrt{3}$ etc are quadratic irrationals. A quadratic over rational numbers has the form ax^2+bx+c, where a, b, c are rationals, thus a quadratic irrational can be written as $\frac{-b\pm\sqrt{d}}{2a}$ where $d=b^2-4ac$ is not the square of a rational number. In other words, a quadratic irrational is of the form $A+B\sqrt{d}$, where A, B are rational numbers, and d can be taken as a square-free integer, by changing B if necessary.

PROPOSITION 8.15. *A purely periodic continued fraction represents a quadratic irrational.*

Proof: Suppose a real number α has partial quotients $q_0,\cdots,q_n,q_0,\cdots q_n,\cdots$. Then,

$$\begin{aligned}
\alpha &= q_0+\frac{1}{q_1+}\frac{1}{q_2+}\cdots\frac{1}{q_n+}\frac{1}{q_1+}\frac{1}{q_2+}\cdots\frac{1}{q_n+}\cdots\\
\alpha &= q_0+\frac{1}{q_1+}\frac{1}{q_2+}\cdots\frac{1}{q_n+}\frac{1}{\alpha}\\
\Longrightarrow\ \alpha &= \frac{\big[q_0,q_1,\cdots,q_n,\alpha\big]}{\big[q_1,q_2,\cdots q_n,\alpha\big]}\\
&= \frac{\alpha A_n+A_{n-1}}{\alpha B_n+B_{n-1}}.
\end{aligned}$$

As A_m and B_m are all integers, we obtain α as a root of

$$B_n\alpha^2-(A_n-B_{n-1})\alpha-A_{n-1}=0.$$

Observe that if α were rational, it will not be represented by an infinite continued fraction. Hence the discriminant of the above equation is not a square. □

COROLLARY 8.16. *A periodic continued fraction represents a quadratic irrational.*

Proof: Suppose β is a real number which is represented by the partial quotients

$$p_0,p_1,\cdots,p_l,q_0,q_1,\cdots,q_n,q_0,q_1,\cdots,q_n,q_0,q_1,\cdots,q_n,\cdots.$$

Let α be represented by $q_0,q_1,\cdots,q_n,q_0,q_1,\cdots,q_n,q_0,q_1,\cdots,q_n,\cdots$. By the above

proposition, α is a quadratic irrational. Now,

$$\begin{aligned}\beta &= p_0 + \frac{1}{p_1+}\frac{1}{p_2+}\cdots\frac{1}{p_l+}\frac{1}{q_1+}\frac{1}{q_2+}\cdots\frac{1}{q_n+}\frac{1}{q_1+}\frac{1}{q_2+}\cdots\frac{1}{q_n+}\cdots \\ &= p_0 + \frac{1}{p_1+}\frac{1}{p_2+}\cdots\frac{1}{p_l+\alpha} \\ &= \frac{[p_0,\cdots p_l,\alpha]}{[p_1,\cdots p_l,\alpha]} = \frac{\alpha A'_l + A'_{l-1}}{\alpha B'_l + B'_{l-1}},\end{aligned}$$

where $\frac{A'_i}{B'_i}$'s are the first l convergents of β. As A'_i, B'_i are integers, it is clear that β can be expressed in the form $u + v\alpha$ where u and v are rational numbers. Hence β itself will be a quadratic irrational. □

The converse of the above is also true, i.e, the infinite continued fraction representing a quadratic irrational is necessarily periodic. This was first proved by Lagrange. Before proving the converse, we need to introduce the notion of conjugate of an quadratic irrational, and reduced quadratic irrational.

8.5 Lecture 5

Preamble: In this lecture, we will continue our discussion on continued fractions of quadratic irrationals. We will specify the quadratic irrationals which will be shown to have purely periodic continued fraction.

Keywords: conjugate, reduced quadratic irrational

8.5.1 Conjugate of a Quadratic Irrational

DEFINITION 8.17. *Let α be a quadratic irrational satisfying the equation $ax^2+bx+c=0$, where $a \neq 0$, b, c are rational numbers. Let α' be the second root of the above quadratic equation. We call α and α' to be conjugates. Clearly, $\alpha+\alpha' = -\frac{b}{a}$ and $\alpha\alpha' = \frac{c}{a}$.*

For example, $-\sqrt{3}$ is a conjugate of $\sqrt{3}$. and $11+\sqrt{3}$ is a conjugate of $11-\sqrt{3}$. It is easy to observe that

PROPOSITION 8.18. *Let α' be the conjugate of the quadratic irrational α. If r and s are rational numbers, then conjugate of $r+s\alpha$ will be $r+s\alpha'$. Similarly, the conjugate of $r+\frac{s}{\alpha}$ will be $r+\frac{s}{\alpha'}$*

Proof: Clearly, $r+s\alpha$ and $r+s\alpha'$ are the roots of the following quadratic polynomial with rational coefficients

$$(x-r-s\alpha)(x-r-s\alpha') = (x-r)^2 - s(x-r)(\alpha+\alpha') + s^2\alpha\alpha'.$$

Similarly, $r+\frac{s}{\alpha}$ and $r+\frac{s}{\alpha'}$ are the two roots of the following quadratic polynomial with rational coefficients:

$$\begin{aligned}\Big(x-r-\frac{s}{\alpha}\Big)\Big(x-r-\frac{s}{\alpha'}\Big) &= (x-r)^2 - s(x-r)\Big(\frac{1}{\alpha}+\frac{1}{\alpha'}\Big) + \frac{s^2}{\alpha\alpha'} \\ &= (x-r)^2 - s(x-r)\frac{\alpha+\alpha'}{\alpha\alpha'} + \frac{s^2}{\alpha\alpha'}. \qquad \square\end{aligned}$$

The following proposition tells us the relation between the quadratic irrationals represented by a purely periodic continued fraction and the purely periodic continued fraction obtained by reversing its period.

PROPOSITION 8.19. *Let $\overline{q_0, q_1, \cdots, q_n}$ be a purely periodic continued fraction representing the quadratic irrational α. Then the purely periodic continued fraction $\overline{q_n, \cdots, q_1, q_0}$ represents the quadratic irrational $-\frac{1}{\alpha'}$, where α' is the conjugate of α.*

Proof: We have

$$\begin{aligned} \alpha &= q_0 + \frac{1}{q_1+}\frac{1}{q_3+}\cdots\frac{1}{q_n+}\frac{1}{\alpha} \\ \implies \alpha &= \frac{\big[q_0, q_1, q_2, \cdots, q_n, \alpha\big]}{\big[q_1, q_2, \cdots, q_n, \alpha\big]} \\ &= \frac{\alpha\big[q_0, q_1, q_2, \cdots, q_n\big] + \big[q_0, q_1, \cdots, q_{n-1}\big]}{\alpha\big[q_1, q_2, \cdots, q_n\big] + \big[q_1, q_2, \cdots, q_{n-1}\big]} \\ &= \frac{\alpha A_n + A_{n-1}}{\alpha B_n + B_{n-1}} \end{aligned}$$

Thus, α satisfies

$$B_n\alpha^2 - (A_n - B_{n-1})\alpha - A_{n-1} = 0. \tag{8.6}$$

If the periodic continued fraction $\overline{q_n, \cdots, q_0}$ represent the quadratic irrational β, then ,

$$\begin{aligned} \beta &= \frac{\big[q_n, q_{n-1}, \cdots, q_0, \beta\big]}{\big[q_1, q_2, \cdots, q_n, \beta\big]} \\ &= \frac{\beta\big[q_n, q_{n-1}, q_2, \cdots, q_0\big] + \big[q_n, q_2, \cdots, q_1\big]}{\beta\big[q_{n-1}, \cdots, q_0\big] + \big[q_{n-1}, q_2, \cdots, q_1\big]} \\ &= \frac{\beta A_n + B_n}{\beta A_{n-1} + B_{n-1}}. \end{aligned}$$

Thus, β satisfies the equation

$$A_{n-1}\beta^2 - (A_n - B_{n-1})\beta - B_n = 0. \tag{8.7}$$

By comparing equations (8.6) and (8.7), we see that $-\frac{1}{\beta}$ is a root of (8.6). But α and β are positive (as $q_i \geq 1$ for all $i = 0, 1, \cdots, n$ for the purely periodic continued fractions). Hence $-\frac{1}{\beta}$ is negative and it must be the conjugate α' of α. □

Observe that $-1 < \alpha' < 0$, as $\beta > 1$. In other words, the conjugate of a quadratic irrational which is represented by a purely periodic continued fraction must lie stricylt betwen -1 and 0. We will term such irrational as '*reduced quadratic irrational*' and show that the converse also holds. In other words, any rduced quadratic irrational has a periodic continued fraction.,

8.5.2 Reduced Quadratic Irrational

DEFINITION 8.20. *Let α be a quadratic irrational satisfying the equation $ax^2+bx+c = 0$, where $a \neq 0$, b, c are rational numbers. Let α' be the conjugate of α. If $\alpha > 1$ and $-1 < \alpha' < 0$, then we say α is a reduced quadratic irrational.*

For example, $\sqrt{2}+1 > 1$ satisfies the equation $(x-1)^2 = 2$, i.e., $x^2 - 2x - 1 = 0$, and its conjugate is $-\sqrt{2}+1$, which lies between -1 and 0, hence $\sqrt{2}+1$ is a reduced quadratic irrational.

We will next show that reduced quadratic irrationals have very special continued fraction representing them. A reduced quadratic irrational has a continued fraction which is not just periodic, but it is periodic from the beginning, i.e., it is purely periodic continued fraction. First, we will prove only the periodicity.

LEMMA 8.21. *A reduced quadratic irrational has a periodic continued fraction.*

Proof: Let α be a quadratic irrational satisfying the equation $ax^2 + bx + c = 0$, where $a \neq 0,\ b,\ c$ can be taken as integers. Let $D = b^2 - 4ac$ and α' be the conjugate α. We can write

$$\alpha = \frac{P + \sqrt{D}}{Q},\ \ P, Q, D \in \mathbb{Z}$$

where we take the + sign for $\sqrt{D}$ by changing the sign of P and Q of necessary. It is not hard to see that $Q = 2a$ or $Q = -2a$. Now,

$$\alpha' = \frac{P - \sqrt{D}}{Q}.$$

As α is reduced, $\alpha > 1$ and $-1 < \alpha' < 0$. Now,

$$\begin{aligned}
\alpha - \alpha' > 0 &\implies \tfrac{2\sqrt{D}}{Q} > 0 &&\implies 0 < Q.\\
\alpha + \alpha' > 0 &\implies \tfrac{2P}{Q} > 0 &&\implies 0 < P.\\
\alpha' < 0 &\implies \tfrac{P-\sqrt{D}}{Q} < 0 &&\implies P < \sqrt{D}.\\
\alpha > 1 &\implies \tfrac{P+\sqrt{D}}{Q} > 1 &&\implies Q < P + \sqrt{D} < 2\sqrt{D}.\\
2a\alpha\alpha' = 2c \in \mathbb{Z} &\implies Q.\tfrac{P^2-D}{Q^2} \in \mathbb{Z} &&\implies P^2 - D \equiv 0 \bmod Q.
\end{aligned}$$

Let us now look at the continued fractionof α. Let q_0 be the integral part of α, then

$$\alpha = q_0 + \frac{1}{\alpha_1},\ \ \alpha_1 > 1.$$

By proposition 2.2, the conjugate of α will clearly be

$$\alpha' = q_0 + \frac{1}{\alpha_1'},$$

where α_1' is the conjugate of α_1. Moreover, α_1 will be reduced, as $\alpha' > 1$ and its conjugate α_1' satisfies

$$-1 < \frac{1}{\alpha' - q_0} = \alpha_1' < 0,\ \ \text{as } \alpha' < 0 < q_0.$$

Now,

$$\frac{1}{\alpha_1} = \alpha - q_0 = \frac{P - q_0 Q + \sqrt{D}}{Q}.$$

Let $P_1 = -P + q_0 Q$, then

$$\alpha_1 = \frac{Q}{-P_1 + \sqrt{D}} = \frac{Q(-P_1 - \sqrt{D})}{P_1^2 - D}.$$

As $P_1 \equiv -P \bmod Q$, and $P^2 - D$ is divisible by Q, we have $P_1^2 - D = -QQ_1$ for some positive integer Q_1. Thus,

$$\alpha_1 = \frac{Q(-P_1 - \sqrt{D})}{P_1^2 - D} = \frac{P_1 + \sqrt{D}}{Q_1}.$$

As α_1 is reduced, we will again have

$$0 < P_1 < \sqrt{D}, \;\; 0 < Q_1 < 2\sqrt{D}, \;\; P_1^2 - D \equiv 0 \bmod Q_1.$$

Proceeding in this way, the n-th complete quotient α_n will also turn out to be a reduced quadratic irrational, and

$$\alpha_n = \frac{P_n + \sqrt{D}}{Q_n}, \;\; 0 < P_n < \sqrt{D}, \;\; 0 < Q_n < 2\sqrt{D}, \;\; P_n^2 - D \equiv 0 \bmod Q_n.$$

Since there are only finitely many such pairs of integers P_n and Q_n, we will have repetition after some stage, and α_l will equal α_m for some integers $m > l$. Thus, the continued fraction of α will be periodic. $\square$

8.6 Lecture 6

Preamble: We will show that a reduced quadratic irrational has a purely periodic continued fraction, periodic from the beginning. Then we will show that any quadratic irrational has periodic continued fraction.

Keywords: reduced quadratic irrational

8.6.1 Continued Fractions of Reduced Quadratic Irrationals

Our goal is to prove that any quadratic irrational has periodic continued fraction. First, we will look at the special case of reduced quadratic irrational α with its conjugate α' satisfying $-1 < \alpha' < 0$ and $\alpha > 1$. In the previous lecture, we showed that such an α has periodic continued fraction. Now, we will first show that a reduced quadratic irrational has continued fraction which is periodic from the beginning.

THEOREM 8.22. *Let α be a reduced quadratic irrational. Then it is represented by a purely periodic continued fraction.*

Proof: Let α be a reduced quadratic irrational. If α_n denotes the n-th complete quotient of α, it will be enough to show that

$$\alpha_n = \alpha_m (n > m) \implies \alpha_{n-1} = \alpha_{m-1}.$$

Let

$$\alpha_{n-1} = q_{n-1} + \frac{1}{\alpha_n}, \;\; \alpha_{m-1} = q_{m-1} + \frac{1}{\alpha_m}.$$

It is enough to show that $q_{n-1} = q_{m-1}$. Let α'_n be the conjugate of α and $\beta_n = -\frac{1}{\alpha'_n}$. In the proof of the lemma in the previous lecture, we saw that each complete quotient α_n of α is reduced. Now,

$$\alpha'_{n-1} = q_{n-1} + \frac{1}{\alpha'_n} \implies \beta_n = q_{n-1} + (-\alpha'_{n-1}).$$

As $-1 < \alpha'_{n-1} < 0$, q_{n-1} is the integral part of β_n. But

$$\alpha_n = \alpha_m \implies \alpha'_n = \alpha'_m \implies \beta_n = \beta_m \implies q_{n-1} = q_{m-1}. \;\; \square$$

8.6.2 Continued Fraction for $\sqrt{N}$

Let N be a natural number which is not a perfect square. Then the following theorem tells us that the continued fraction of $\sqrt{N}$ also behaves nicely.

THEOREM 8.23. *The continued fraction of $\sqrt{N}$ is periodic with period $q_0,\ q_1,\ \cdots,\ q_n,\ 2q_0$, where $q_1 = q_n$, $q_2 = q_{n-2}$ and so on.*

Proof: The conjugate of $\sqrt{N}$ is $-\sqrt{N}$ which is strictly less than 1, hence $\sqrt{N}$ is not a reduced quadratic irrational. Let q_0 be the integral part of $\sqrt{N}$. Then we can easily see that $q_0 + \sqrt{N}$ is a reduced quadratic irrational. Clearly, $\alpha = q_0 + \sqrt{N} > 1$ and its conjugate $\alpha' = q_0 - \sqrt{N}$ lies strictly between -1 and 0. The integral part α is $2q_0$. Let $\alpha = \sqrt{N} + q_0$ be represented by the purely periodic continued fraction with period $2q_0, q_1, \cdots, q_n$. Then, the purely periodic continued fraction with the reverse period $q_n, q_{n-1}, \cdots, q_1, 2q_0$ represents

$$-\frac{1}{\alpha'} = -\frac{1}{-\sqrt{N}+q_0} = \frac{1}{\sqrt{N}-q_0} = q_1 + \frac{1}{q_2+}\frac{1}{q_3+}\cdots\frac{1}{q_n+}.$$

Since the continued fraction representation of $\alpha = -\frac{1}{\alpha'}$ is unique, we must have $q_1 = q_n$, $q_2 = q_{n-2}$, etc. $\square$

For example, $\sqrt{6} = 2, \overline{2,4}$:

$$\begin{aligned}
\sqrt{6} &= 2 + \sqrt{6} - 2 = 2 + \frac{1}{\frac{1}{\sqrt{6}-2}} = 1 + \frac{1}{\frac{\sqrt{6}+2}{2}} \\
&= 1 + \frac{1}{2 + \frac{\sqrt{6}-2}{2}} = 1 + \frac{1}{2 + \frac{1}{\sqrt{6}+2}} \\
&= 1 + \frac{1}{2 + \frac{1}{4+\sqrt{6}-2}} \\
&= 2, \overline{2,4}.
\end{aligned}$$

8.6.3 Continued Fraction for Any Quadratic Irrational

We have already seen that a periodic continued fraction represents a quadratic irrational. We will now show that the converse is also true. The converse is known as Lagrange's

theorem.

THEOREM 8.24. *A quadratic irrational α is represented by a periodic continued fraction.*

Proof: Let $\frac{A_n}{B_n}$ denote the n-th convergent of α, and let α_n denote the n-th complete quotient of α. It is enough to show that α_n is a reduced quadratic irrational for some natural number n. Then, the continued fraction will be periodic from that step. Now we have to show that there is an integer n for which the conjugate α'_{n+1} of the n-th complete quotient α_{n+1} satisfies $-1 < \alpha'_{n+1} < 0$. Now

$$\alpha = \frac{\alpha_{n+1}A_n + A_{n-1}}{\alpha_{n+1}B_n + B_{n-1}}.$$

If α' is the conjugates of α, then

$$\alpha' = \frac{\alpha'_{n+1}A_n + A_{n-1}}{\alpha'_{n+1}B_n + B_{n-1}}$$

because A_n, A_{n-1}, B_n, B_{n-1} are all integers. Solving the above for α'_{n+1} in terms of α', we obtain

$$\alpha'_{n+1} = -\frac{B_{n-1}\alpha' - A_{n-1}}{B_n\alpha' - A_n} = -\frac{B_{n-1}}{B_n} \cdot \left(\frac{\alpha' - \frac{A_{n-1}}{B_{n-1}}}{\alpha' - \frac{A_n}{B_n}}\right).$$

We know that $\frac{A_n}{B_n}$ approach α as n increases. Hence, the fraction in brackets approach 1 as n increases. Hence sign of the right hands side in the above equality is determined by the sign of $-\frac{B_{n-1}}{B_n}$, which is negative as $0 < B_{n-1} < B_n$. Thus, $\alpha'_{n+1} < 0$ for all sufficiently large integer n.

Recall that if n is even, then

$$\frac{A_n}{B_n} < \alpha < \frac{A_{n-1}}{B_{n-1}}.$$

Hence

$$\left(\frac{\alpha' - \frac{A_{n-1}}{B_{n-1}}}{\alpha' - \frac{A_n}{B_n}}\right) < 1$$

for any sufficiently large even integer n, and

$$\alpha'_{n+1} = -\frac{B_{n-1}}{B_n} \cdot \left(\frac{\alpha' - \frac{A_{n-1}}{B_{n-1}}}{\alpha' - \frac{A_n}{B_n}}\right) < -1.$$

Therefore, by choosing a sufficiently large even integer n, we can conclude that α_{n+1} satisfies $-1 < \alpha'_{n+1} < 0$. Thus we have proved that α_{n+1} is a reduced quadratic irrational, and its continued fraction is purely periodic continued fraction. Consequently, α has a periodic continued fraction. □

8.7 Lecture 7

Preamble: We will show that the best approximation to a quadratic irrational by a rational sequence is given by the convergents of the infinite continued fraction of the irrational.

Keywords: best approximation to a quadratic irrational

8.7.1 Best Rational Approximation to an Irrational

We will show that the best rational approximation to an irrational number is given by the convergents of its continued fraction.

THEOREM 8.25. *Let x be an irrational number, and $\frac{A_n}{B_n}$ be a convergent of its continued fraction. Then $\frac{A_n}{B_n}$ is the closest rational number to x amongst all rational numbers $\frac{a}{b}$ with denominators $b \leq B_n$, i.e.,*

$$| x - \frac{A_n}{B_n} | \leq | x - \frac{a}{b} | \qquad a,\ b \in \mathbb{Z},\ \ 1 \leq b < B_n.$$

We will first prove the following lemma:

LEMMA 8.26. *If $\frac{A_i}{B_i}$ denotes the i-th convergent of an irrational number x then for any $a,\ b \in \mathbb{Z}$ satisfying $1 \leq b < B_{n+1}$, we have*

$$| B_n x - A_n | \ \leq \ | bx - a | .$$

Proof: Note that x lies between $\frac{A_n}{B_n}$ and $\frac{A_{n+1}}{B_{n+1}}$, so that $B_n x - A_n$ and $B_{n+1}x - A_{n+1}$ have opposite signs. If we can can express

$$b = B_n\alpha + B_{n+1}\beta \tag{8.8}$$
$$a = A_n\alpha + A_{n+1}\beta, \tag{8.9}$$

where $\alpha \neq 0$ and β are integers of opposite signs (except when $\beta = 0$), then we can write

$$\begin{aligned} | bx - a | &= | \alpha(B_n x - A_n) + \beta(B_{n+1}x - A_{n+1}) | \\ &= | \alpha(B_n x - A_n) | + | \beta(B_{n+1}x - A_{n+1}) | \\ &= | \alpha | \ | (B_n x - A_n) | + | \beta | \ | (B_{n+1}x - A_{n+1}) | \\ &\geq | \alpha | \ | (B_n x - A_n) | \\ &\geq | (B_n x - A_n) | . \end{aligned}$$

The coefficients in (8.8) satisfy $A_{n+1}B_n - A_nB_{n+1} = (-1)^n$, hence we can solve the system and obtain,

$$\alpha = (-1)^n(A_{n+1}b - B_{n+1}a) \quad \beta = (-1)^n(A_nb - B_na).$$

If $\alpha = 0$, then $b = B_{n+1}\beta$, hence $\beta > 0$ and $b \geq B_{n+1}$, which is a contradiction. Now, $\beta = 0$ implies $b = B_n\alpha$, and $a = A_n\alpha$, and the inequality in the lemma follows easily. Suppose $\beta > 0$. Then $B_n\alpha + B_{n+1}\beta = b < B_{n+1}$ implies $B_n\alpha < 0$ hence $\alpha < 0$. If $\beta < 0$, then $B_n\alpha + B_{n+1}\beta = b \geq 1$ implies $B_n\alpha > 0$, i.e., $\alpha > 0$. Thus, either $\beta = 0$ or α and β have opposite signs, and the inequality in the lemma follows. □

Proof of the theorem: Consider a rational number $\frac{a}{b}$ where a is any integer and $1 \leq b < B_n (< B_{n+1})$. By the previous lemma, we have

$$\begin{array}{rrcl} & \mid B_nx - A_n \mid & \leq & \mid bx - a \mid \\ \Longrightarrow & \mid B_n \mid \mid x - \frac{A_n}{B_n} \mid & \leq & \mid b \mid \mid x - \frac{a}{b} \mid \\ \Longrightarrow & \mid x - \frac{A_n}{B_n} \mid & \leq & \mid \frac{b}{B_n} \mid \mid x - \frac{a}{b} \mid \\ \Longrightarrow & \mid x - \frac{A_n}{B_n} \mid & \leq & \mid x - \frac{a}{b} \mid, \end{array}$$

as $\frac{b}{B_n} \leq 1$. □

8.7.2 A Sufficiently Close Rational is a Convergent

Let x be an irrational number, and let $\frac{a}{b}$ be a rational number. If $\frac{a}{b}$ is sufficiently close to x, we can show that $\frac{a}{b}$ has to be a convergent of the continued fraction of x.

PROPOSITION 8.27. *Let $\frac{a}{b}$ be a rational number with $1 \leq b$, $gcd(a, b) = 1$ and*

$$\mid \frac{a}{b} - x \mid \; < \; \frac{1}{2b^2}.$$

Then, $\frac{a}{b}$ is a convergent of the continued fraction of x.

Proof: As the denominator B_i of convergents $\frac{A_i}{B_i}$ forms an increasing sequence of integers, we have $B_n \leq b < B_{n+1}$ for some n. Suppose, $\frac{a}{b} \neq \frac{A_n}{B_n}$, i.e., $\mid aB_n - bA_n \mid \geq 1$. As

$b < B_{n+1}$, by the preceding lemma we have

$$\begin{aligned}
& | B_n x - A_n | && \leq && | bx - a | < b.\frac{1}{2b^2} = \frac{1}{2b} \\
\Longrightarrow \quad & | x - \tfrac{A_n}{B_n} | && \leq && \frac{1}{2bB_n} \\
\Longrightarrow \quad & | \tfrac{a}{b} - x | + | x - \tfrac{A_n}{B_n} | && < && \frac{1}{2b^2} + \frac{1}{2bB_n} \\
\Longrightarrow \quad & | \tfrac{a}{b} - \tfrac{A_n}{B_n} | && \leq && | \frac{a}{b} - x | + | x - \frac{A_n}{B_n} | < \frac{1}{2b^2} + \frac{1}{2bB_n} \\
\Longrightarrow \quad & \tfrac{|aB_n - bA_n|}{|bB_n|} && < && \frac{1}{2b^2} + \frac{1}{2bB_n} \\
\Longrightarrow \quad & \tfrac{1}{bB_n} && < && | \frac{aB_n - bA_n}{bB_n} | < \frac{1}{2b^2} + \frac{1}{2bB_n} \\
\Longrightarrow \quad & b && < && B_n,
\end{aligned}$$

which is a contradiction. □

8.8 Lecture 8

Preamble: In the previous lectures, we have seen that the continued fraction of $\sqrt{N}$ has a very special periodic form for any natural number N. As an application, we will now show how to solve a classical Diophantine equation of degree 2, which is known as Pells's equation. Solution of Pell's equations are very much related with the question of finding units in a special class of rings.

Keywords: Pells' equation, fundamental solution

8.8.1 Pell's Equation

DEFINITION 8.28. *Let N be natural number which is not a square. The quadratic Diophantine equation in two variables*

$$x^2 - Ny^2 = 1.$$

is known as Pell's equation.

We are interested in finding all the integers x, y satisfying the above equation. We will show that the solutions are very much related to the continued fractionof $\sqrt{N}$.

PROPOSITION 8.29. *Let a and b be two positive integers such that $a^2 - Nb^2 = 1$. Then $\frac{a}{b}$ must be a convergent of the continued fractionof $\sqrt{N}$.*

Proof: First observe that $(a - b\sqrt{N})(a + b\sqrt{N}) = 1$ implies $a > b\sqrt{N}$.

$$\begin{aligned} a^2 - Nb^2 &= 1 \\ \implies (a - b\sqrt{N})(a + b\sqrt{N}) &= 1 \\ \implies \frac{a}{b} - \sqrt{N} &= \frac{1}{b(a + b\sqrt{N})} \\ \implies \mid \frac{a}{b} - \sqrt{N} \mid &< \frac{1}{b(b\sqrt{N} + b\sqrt{N})} \\ \implies \mid \frac{a}{b} - \sqrt{N} \mid &< \frac{1}{2b^2}. \end{aligned}$$

Hence, $\frac{a}{b}$ must be a convergent of $\sqrt{N}$. □

We will now try to identify precisely which of the convergents of $\sqrt{N}$ give rise to solutions of the Pell's equation $x^2 - Ny^2 = 1$.

PROPOSITION 8.30. *Let $\sqrt{N} = \overline{q_0,\ q_1,\ \cdots,\ q_n,\ 2q_0}$, and let $\frac{A_i}{B_i}$ denote the i-th convergent of $\sqrt{N}$. Then*

$$A_{n-1}^2 - dB_{n-1}^2 = (-1)^{n-1}.$$

Proof: Let α_{n+1} be the complete quotient after q_n in the continued fractionof $\sqrt{N}$. Then,

$$\sqrt{N} = \frac{\alpha_{n+1}A_n + A_{n-1}}{\alpha_{n+1}B_n + B_{n-1}},$$

and

$$\alpha_{n+1} = 2q_0 + \frac{1}{q_1 +} \cdots = q_0 + \sqrt{N}.$$

Therefore, substituting for α_{n+1}, we obtain

$$\begin{aligned}
\sqrt{N} &= \frac{(q_0 + \sqrt{N})A_n + A_{n-1}}{(q_0 + \sqrt{N})B_n + B_{n-1}} \\
\implies \sqrt{N}(q_0 + \sqrt{N})B_n + \sqrt{N}B_{n-1} &= (q_0 + \sqrt{N})A_n + A_{n-1} \\
\implies NB_n + \sqrt{N}(q_0B_n + B_{n-1}) &= q_0A_n + A_{n-1} + \sqrt{N}A_n. \\
\implies NB_n = q_0A_n + A_{n-1}, &\quad q_0B_n + B_{n-1} = A_n \\
\implies A_{n-1} &= NB_n - q_0A_n, \\
B_{n-1} &= A_n - q_0B_n.
\end{aligned}$$

Recall the relation

$$A_nB_{n-1} - A_{n-1}B_n = (-1)^{n-1}.$$

Substituting, we obtain

$$\begin{aligned}
A_n(A_n - q_0B_n) - (NB_n - q_0A_n)B_n &= (-1)^{n-1} \\
A_n^2 - NB_n^2 &= (-1)^{n-1}. \qquad \square
\end{aligned}$$

THEOREM 8.31. *Let $\sqrt{N}$ be a natural number which is not a square. Let*

$$\sqrt{N} = \overline{q_0,\ q_1,\ \cdots,\ q_n,\ 2q_0},$$

and let $\frac{A_i}{B_i}$ denote the i-th convergent of $\sqrt{N}$. If n is odd, then $x = A_n,\ y = B_n$ is a solution of the Pell's equation $x^2 - Ny^2 = 1$. If n is even, then $x = A_{2n+1},\ y = B_{2n+1}$ is a solution of $x^2 - dy^2 = 1$.

Proof: The case when n is odd follows straightway from the previous proposition. If n is even, then observe that

$$\sqrt{N} = \overline{q_0,\ q_1,\ \cdots,\ q_n,\ 2q_0} = q_0,\ q_1,\ \cdots,\ q_n,\ 2q_0, \overline{q_0,\ q_1,\ \cdots,\ q_n,\ 2q_0}.$$

Hence, we can consider the convergents $\frac{A_{2n+1}}{B_{2n+1}}$ and $\frac{A_{2n}}{B_{2n}}$ at the end of the next period in the previous proposition to obtain

$$A_{2n+1}^2 - NB_{2n+1}^2 = (-1)^{2n} = 1. \qquad \square$$

8.8.2 Fundamental Solution

DEFINITION 8.32. *Consider Pell's equation $x^2 - Ny^2 = 1$. A solution a, b where a, b are both positive is called a positive solution. A positive solution a, b is called the fundamental solution of the equation if $a < \alpha$ and $b < \beta$ for any other solution α, β.*

Note that if a, b and $\alpha, \beta$are two solutions, then $a < \alpha \Leftrightarrow b < \beta$ as $\alpha^2 - a^2 = N(\beta^2 - b^2)$, and $N \in \mathbb{N}$. Fundamental solution is important, as one can obtain all other solutions of Pell's equation from the fundamental solution.

PROPOSITION 8.33. *Let x_1, y_1 denote the fundamental solution of $x^2 - Ny^2 = 1$. Let*

$$x_n + y_n\sqrt{N} = (x_1 + y_1\sqrt{N})^n, \qquad n \in \mathbb{N}$$

Then x_n, y_n is a positive solution of $x^2 - Ny^2 = 1$.

Proof:

$$\begin{aligned} x_n^2 - Ny_n^2 &= \left(x_n + y_n\sqrt{N}\right)\left(x_n - \sqrt{N}y_n\right) \\ &= \left(x_1 + y_1\sqrt{N}\right)^n\left(x_1 - y_1\sqrt{N}\right)^n \\ &= \left(x_1^2 - Ny_1^2\right)^n = 1. \qquad \square \end{aligned}$$

The next theorem shows that every positive solution of Pell's equation can be obtained from some power of the fundamental solution.

THEOREM 8.34. *Let x_1, y_1 denote the fundamental solution and u, v be any positive solution of $x^2 - Ny^2 = 1$. Then, there is a natural number n such that*

$$u + v\sqrt{N} = (x_1 + y_1\sqrt{N})^n.$$

Proof: Suppose $u+v\sqrt{N}$ does not equal $(x_1+y_1\sqrt{N})^m$ for any m. Then we can show the existence of a solution smaller than the fundamental solution, which is a contradiction. As $x_1 + y_1\sqrt{N} > 1$, we must have

$$(x_1 + y_1\sqrt{N})^n \;<\; u + v\sqrt{N} \;<\; (x_1 + y_1\sqrt{N})^{n+1}$$

for some n. It follows that

$$x_n + y_n\sqrt{N} \;<\; u + v\sqrt{N} \;<\; (x_n + y_n\sqrt{N})(x_1 + y_1\sqrt{N}).$$

As $(x_n - y_n\sqrt{N}) > 0$ for the positive solution $x_n + y_n\sqrt{N}$, we can multiply the previous inequalities with $(x_n - y_n\sqrt{N})$ and obtain

$$\begin{aligned}(x_n + y_n\sqrt{N})(x_n - y_n\sqrt{N}) &< (u + v\sqrt{N})(x_n - y_n\sqrt{N}) \\ &< (x_n + y_n\sqrt{N})(x_n - y_n\sqrt{N})(x_1 + y_1\sqrt{N}).\end{aligned}$$

It follows that

$$1 < (ux_n - Nvy_n) + (vx_n - uy_n)\sqrt{N} < x_1 + y_1\sqrt{N}.$$

But $ux_n - Nvy_n$, $vx_n - uy_n$ clearly satisfies $x^2 - Ny^2 = 1$, as

$$(ux_n - Nvy_n)^2 - N(vx_n - uy_n)^2 = (u^2 - Nv^2)(x_n^2 - Ny_n^2) = 1.$$

Thus, we would obtain a solution smaller than the fundamental solution if $u + v\sqrt{N}$ is not a power of the fundamental solution. □

Example: Find all the solutions of the Diophantine equation

$$x^2 - 6y^2 = 1.$$

Solution: We have seen that the continued fraction of $\sqrt{6}$ is $\overline{2, 2, 4}$. Hence A_2, B_2 will be the fundamental solution, where

$$\frac{A_2}{B_2} = 2 + \frac{1}{2} = \frac{5}{2}.$$

We can verify that $5^2 - 6.2^2 = 1$. Any other (positive) solution can be obtained by taking powers $(5 + 2\sqrt{6})$. For example, $(5 + 2\sqrt{6})^2 = 49 + 20\sqrt{6}$ indicates that 49, 20 is another solution. □

8.9 Exercises

1. Find the continued fraction expansion of the following rational numbers:

$$\frac{23}{5}, \quad \frac{72}{11}, \quad \frac{56}{13}.$$

2. Find the continued fraction expansion of the following irrational numbers:

$$\sqrt{5}, \quad \sqrt{7}, \quad \sqrt{10}, \quad \sqrt{11}, \quad \sqrt{37}.$$

3. Determine the first four convergents of each of the continued fractions above.

4. Determine the real numbers represented by the following periodic continued fractions:

   (A) $2; \overline{1, 2, 4}$

   (B) $\overline{2, 3, 4}$

   (C) $3; \overline{1, 3, 6}$

5. (A) Determine the real numbers represented by the following periodic continued fractions:

$$(i) \ \overline{1, 2, 3}, \qquad (ii) \ \overline{3, 2, 1}, \qquad (iii) \ 3; \overline{3, 2, 1}, \qquad (iv) \ 3; \overline{1, 2, 3}.$$

   (B) Verify which one of those real numbers are reduced quadratic irrationals.

6. (A) Determine whether the following numbers are reduced quadratic irrationals:

$$(i) \ \frac{1 + \sqrt{5}}{2}, \quad (ii) \ 3 + \sqrt{10}, \quad (iii) \ 2 + \sqrt{10}, \quad (iv) \ \frac{2 + \sqrt{10}}{2}.$$

   (B) Find the continued fraction of each of the reduced quadratic irrationals above.

   (C) Verify that their continued fractions are purely periodic.

7. Let n be any positive integer.

   (A) Show that the continued fraction of $\sqrt{n^2 + 1}$ is given by $n; \overline{2n}$.

   (B) Show that the continued fraction of $\sqrt{n^2 + 2}$ is given by $n; \overline{n, 2n}$.

   (C) Show that the continued fraction of $\sqrt{n^2 + 2n}$ is given by $n; \overline{1, 2n}$.

   (D) Verify the above results by directly computing the continued fraction of $\sqrt{17}$, $\sqrt{11}$ and $\sqrt{15}$.

8. (A) Show that
$$| \sqrt{7} - \frac{8}{3} | < \frac{1}{2.3^2}.$$
   (B) Confirm directly that $\frac{8}{3}$ appear as a convergent in the continued fraction of $\sqrt{7}$.

9. Find all the solutions of the following linear Diophantine equation using continued fraction:
$$52x - 92y = 100.$$

10. Find a pair of integers x and y satisfying
$$x^2 - 5y^2 = 1.$$

11. Find the fundamental solution of
$$x^2 - 37y^2 = 1.$$

12. Determine all integers x and y satisfying
$$x^2 - 10y^2 = 1.$$

13. (A) By hit and trial, find a pair of integers x and y satisfying
$$x^2 - 10y^2 = 6.$$
   (B) Can you find four other pairs of solutions?
   (C) Can you prove that there are infinitely many solutions?

14. Show that if $x^2 - Ny^2 = -1$ has a solution in integers for a positive integer N, then N can not be divisible by a prime of the form $4k + 3$.

Module 9

Riemann Zeta Function

9.1 Lecture 1

Preamble: In this lecture, we will introduce Riemann zeta function. The theory of infinite series and results from real and complex analysis will also be used in this part of the course.

Keywords: Riemann zeta function

9.1.1 Riemann Zeta Function

Recall that an infinite series is an infinite sum of the form

$$\sum_{n=1}^{\infty} a_n = a_0 + a_1 + a_2 + \cdots,$$

where a_i are complex numbers. One of the most familiar infinite series is the harmonic series, defined as

$$\sum_{n=1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots.$$

Riemann considered a more general series, where the terms $\frac{1}{n}$ is replaced by $\frac{1}{n^s}$, where s is a variable that takes complex values:

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots. \tag{9.1}$$

We will show that the series converges absolutely for all complex values s with real part $Re(s) > 1$. Thus, the series represents an analytic function for $Re(s) > 1$. This function can be extended to the whole complex plane (i.e., for $Re(s) \leq 1$). The extended function is analytic everywhere except at $s = 1$, where it has a simple pole of residue 1. This function is known as the *Riemann zeta function*, and is denoted by $\zeta(s)$. Thus, the Riemann zeta function can be defined as the function

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$$

when $Re(s) > 1$. For $Re(s) \leq 1$, $\zeta(s)$ is not defined by the series, but by its meromorphic continuation. Riemann discovered many interesting properties of this function in the later half of the nineteenth century. Much before Riemann, Euler studied this function, and obtained various significant results.

9.1.2 Convergence

PROPOSITION 9.1. *The infinite series*

$$1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$$

converges absolutely for all complex values of s with $Re(s) > 1$.

Proof: Let s be a complex number with real part r and imaginary part t, i.e., $s = r + it$. Observe that for any real number t,

$$\begin{aligned} n^{it} &= e^{\log_e(n^{it})} \\ &= e^{it \log_e n} \\ &= \cos(t \log_e n) + i \sin(t \log_e n) \\ \Longrightarrow \mid n^{it} \mid &= \cos^2(t \log_e n) + \sin^2(t \log_e n) = 1. \end{aligned}$$

Therefore,

$$\mid \frac{1}{n^s} \mid = \frac{1}{\mid n^r \mid \mid n^{it} \mid} = \frac{1}{n^r}.$$

It suffices to show the sequence S_n of partial sums of the series

$$1 + \frac{1}{2^r} + \frac{1}{3^r} + \frac{1}{4^r} + \cdots$$

converges for $r > 1$. Since the above series consists of positive real terms, it is enough to show that the subsequence S_{2^n-1} of partial sums is convergent, where

$$S_{2^n-1} = 1 + \frac{1}{2^r} + \frac{1}{3^r} + \frac{1}{4^r} + \cdots + \frac{1}{(2^n-1)^r}.$$

Now,

$$\begin{aligned} S_{2^n-1} &= 1+\left[\frac{1}{2^r}+\frac{1}{3^r}\right]+\left[\frac{1}{4^r}+\frac{1}{5^r}+\frac{1}{6^r}+\frac{1}{7^r}\right]+\cdots+\left[\frac{1}{(2^{n-1})^r}+\cdots+\frac{1}{(2^n-1)^r}\right] \\ &< 1+\left[\frac{1}{2^r}+\frac{1}{2^r}\right]+\left[\frac{1}{4^r}+\frac{1}{4^r}+\frac{1}{4^r}+\frac{1}{4^r}\right]+\cdots+\left[\frac{1}{(2^{n-1})^r}+\cdots+\frac{1}{(2^{n-1})^r}\right] \\ &= 1+\frac{2}{2^r}+\frac{4}{4^r}+\cdots+\frac{2^{n-1}}{(2^{n-1})^r} \\ &= 1+\frac{1}{2^{r-1}}+\frac{1}{4^{r-1}}\cdots+\frac{1}{(2^{n-1})^{r-1}} \end{aligned}$$

The sum on the right is the sequence of partial sums of a geometric series with common ration $\frac{1}{2^{r-1}}$, and the geometric series converges for $r > 1$. Hence the subsequence S_{2^n-1} of partial sums is convergent. We can conclude that the series in the theorem converges absolutely for $Re(s) > 1$. □

When s is a real number less than 1, it is easy to see that the series (9.2) diverges.

PROPOSITION 9.2. *Let r be a real number with $r \leq 1$. Then the series*

$$\sum_{n=1}^{\infty}\frac{1}{n^r} = 1+\frac{1}{2^r}+\frac{1}{3^r}+\frac{1}{4^r}+\cdots$$

diverges.

Proof: If $r \leq 0$, the n-th term of the above series is $\frac{1}{n^r} \geq 1$, and hence the n-th term does not approach 0 as n approach infinity. Hence the series clearly diverges for $r \leq 0$. Since the given series is a series of positive terms, it is enough to show that the subsequence $S_{2^{n-1}}$ of partial sums given by

$$S_{2^{n-1}} = 1+\frac{1}{2^r}+\frac{1}{3^r}+\frac{1}{4^r}+\cdots+\frac{1}{(2^n)^r}.$$

diverges. Now, noting that $\frac{1}{n^r} \geq \frac{1}{n}$ for $r \leq 1$,

$$\begin{aligned} S_{2^n} &= 1+\frac{1}{2^r}+\left[\frac{1}{3^r}+\frac{1}{4^r}\right]+\left[\frac{1}{5^r}+\frac{1}{6^r}+\frac{1}{7^r}+\frac{1}{8^r}\right]+\cdots+\left[\frac{1}{(2^{n-1}+1)^r}+\cdots+\frac{1}{(2^n)^r}\right] \\ &> 1+\frac{1}{2}+\left[\frac{1}{4}+\frac{1}{4}\right]+\left[\frac{1}{8}+\frac{1}{8}+\frac{1}{8}+\frac{1}{8}\right]+\cdots+\left[\frac{1}{2^n}+\cdots+\frac{1}{2^n}\right] \\ &= 1+\frac{1}{2}+\frac{2}{4}\cdots+\frac{2^{n-1}}{2^n} \\ &= \frac{n}{2}. \end{aligned}$$

Hence, the given series diverges for real numbers $r \leq 1$. □

9.1.3 Euler Product

It was Euler who studies the series (9.2) much before Riemann. He found that the series can also be expressed as an infinite product of factors, one for each prime p. The expression is known as the Euler product.

THEOREM 9.3. *For $Re(s) > 1$,*

$$\zeta(s) = \prod_p \Big(\frac{1}{1-p^{-s}}\Big) = \prod_p \Big(1-p^{-s}\Big)^{-1}.$$

Proof: First observe that

$$\frac{1}{1-p^{-s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots,$$

where the RHS is an infinite geometric series with common ration p^{-s}, and the series converges absolutely to $\zeta(s)$ as $\mid\ p^{-s}\ \mid = p^{-Re(s)} < 1$. Let $\{p_1, \cdots, p_k\}$ be the first k primes, and

$$P_k(s) = \prod_{i=1}^{k} \Big(\frac{1}{1-p_i^{-s}}\Big) = \prod_{i=1}^{k} \Big(1 + \frac{1}{p_i^s} + \frac{1}{p_i^{2s}} + \cdots\Big).$$

We have to show that $P_k(s)$ approaches $\zeta(s)$ as k approaches infinity. By the fundamental theorem of arithmetic, any natural number can be uniquely written as a product of prime powers. Let $N_k = \{p_1^{e_1}.\cdots.p_k^{e_k} \mid\ e_i \geq 0\}$ be the set of natural numbers which can be written as a product of power of the first k primes. Then we have

$$P_k(s) = \prod_{i=1}^{k} \Big(1 + \frac{1}{p_i^s} + \frac{1}{p_i^{2s}} + \cdots\Big) = \sum_{e_i \geq 0} \frac{1}{(p_1^{e_1}.\cdots.p_k^{e_k})^s} = \sum_{n \in N_k} \frac{1}{n^s}.$$

Now, $n \notin N_k$ implies $n > p_k$.

$$\begin{aligned}
\mid\ P_k(s) - \zeta(s)\ \mid &= \mid\ \zeta(s) - \sum_{n \in N_k} \frac{1}{n^s}\ \mid \\
&= \mid \sum_{n \notin N_k} \frac{1}{n^s}\ \mid \\
&\leq \mid \sum_{n > p_k} \frac{1}{n^s}\ \mid \\
&= \mid\ \zeta(s) - \sum_{n > p_k} \frac{1}{n^s}\ \mid
\end{aligned}$$

As we have already seen that the series (9.2) converges absolutely to $\zeta(s)$ for $Re(s) > 1$, we must have the RHS above converge to 0 as k approaches infinity, hence

$$\lim_{k\to\infty} P_k(s) = \zeta(s). \qquad \square$$

9.1.4 Riemann Hypothesis

The function $\zeta(s)$ defined by the infinite series $\sum_{n=1}^{\infty} n^{-s}$ is analytic in the region $Re(s) > 1$ as we have shown. But it can be extended to the whole complex plane. The extended function satisfies the following relation involving the values at s and $1-s$:

$$\zeta(1-s) = 2(2\pi)^{-s}\Gamma(s)\cos\Big(\frac{\pi s}{2}\Big)\zeta(s),$$

where the $\Gamma(s)$ denotes the analytic continuation of the usual Gamma function defined by the improper integral

$$\Gamma(s) = \int_0^{\infty} x^{s-1}e^{-x}dx, \qquad Re(s) > 1.$$

It is clear from the above relation that $\zeta(-2k) = 0$ for $k = 1,\ 2,\ 3,\ \cdots$. These are known as the *trivial zeros* of the Riemann zeta function. In 1859, Riemann conjectured that all the other zeros of (the extended) $\zeta(s)$ lies on the line $Re(s) = \frac{1}{2}$. This conjecture is famously known as the Riemann Hypothesis, and is recognized as one of the seven Milennium problems with a million dollar prize-tag.

It is noteworthy that if we normalize $\zeta(s)$ as

$$\Lambda(s) = \pi^{\frac{-s}{2}}\Gamma\Big(\frac{s}{2}\Big)\zeta(s),$$

then we have

$$\Lambda(s) = \Lambda(1-s),$$

which is referred to as the functional equation for the Riemann zeta function. The values of the zeta function at even positive integers turn out to be a rational multiple of π^{2k}. More precisely,

$$\zeta(2k) = (-1)^{k+1}\frac{(2\pi)^{2k}B_{2k}}{2.(2k)!}, \qquad k = 1,\ 2,\ \cdots$$

where B_n denotes the n-th Bernoulii number, defined as coefficient of z^n in

$$\frac{z}{e^z - 1} = \sum_{n=0}^{\infty}\frac{B_n}{n!}z^n.$$

For example, we can easily compute that $B_2 = \frac{1}{4}$ and $B_4 = -\frac{1}{30}$. Hence, $\zeta(2) = \frac{\pi^2}{6}$ and $\zeta(4) = \frac{\pi^4}{90}$.

9.2 Lecture 2

Preamble: In this lecture, we will generalize the definition of Riemann Zeta function and introduce the Dirichlet series of an arithmetic function. We will discuss convergence of Dirichlet series. We will also show that if $f(mn) = f(m)f(n)$ for all integers m, n, then we obtain a Euler product formula for the Dirichlet series of f.

Keywords: Dirichlet series, completely multiplicative function, Euler product

9.2.1 Dirichlet series

Let $f : \mathbb{N} \longrightarrow \mathbb{C}$ be an arithmetic function. For any complex number s, one can define the infinite series

$$L(f,s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s} = 1 + \frac{f(1)}{2^s} + \frac{f(3)}{3^s} + \frac{f(4)}{4^s} + \cdots . \tag{9.2}$$

The series used in the definition of $\zeta(s)$ can be considered as the special case when the arithmetic function f is the constant function $f(n) = 1$ for all n. We will first prove that multiplication of two Dirichlet series corresponds to the convolution of the corresponding arithmetic functions:

THEOREM 9.4. *Let f and g be two arithmetic functions, and $h = f \star g$ be their convolution. Then,*

$$L(h,s) = L(f,s)L(g,s)$$

for all complex values of s for which the series $L(f,s)$ and $L(g,s)$ converge absolutely.

Proof: When the series $L(f,s)$ and $L(g,s)$ converge absolutely, we can multiply them

and rearrange the terms to obtain

$$\begin{aligned} L(f,s)L(g,s) &= \Big[\sum_{n=1}^{\infty}\frac{f(n)}{n^s}\Big]\Big[\sum_{m=1}^{\infty}\frac{g(m)}{m^s}\Big] \\ &= \sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\frac{f(n)g(m)}{(mn)^s} \\ &= \sum_{k=1}^{\infty}\sum_{nm=k}\frac{f(n)g(m)}{k^s} \\ &= \sum_{k=1}^{\infty}\frac{(f\star g)(k)}{k^s} \\ &= L(f\star g,s). \qquad \square \end{aligned}$$

For example, let us consider the Mobius function $\mu(n)$, the function $u(n)=1$ for all n, and the function I given by $I(n)=0$ for all $n\neq 0$, and $I(1)=1$. We have seen that $\mu\star u = I$. Also, the series

$$L(\mu,s)=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}$$

converges absolutely for $Re(s)>1$, as $|\frac{\mu(n)}{n^s}|\leq|\frac{1}{n^s}|$ for all n, and the zeta series converges absolutely for $Re(s)>1$. Thus,

$$\Big[\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}\Big].\Big[\sum_{n=1}^{\infty}\frac{1}{n^s}\Big]=1.$$

We obtain the interesting identity

$$\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}=\frac{1}{\zeta(s)} \qquad Re(s)>1.$$

9.2.2 Euler Product for Dirichlet Series

DEFINITION 9.5. *An arithmetic function $f:\mathbb{Z}\longrightarrow\mathbb{C}$ is called completely multiplicative if*

$$f(mn)=f(m)f(n) \qquad \forall m,\ n\in\mathbb{N}.$$

Examples:

1. The arithmetic function I where $I(n)=0$ when $n\neq 0$ and $I(1)=1$
2. The arithmetic function u: $u(n)=1$ for all n;

3. The arithmetic function N where $N(n) = n$ for all n.

But μ and ϕ are not completely multiplicative. Note that

$$\begin{aligned} 0 = \mu(9) &\neq \mu(3)\mu(3), \\ 4 = \phi(8) &\neq \phi(4)\phi(2) = 2.1. \end{aligned}$$

We have the following theorem.

THEOREM 9.6. *Let f be a multiplicative function and suppose the series $L(f,s)$ converges absolutely. Then,*

$$L(s,f) = \prod_p \Big(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots\Big).$$

If f is completely multiplicative, then we have a Euler product formula

$$L(s,f) = \prod_p \Big(\frac{1}{1 - f(p)p^{-s}}\Big) = \prod_p \Big(1 - f(p)p^{-s}\Big)^{-1}.$$

Proof: Let $\{p_1, \cdots, p_k\}$ be the first k primes, and let

$$Q_k(s) = \prod_{i=1}^{k} \Big(1 + \frac{f(p_i)}{p_i^s} + \frac{f(p_i^2)}{p_i^{2s}} + \cdots\Big).$$

We have to show that $Q_k(s)$ approaches $L(f,s)$ as k approaches infinity. By the fundamental theorem of arithmetic, any natural number can be uniquely written as a product of prime powers. Let $N_k = \{p_1^{e_1}.\cdots.p_k^{e_k} | e_i \geq 0\}$ be the set of natural numbers which

can be written as a product of power of the first k primes. Then we have

$$\begin{aligned} Q_k(s) &= \prod_{i=1}^{k} \Big(1 + \frac{f(p_i)}{p_i^s} + \frac{f(p_i^2)}{p_i^{2s}} + \cdots\Big) \\ &= \sum_{e_i \geq 0} \frac{f(p_1^{e_1}).\cdots.f(p_k^{e_k})}{(p_1^{e_1}.\cdots.p_k^{e_k})^s} \\ &= \sum_{e_i \geq 0} \frac{f(p_1^{e_1}.\cdots.p_k^{e_k})}{(p_1^{e_1}.\cdots.p_k^{e_k})^s} \\ &= \sum_{n \in N_k} \frac{f(n)}{n^s}. \\ \Rightarrow \quad |Q_k(s) - L(f,s)| &= |L(f,s) - \sum_{n \in N_k} \frac{f(n)}{n^s}| \\ &= |\sum_{n \notin N_k} \frac{f(n)}{n^s}| \\ &\leq |\sum_{n > p_k} \frac{f(n)}{n^s}| \\ &= |L(f,s) - \sum_{n \in N_k} \frac{f(n)}{n^s}| \end{aligned}$$

By our assumption on absolute convergence, we must have the RHS above converge to 0 as k approaches infinity, hence

$$\lim_{k \to \infty} Q_k(s) = L(f,s).$$

If f is completely multiplicative, we have

$$\begin{aligned} & 1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots \\ = \quad & 1 + f(p)p^{-s} + \big(f(p)p^{-s}\big)^2 + \cdots \\ = \quad & \big(1 - f(p)p^{-s}\big)^{-1}. \qquad \square \end{aligned}$$

Module 10

Additional Topics

10.1 Lecture 1

Preamble: Determining whether a given integer is prime or composite is knows as primality testing. There are primality tests which merely tells us whether a given integer is prime or not, without giving us the factors in case the given number is composite. There has been lot of progress in recent years in primality testing. In 2002, three Indian computer scientists found an algorithm to determine whether a given integer is prime or not. It is known as AKS algorithm, named after the three persons involved: Agarwal, Kayal and Saxena. but we are not going to elaborate on this algorithm. In this lecture we will discuss Lucas Test, and Miller-Rabin Test for primality .

Keywords: Lucas Test, Miller-Rabin Test

10.1.1 Lucas Test for primality

Lucas Test is based on Euler's theorem which states that if n is any integer and a is coprime to n, then

$$a^{\phi(n)} \equiv 1 \bmod n.$$

A special case of Euler's theorem is Fermat's Little Theorem, which says that if p is a prime number then

$$a^{p-1} \equiv 1 \bmod p$$

for any integer a not divisible by p. Lucas showed how one can use Euler's theorem to prove primality. Recall that the order of an integer a (coprime to n) modulo n is the least positive integer h such that

$$a^h \equiv 1 \bmod n.$$

By division algorithm, one can show that h must divide any integer k for which

$$\begin{aligned} a^k &\equiv 1 \bmod n : \\ \text{as } k &= hq + r, \qquad 0 \leq r < h \\ \implies a^k &= \left(a^h\right)^q . a^r \bmod n \\ \implies 1 &\equiv a^r \bmod n \\ \implies r &= 0 \end{aligned}$$

by minimality of h.

THEOREM 10.1. *Let n be a positive integer and a be an integer coprime to n such that*

$$a^{n-1} \equiv 1 \ mod\ n, \qquad but \qquad a^{\frac{n-1}{p}} \neq 1 \ mod\ n \qquad \forall p \mid (n-1),$$

where p is any prime dividing $n-1$. Then n must be prime.

Proof: Let

$$n - 1 = p_1^{e_1} \ldots . p_k^{e_k}$$

be the factorization of $n-1$ into distinct prime powers. Let h be the order of a modulo n. We know that h must divide $\phi(n)$. By the hypothesis, we have

$$\begin{aligned} & h \mid (n-1), \quad h \nmid \frac{n-1}{p_i} \\ \implies & {p_i}^{e_i} \mid h \qquad \forall i. \\ \implies & {p_i}^{e_i} \mid \phi(n) \qquad \forall i. \\ \implies & (n-1) \mid \phi(n) \\ \implies & \phi(n) = n - 1. \end{aligned}$$

Thus, n must be a prime. □

Example: Consider $n = 197$. We observe that

$$197 - 1 = 2^2 . 7^2.$$

Therefore, if we can find an integer $a > 1$ coprime to n such that

$$a^{196} \equiv 1 \bmod 197, \qquad a^{\frac{196}{2}} = a^{98} \not\equiv 1 \bmod 197, \qquad a^{\frac{196}{7}} = a^{28} \not\equiv 1 \bmod 197,$$

n will be prime. Now we try $a = 2$ and compute that

$$2^{196} \equiv 1 \bmod 197, \qquad 2^{98} \equiv -1 \bmod 197, \qquad 2^{28} \equiv 104 \bmod 197.$$

Therefore, 197 must be a prime. □

It is not necessary that we need a common base a which satisfies the hypothesis of Lucas test for each prime p dividing $n-1$. We have the following generalization:

THEOREM 10.2. *Let n be a positive integer. Assume that for each prime p_i, we have an integer a_i such that*

$$a_i^{n-1} \equiv 1 \ mod\ n, \qquad but\ a_i^{\frac{n-1}{p_i}} \neq 1 \ mod\ n \qquad \forall p \mid (n-1).$$

Then n must be prime.

Proof: Again, let

$$n - 1 = p_1^{e_1} \ldots . p_k^{e_k}$$

be the factorization of $n-1$ into distinct prime powers. Let h_i be the order of a_i modulo n. We know that h_i must divide $\phi(n)$. By the hypothesis, we have

$$\begin{aligned} & h_i \mid (n-1), \qquad h_i \nmid \frac{n-1}{p_i} \\ \Longrightarrow \quad & {p_i}^{e_i} \mid h_i \qquad \forall i. \\ \Longrightarrow \quad & {p_i}^{e_i} \mid \phi(n) \qquad \forall i. \\ \Longrightarrow \quad & (n-1) \mid \phi(n) \\ \Longrightarrow \quad & \phi(n) = n - 1. \end{aligned}$$

Thus, n must be a prime. □

Example: let us consider $n = 151$. We observe that

$$151 - 1 = 2.3.5^2.$$

Therefore, if we can find integers $a_1,\ a_2,\ a_3 > 1$ coprime to n such that

$$a_i^{150} \equiv 1 \bmod 151, \qquad a_1^{\frac{150}{2}} = a^{75} \not\equiv 1 \bmod 151,$$
$$a_2^{\frac{150}{3}} = a^{50} \not\equiv 1 \bmod 151, \qquad a_3^{\frac{150}{5}} = a^{30} \not\equiv 1 \bmod 151,$$

n will be prime. We take $a_1 = 3 = a_3$ and $a_2 = 2$ and compute that

$$3^{75} \equiv -1 \bmod 151, \qquad 2^{50} \equiv 145 \bmod 151, \qquad 3^{30} \not\equiv 59 \bmod 151,$$
$$3^{150} \equiv 1 \bmod 151, \qquad 2^{150} \equiv 1 \bmod 151.$$

Therefore, 197 must be a prime. □

One drawback of Lucas test is that it may not be too easy to find all the prime dividing $n-1$, though in cases that we use it will always be even. One way to avoid finding all prime factors of $(n-1)$ was shown by Pocklington. He showed that it is enough to factorize $n-1$ into prime powers which multiply to an integer at least $\sqrt{n}$. While we do not have to factorize $n-1$ completely, we will have to check a stronger condition than the second part of the hypothesis in Lucas Test.

THEOREM 10.3. *Let n be a positive integer. Suppose we have*

$$n - 1 = md, \qquad m \geq \sqrt{n},$$

and we know the prime factors p_i of m completely. Assume that for each prime p_i, we have an integer a_i such that

$$a_i^{n-1} \equiv 1 \ mod\ n, \qquad gcd\Big(a_i^{\frac{n-1}{p_i}} - 1, n\Big) = 1 \ mod\ n \qquad \forall p_i \mid m.$$

Then n must be prime.

Proof: Consider the prime factorization of $n-1$:

$$n - 1 = p_1^{e_1} \ldots . p_k^{e_k}.$$

Let p be the smallest prime divisor of n. Let h_i be the order of a_i modulo p. Then h_i must divide $p-1$. Further, we know from the hypothesis that

$$a_i^{n-1} \equiv 1 \bmod p, \qquad a_i^{\frac{n-1}{p_i}} \not\equiv 1 \bmod p.$$

Then,

$$p_i^{e_i} \mid h_i \implies p_i^{e_i} \mid (p-1).$$

In other words $p-1$ is divisible by m. Therefore, the smallest prime divisor of n is bigger than $\sqrt{n}$. Hence, p must be n itself, and n is a prime. □

Example:

10.1.2 Miller-Rabin Test for Primality

Miller-Rabin test is based on Fermat's little theorem as well. If an integer fails the test, one can confirm that the integer is composite. If an integer passes this test, there is still a small probability that the integer may be composite. It serves as a probabilistic test for primality. The following theorem forms the basis of Miller-Rabin test.

THEOREM 10.4. *Let p be an odd prime. Let*

$$p - 1 = 2^e m, \qquad gcd(2, m) = 1.$$

For any integer a such that $1 < a < p - 1$, either

$$a^m \equiv 1 \ mod\ p,$$

or for some $j = 1,\ 2,\ \ldots,\ e - 1$,

$$a^{2^j m} \equiv 1 \ mod\ p.$$

Proof: Let h be the order of a modulo p. We know that h divides $p - 1$. Hence,

$$h = 2^k m_1, \qquad m_1 \mid m,\ \ 0 \le k \le e.$$

Now,

$$\begin{aligned} k = 0 \qquad &\implies a^{m_1} \equiv 1 \bmod p \\ &\implies a^m \equiv 1 \bmod p \\ k > 0 \quad &\implies \left(a^{2^{k-1} m_1}\right)^2 \equiv 1 \bmod p \\ &\implies a^{2^{k-1} m_1} \equiv 1 \bmod p \\ &\text{or } a^{2^{k-1} m_1} \equiv -1 \bmod p. \end{aligned}$$

But the we can not have the congruence $a^{2^{k-1} m_1} \equiv 1 \bmod p$, as it is strictly less tan h. The theorem follows. □

In order to apply the theorem to decide primality of a given integer n, we pick a random integer $1 < a < n - 1$ and consider the set

$$a^m,\ a^{2m},\ \ldots,\ a^{2^e m} = a^{n-1}$$

where

$$n - 1 = 2^e m, \qquad 2 \nmid m.$$

In the above set modulo n, if the occurrence of 1 is either at the first place or is preceded by -1, we say that the integer n passes the Miller-Rabin test with base a. Then the integer n is more likely to be prime, but the test is not confirmatory. But if n fails the test, we can immediately say from the above theorem that n must be composite. In that case, the base a is referred to as 'witness'. If the integer n passes the Miller-Rabin test with base a, we can try another base to be a. If we pick k integers $a_1, a_2, \ldots, a_k$ randomly and perform the Miller-Rabin test, the probability that an integer which passes the test is still composite turns out to be $\left(\frac{1}{4}\right)^k$. Hence, there is a very small chance that a composite number passes the Miller-Rabin test. For example, if we perform the test with 20 bases then the integer passing the test is prime with the probability $1 - \left(\frac{1}{4}\right)^{20}$, which is very close to 1.

Example: let is demonstrate the method with $n = 341$, which is a Euler psedo-prime. Observe that

$$341 - 1 = 2^2 \times 5 = 2^2.85.$$

Let us take $a = 2$, and compute

$$2^{85} \bmod 32 \bmod 341, \qquad 2^{170} \equiv 1, \qquad 2^{340} \equiv 1 \bmod 341.$$

Since the occurrence of 1 is not preceded by -1 in the above, we can conclude that 341 fails the Miller-Rabin test for primality. Therefore, 341 must be composite and 2 is a witness. □

10.2 Lecture 2

Preamble: While many a primality test only tells merely about the existence of non-trivial factors, it does not actually produce a non-trivial factor. Cryptosystems like RSA are based on the fact that it is very time consuming to find the factors of large composite numbers. In this lecture we will study two efficient methods of factorization due to Pollard.

Keywords: Pollard's ρ-method, Pollard's $(p-1)$-method

10.2.1 Pollard's ρ-Method for Factorization

Pollard suggested a simple procedure which may produce factors of a composite number n. Given an integer n, one chooses a polynomial over integers of degree at least two, and an integer x_0 and iteratively calculates integers

$$x_{k+1} = f(x_k) \qquad \forall k \geq 1.$$

If n has a factor d (yet unknown), one expects that in the sequence of integers x_k's, x_i will be congruent to x_j modulo d for some $i > j$. One checks the gcd of $x_i - x_j$ and n by Euclid's algorithm. If the gcd is nontrivial (other than 1 and n), then one obtains a factor of n. If it does not yield a non-trivial factor one can take a different choice of x_0, or replace the polynomial $f(x)$ will another one. It is somewhat surprising that this method can be quite effective.

Example: Let us try the integer $n = 70723$. we will take $f(x) = x^2 + 3$ and $x_0 = 1$. Then

$$x_1 = f(x_0) = 4, \quad x_2 = f(x_1) = 19, \quad x_3 = 364, \quad \ldots.$$

We find that $gcd(x_3 - x_1, n) = 359$. Thus, 359 divides n, and we obtain

$$n = 359 \times 197. \qquad \square$$

There is another useful variant of the above method of Pollard. Note that if $x_i \equiv x_j \bmod d$ for some $i > j$, then $x_{i+1} = f(x_i) \equiv f(x_j) = x_{j+1} \bmod d$. Once we have $x_i \equiv x_j \bmod d$ for some $i > j$, the sequence x_k modulo d will be periodic where $i - j$ elements are repeated infinitely many times. If k is a multiple of $(i - j)$ larger than j, then $x_i \equiv x_j \bmod d$ will result in $x_{2k} \equiv x_k \bmod d$. Therefore, we can reduce the number of steps in the above method by just trying $gcd(x_{2k} - x_k, n)$ for various k's rather than

trying $gcd(x_i - x_j, n)$ for each i and j.

Example: Let us try the integer $n = 19109$. we will take $f(x) = x^2 + 1$ and $x_0 = 0$. Then

$$\begin{aligned} x_1 = f(x_0) = 1, \quad x_2 &= f(x_1) = 2, \\ x_3 = 5, \quad x_4 &= 26, \\ x_5 = 677, \quad x_6 &\equiv 18823 \bmod 19109. \end{aligned}$$

We observe that $x_4 - x_2 = 24$ and n have gcd 1. Now, $x_6 - x_3 = 18818$. We then compute the gcd of 18818 and $n = 19109$. If the gcd turns out to be trivial, we will compute $x_8 - x_4$ etc. The gcd of 18818 and 19109 can be computed using Euclid's algorithm as follows:

$$\begin{aligned} 19109 &= 18818 \times 1 + 291 \\ 18818 &= 291 \times 64 + 194 \\ 291 &= 194 \times 1 + 97 \\ 194 &= 97 \times 2 + 0. \end{aligned}$$

Hence, 97 is a factor of 19109. if we divide by 97 w find that $n = 97 \times 197$. □

10.2.2 Pollard's $(p-1)$-Method for Factorization

This method works when the integer n that we want to factorize has a prime divisor p such that $p - 1$ is a factor of primes of small size. Suppose $(p - 1)$ has small enough prime factors so that $(p - 1)$ divides a fixed integer q. For example, we may take $q = k!$ or $q = lcm(1, 2, \ldots, k)$ for some fixed choice of k. Then, we take an integer a coprime to n, and compute $a^q \equiv m \bmod n$. Now,

$$\begin{aligned} m &\equiv a^q \bmod p \\ \implies m &\equiv 1 \bmod p \\ \implies p &\mid (m-1). \end{aligned}$$

Then, we look for $gcd(m-1, n)$, which must be nontrivial as p certainly divides the gcd. If the gcd turns out to be n itself, then we take a different choice of a. If the gcd turns out to be 1, then we have to take a larger q.

Example: Let us demonstrate how Pollard's $(p-1)$-method works by considering $n = 54227$. We will work under the assumption that n has a prime factor p such that $p-1$ divides the lcm of the first 8-numbers, i.e., we will assume that $q = 420$, which is the lcm of the first eight natural numbers. If the method does not yield a factor, we may have to take a larger q. Let us take $a = 2$ which is clearly coprime to $n = 54227$. We have to compute $m \equiv 2^{420} \bmod n$, and then then $gcd(m-1, n)$. Observe that the binary expansion of 420 is

$$420 = 2^8 + 2^7 + 2^4 = 256 + 128 + 16.$$

Therefore, we proceed as follows.

$$\begin{aligned}
2^2 &\equiv 4 \bmod 54227 \\
2^4 &\equiv 16 \bmod 54227 \\
2^8 &\equiv 256 \bmod 54227 \\
2^{16} &\equiv 11309 \bmod 54227 \\
2^{32} &\equiv 26215 \bmod 54227 \\
2^{64} &\equiv 7454 \bmod 54227 \\
2^{128} &\equiv 33668 \bmod 54227 \\
2^{256} &\equiv 27243 \bmod 54227 \\
\implies 2^{420} = 2^{256}2^{128}2^{32}2^4 &\equiv 24688 \bmod 54227
\end{aligned}$$

Therefore, we now take $m = 24688$ and compute the gcd of $m-$ and n by Eucld's algorithm:

$$\begin{aligned}
54227 &= 24688 \times 2 + 4853 \\
24688 &= 4853 \times 4 + 422 \\
4853 &= 422 \times 11 + 211 \\
422 &= 211 \times 2 + 0.
\end{aligned}$$

therefore, we find that 211 is a factor of $n = 54227$, and now we can compute express $n = 211 \times 257$. □

10.3 Lecture 3

Preamble: In this lecture we will discuss a few methods for factorizing a given natural number, namely Fermat's factorization and the coninued fraction method.

Keywords: Fermat's factorization, continued fraction

10.3.1 Fermat's Factorization

If a given integer n is the difference of two squares, then we can express it as th product of two factors in the following way:

$$n = x^2 - y^2 \Rightarrow n = (x - y)(x + y).$$

Conversely, if $n = ab$ is an odd composite number, we can express n as the difference of two squares of integers:

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2.$$

Note that as n is odd, both a and b are odd, and hence $a+b$ and $a-b$ are even integers. The argument works for any integer, as we can easily extract the power of 2, and then use the above procedure for factorizing the odd part. Of course it is not always easy to find the two squares whose difference is the odd integer n. One can try squares a^2 bigger than n and try to solve the Diophantine equation

$$a^2 - n = b^2.$$

Example: Consider $n = 4891$. Observe that $69^2 < 4891 < 70^2$. Now, we find that $70^2 - 4891 = 3^2$. Hence we can easily factorize 4891 as

$$4891 = (70 + 3)(70 - 3) = 73.67.$$

If $70^2 - 4891$ had not been a square, we would have tried to find whether $71^2 - 4891$ is a square, and so on. □

10.3.2 Continued Fraction Method

One can use continued fraction to factorize an integer. Let n be a natural number which is not a square and consider its continued fraction

$$\sqrt{n} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ldots + \cfrac{1}{q_k + \cfrac{1}{\alpha_{k+1}}}}}.$$

Recall that while q_i's are natural numbers, α_k is irrational. Let $\frac{A_k}{B_k}$ be the k-th convergent given by

$$\frac{A_k}{B_k} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ldots + \cfrac{1}{q_{k-1} + \cfrac{1}{q_k}}}},$$

then we have the relation

$$A_k B_{k-1} - A_{k-1} B_k = (-1)^{k-1},$$

and we can write

$$\sqrt{n} = \frac{\alpha_{k+1} A_k + A_{k-1}}{\alpha_{k+1} B_k + B_{k-1}}.$$

One can try to find factors of n from the convergents as we will see now. First we want another relation involving the A_i's and B_i's which will be useful in the finding factors.

LEMMA 10.5. *Let us define two sequence s_k and t_k recursively by setting*

$$s_0 = 0, \;\; t_0 = 1, \qquad s_{k+1} = q_k t_k - s_k, \;\; t_{k+1} = \frac{n - s_{k+1}^2}{t_k} \qquad k \geq 0.$$

Then s_k and $t_k \neq 0$ are integers, $t_k \mid (n - s_k^2)$ and

$$\alpha_k = \frac{s_k + \sqrt{n}}{t_k}.$$

Proof: We will use induction. The case $k = 0$ is obvious, as $\alpha_0 = \sqrt{n}$. Assume the lemma is true for k. Clearly, s_{k+1} is an integer, and

$$\begin{aligned} t_{k+1} &= \frac{n - s_{k+1}^2}{t_k} \\ &= \frac{n - s_k^2}{t_k} + 2q_k s_k - q_k^2 t_k \end{aligned}$$

By induction hypothesis, $t_k \mid \left(n - s_k^2\right)$ and t_{k+1} is clearly an integer. $t_{k+1} = 0$ would mean $n = s_{k+1}^2$ but we assumed that n is not a square. Noting t_k is an integer, it follows from the recursive formula

$$t_k t_{k+1} = n - s_{k+1}^2 \implies t_{k+1} \mid (n - s_{k+1}^2).$$

Observe now that

$$\begin{aligned} \alpha_k &= q_k + \frac{1}{\alpha_{k+1}} \\ \implies \alpha_{k+1} &= \frac{1}{\alpha_k - q_k} \\ &= \frac{t_k}{(s_k - t_k q_k) + \sqrt{n}} \\ &= \frac{t_k}{\sqrt{n} - s_{k+1}} \\ &= \frac{t_k(\sqrt{n} + s_{k+1})}{n - s_{k+1}^2} \\ &= \frac{t_k(\sqrt{n} + s_{k+1})}{t_k t_{k+1}} \\ &= \frac{\sqrt{n} + s_{k+1}}{t_{k+1}}. \qquad \square \end{aligned}$$

The following relation is a crucial ingredient in our search for a factor of n.

PROPOSITION 10.6. *We have*

$$A_k^2 - nB_k^2 = (-1)^{k+1} t_{k+1}.$$

Proof: Substituting $\alpha_{k+1} = \frac{s_{k+1}+\sqrt{n}}{t_{k+1}}$ in

$$\begin{aligned}
\sqrt{n} &= \frac{\alpha_{k+1}A_k + A_{k-1}}{\alpha_{k+1}B_k + B_{k-1}} \\
\implies \sqrt{n}(s_{k+1}B_k + t_{k+1}B_{k-1}) + nB_k &= s_{k+1}A_k + t_{k+1}A_{k-1} + \sqrt{n}A_k \\
\implies s_{k+1}B_k + t_{k+1}B_{k-1} &= A_k \\
\text{and } s_{k+1}A_k + t_{k+1}A_{k-1} &= nB_k \\
\implies A_k^2 - nB_k^2 &= (s_{k+1}B_k + t_{k+1}B_{k-1})A_k \\
&\quad -(s_{k+1}A_k + t_{k+1}A_{k-1})B_k \\
&= t_{k+1}(A_kB_{k-1} - A_{k-1}B_k) \\
&= (-1)^{k-1}t_{k+1}. \qquad \square
\end{aligned}$$

In order to factorize n using continued fraction of $\sqrt{n}$, we look for an odd integer k such that t_{k+1} is a perfect square, so that we can write

$$A_k^2 - nB_k^2 = y^2$$

for some integer y. We view this relation as

$$\begin{aligned}
A_k^2 &\equiv y^2 \bmod n \\
\implies (A_k - y)(A_k + y) &\equiv 0 \bmod n.
\end{aligned}$$

We can now apply Euclid's algorithm to obtain $gcd(A_k - y, n)$ and $gcd(A_k + y, n)$. One of these two gcds is bound to be bigger than 1, giving us a factor of n . However it may happen that both the gcds are n itself. Then we look for another odd k such that t_k is a square.

10.4 Lecture 4

Preamble: In this lecture we will briefly discuss Fermat's Last Theorem. Though predicted by Fermat by long ago, it remained a statement without proof for almost 350 years. The proof of Fermat's theorem was one of the greatest achievements in number theory, as it eluded the greatest of mathematicians for centuries. In this lecture, we will provide some historical details, and end with a proof of the case for exponent 4. The method for the proof in this special case is known as Fermat's infinite descent.

Keywords: Fermat's Last Theorem

10.4.1 Fermat's Conjecture

We know that there are infinitely many integers a, b, c satisfying

$$a^2 + b^2 = c^2.$$

The sixteenth century French mathematician Fermat considered exponents higher than 2, and he stated that

THEOREM 10.7. $\mathbf{a^n + b^n = c^n}$ *has no non-trivial solution* $(\mathbf{a}, \mathbf{b}, \mathbf{c})$ *in integers for any integer* $\mathbf{n > 2}$.

By non-trivial solution, we mean a solution (a, b, c) with $abc \neq 0$. The above statement is known as the **Fermat's Last Theorem** (FLT), though it actually remained a conjecture for 350 years until a British mathematician named Andrew Wiles proved it recently. Fermat wrote the statement in the margin of his copy of *Arithmetic* by Diophantus on the page describing Pythagorean triples. Fermat wrote most of his important results in the margin of that book. He mentioned that he had a wonderful proof of the above but the margin was too small for him to write it down. Mathematicians of today do not believe that Fermat really found a correct proof. Many great mathematicians (Kummer, Dirichlet, Legendre, Sophie Germain to name a few) in the following decades and centuries tried unsuccessfully to prove the FLT. Kummer thought he solved Fermat's problem completely, but Dirichlet pointed out that Kummer's assumption about validity of unique factorization for rings of integers was not true in general. When Kummer tried to correct his mistake, it led to an extensive theory of ideals for rings of integers in number fields.

One of the greatest mathematicians of all time, Gauss proved the case $n = 4$. Euler gave a wrong proof for $n = 3$. Dirichlet proves it for $n = 14$, and Liouville $n = 7$. Falting's work on Mordell Conjecture implies that Fermat's equation $x^n + y^n = z^n$ has at most finitely many solutions. The efforts by all these great mathematicians to solve the FLT resulted in many discoveries. The reason the FLT was a blessing for mathematics because of the amount of mathematics it generated and inspired in the following centuries. It was regarded as one of the two greatest unsolved problems in mathematics along with **Riemann Hypothesis**.

Andrew Wiles worked on it in complete secrecy for seven years at Princeton University. He announced the proof in a conference at the Isaac Newton Institute of Cambridge in 1993 and it was a sensation. However, a gap in his proof was discovered which he settled within a year with the help of his former student Richard Taylor. It will be far beyond the scope of this course to discuss Wile's proof. We will content ourselves with a proof for the case when the exponent is 4. The proof for exponent 4 relied heavily on the form of Pythagorean triples, hence we discuss those first.

10.4.2 Pythagorean Triples

A Pyhathgorean triple consists of three integers a, b and c such that $a^2 + b^2 = c^2$. For example, $(3, 4, 5)$ is such a triple, so is $(6, 8, 10)$. A Pythagorean triple (a, b, c) is called primitive if $gcd(a, b, c) = 1$. Clearly, For a primitive Pyathogrean triple (a, b, c), any two of the triple is relatively prime.

PROPOSITION 10.8. *Any primitive Pythagorean triple (a, b, c) can be expressed as*

$$a = m^2 - n^2, \qquad b = 2mn, \qquad c = m^2 + n^2,$$

for two relatively prime integers m and n, not both odd.

Proof: Clearly,

$$(m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2,$$

so we obtain a Pythagorean triple for any coprime-integers m and n as above. We only need to check that the Pythagorean triple is primitive. If p is an odd prime dividing $m^2 + n^2$ and $m^2 - n^2$, then $p \mid 2m^2$ and $p \mid 2n^2$, which implies $p|m$ ad $p|n$, contradicting the fact that m and n are coprime. As exactly one of m and n is even, $2 \nmid m^2 - n^2$. Thus, the three integers $(m^2 - n^2,\ 2mn,\ m^2 + n^2)$ form a primitive Pythagorean triple.

Conversely, let $a^2 + b^2 = c^2$, where $gcd(a, b, c) = 1$. Without loss of generality, we may assume that a is odd, and b is even. Then c must be odd. We have $b^2 = (c - a)(c + a)$. Now, if p is an odd prime such that $p \mid (c - a)$ and $p \mid (c + a)$, then $p|2c, p|2a$. It follows that $p \mid b$ $p \mid c$ and hence $p \mid b$. It contradicts that $gcd(a, b, c) = 1$. Clearly, 2 divides the even integers $c - a$ and $c + a$. Further, considering a and c modulo 4, we deduce that exactly one of $(c - a)$ and $(c + a)$ will not be divisible by 4. By considering the unique factorization of $b^2 = (c - a)(c + a)$, and using the fact that $c - a$ and $c + a$ have no common factors other than 2, we can conclude that

$$c + a = 2m^2, \qquad c - a = 2n^2, \qquad b = 2mn$$

where exactly one of m and n is odd. Hence

$$a = m^2 - n^2, \qquad c = m^2 + n^2, \qquad b = 2mn.$$

Now m and n must be relatively prime, as a common factor of m and n will also be a common factor of a, b and c. □

For Example, we have the Pythagorean triple $(5, 12, 13)$ where

$$5^2 + 12^2 = 13^2.$$

We observe that

$$5 = 3^2 - 2^2, \qquad 12 = 2.2.3, \qquad 13 = 3^2 + 2^2.$$

10.4.3 Method of Infinite Descent

We will now prove that the Fermat's equation with exponent 4

$$x^4 + y^4 = z^4$$

has no non-trivial solution in integers. It will clearly be enough to prove that there is no primitive solution in positive integers, where a solution (a, b, c) will be called primitive if $gcd(a, b, c) = 1$: the common factor removed from a hypothetical solution will still be a solution. We will prove a stronger statement. We will show that if $x^4 + y^4 = u^2$ has a primitive solution in positive integers, then we can find a smaller such solution. By repeating this argument, we will arrive at a contradiction, as there are only finitely many positive integers less that a given a positive number (the initial solution).

Suppose $x^4 + y^4 = u^2$ where $gcd(x, y, z) = 1$. Without loss of generality, we may assume that x is even and y is odd. Then, we can treat (x^2, y^2, u) as a Pythagorean triple, and write

$$x^2 = m^2 - n^2, \qquad y^2 = 2mn, \qquad u = m^2 + n^2,$$

where m, n are coprime integers. Note that m and n can not be both even or both odd, as $gcd(x, y, z) = 1$. As the square of an integer is 1 modulo 4, we can conclude that it is n which must be even, and so m must be odd. By looking at the unique factorization of the integer $y^2 = 2mn$, we deduce that $m = a^2$ and $n = 2b^2$. From the relatively prime pairs $(m - n)$, $(m + n)$ which multiply to give a square x^2, we deduce that $m + n = k^2$ and $m - n = l^2$ for two relatively prime odd integers k and l. The only common factor between $k - l$ and $k + l$ is 2. Then, $2n = k^2 - l^2$ implies $2.2b^2 = (k - l)(k + l)$. Thus, $k - l = 2r^2, k + l = 2s^2$, and we obtain

$$\begin{aligned}
k^2 + l^2 &= 2m \\
\implies \frac{1}{2}.(k-l)^2 + (k+l)^2 &= 2a^2 \\
\implies \frac{1}{2}.\left(4r^4 + 4s^4\right) &= 2a^2 \\
\implies r^4 + s^4 &= a^2 = m < m^2 + n^2 = u.
\end{aligned}$$

This way, we obtain a new solution (r, s, a) with a strictly smaller positive integer $a < u$ as the third component. □

We end with the remark that the above argument of infinite descent is useful in many situations.

Bibliography

1. T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, 1976.
2. A. Baker, *A Concise Introduction to Theory of Numbers*, Cambridge University Press, 1984
3. D. Burton, *Elementary Number Theory*, McGraw Hill, 2005.
4. H. Davenport, *The Higher Arithmetic*, Cambridge University Press, 2008.
5. K. F. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, 1990
6. G.A. Jones and J.M. Jones, *Elementary Number Theory*, Springer UTM, 2007.
7. N. Koblitz, *A Course in Number Theory and Cryptography*, Springer, 2010
8. I. Niven, H.S. Zuckerman and H.L. Montgommery, *Introduction to the Theory of Numbers*, Wiley, 2000.
9. J. P. Serre, *A Course in Arithmetic*, Springer, 1973.