Conspectus for
An Introduction To The Theory of Numbers

Lado Turmanidze

August 4, 2023 - August 21, 2023

Not exactly related, but too awesome to miss out! **Generalization of factorial for real number x. γ is Euler-Mascheroni constant.**

$$\Gamma(x+1) = \Pi(x) = x! = \lim_{N\to\infty} N^x \prod_{k=1}^{N} \frac{k}{x+k} = \int_0^\infty t^x e^{-t}\, dt$$

$$\frac{d}{dx}(\ln(x!)) = H_x - \gamma,\ \gamma \approx 0.5772...$$

1 Divisibility

First and foremost, (a, b) denotes greatest common divisor of $a, b \in \mathbb{N}^+$, whereas $[a, b]$ denotes least common multiple.

Theorem 1.6: For any positive integer $m, (ma, mb) = m(a, b)$.

Theorem 1.8: If $(a, m) = (b, m) = 1$, then $(ab, m) = 1$.

Theorem 1.9: For any integer $x, (a, b) = (b, a) = (a, -b) = (a, b + ax)$..

Theorem 1.13: If $m > 0, [ma, mb] = m[a, b]$. Also $[a, b] \times (a, b) = |ab|$.

Exercise 1.51: If $(a, b) = 1$ and $p > 2$ is a prime, then $\left(a + b, \frac{a^p + b^p}{a + b}\right) = 1$ or p.

Theorem 1.6: *The fundamental theorem of arithmetic or the unique factorization theorem.* The factoring of any integer $a > 1$ into primes is unique apart from the order of the prime factors.

$$a \in \mathbb{N}^+,\ \alpha(p) \in \mathbb{N}, \quad a = \prod_p p^{\alpha(p)}$$

$$(a,b) = \prod_p p^{\min(\alpha(p),\beta(p))}, \quad [a,b] = \prod_p p^{\max(\alpha(p),\beta(p))}$$

Theorem 1.8: Given any positive integer k, there exists k consecutive composite integers.

Proof that **number of primes is infinite**. Suppose that $p_1, p_2, \cdots, p_r$ are primes and $n = 1 + p_1 \times p_2 \times \cdots \times p_r$. Note that $\forall i \in \{1, 2, \cdots, r\}$, $p_i \nmid n$. Since n is either a prime or has a prime factor p, this implies that there is a prime distinct from $p_1, p_2, \cdots, p_r$. For any finite r, the number of primes is not exactly r. Hence the number of primes is infinite.

Theorem 1.20: Let $\mathcal{P}$ be a set containing exactly n elements. For any non-negative integer k, the number of subsets of $\mathcal{P}$ containing precisely k elements is $\binom{n}{k}$.

Theorem 1.21: The product of any k consecutive integers is divisible by $k!$.

Lemma 1.23: Let $P(z) = \sum_{k=0}^{n} a_k z^k$ be a polynomial with real coefficients. Then $a_r = \dfrac{P^{(r)}(0)}{r!}$, $0 \le r \le n$, where $P^{(r)}(0)$ is the rth derivative of $P(z)$ at $z = 0$.

2 Congruences

1. $a \equiv b \mod m \implies b \equiv a \mod m$
2. $(a \equiv b \mod m) \wedge (b \equiv c \mod m) \implies a \equiv c \mod m$
3. $(a \equiv b \mod m) \wedge (c \equiv d \mod m) \implies (a+b) \equiv (c+d) \mod m$
4. $(a \equiv b \mod m) \wedge (c \equiv d \mod m) \implies ac \equiv bd \mod m$
5. $(a \equiv b \mod m) \wedge (d \mid m, d > 0) \implies a \equiv b \mod d$

6. $(a \equiv b \mod m) \implies (ac \equiv bc \mod mc)$, $c > 0$

7. Let f denote a polynomial with integral coefficient. $a \equiv b \mod m \implies f(a) \equiv f(b) \mod m$

8. $ax \equiv bx \mod m$ **iff** $x \equiv y \mod \frac{m}{(a,m)}$

Definition 2.2: If $x = y \mod m$ then y is called a residue of x modulo m.

Theorem 2.4: If $b = c \mod m$, then $(b, m) = (c, m)$

Fermat's Theorem: Let p denote a prime. If $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$. For every integer $a, a^p \equiv a \mod p$.

Euler's generalization of Fermat's theorem: If $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \mod m$.

Theorem 2.9: If $(a, m) = 1$, then there is an x such that $ax = 1 \mod m$. Any two such x are congruent mod m. If $(a, m) > 1$, then there is no such x.

Lemma 2.10: Let p be a prime number. Then $x^2 \equiv 1 \mod p$ **iff** $x \equiv \pm 1 \mod p$.

Theorem 2.11: *Wilson's Theorem.* p is a prime $\implies$ $(p-1) \equiv -1 \mod p$

Theorem 2.12: Let p denote a prime. Then $x^2 \equiv -1 \mod p$ has solutions **iff** $p = 2$ or $p \equiv 1 \mod 4$.

Lemma 2.13: If $p > 2$ is a prime number and $p \equiv 1 \mod 4$, then $\exists a, b \in \mathbb{N}^+$, $a^2 + b^2 = p$.

Lemma 2.14: Let q be a prime factor of $a^2 + b^2$. If $q \equiv 3 \mod 4$, then $q \mid a$ and $q \mid b$.

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ac + bc)^2, \forall a, b, c, d \in \mathbb{R}$$

Definition 2.4: Let $r_1, r_2, \cdots, r_m$ denote a complete residue system modulo m. The number of solutions of $f(x) \equiv 0 \mod m$ is the number of the r_i, such that $f(r_i) \equiv 0 \mod m$.

Theorem 2.16: $d \mid m$, $d > 0$ and u is a solution of $f(x) \equiv 0 \mod m$, then u is a solution of $f(x) \equiv 0 \mod d$.

The Chinese Remainder Theorem:

$$x \equiv a \mod m_1, x \equiv a_2 \mod m_2, \cdots, x \equiv a_r \mod m_r$$

Let $m_1, m_2, \cdots, m_r$ denote r positive integers that are relatively prime in pairs and let $a_1, a_2, \cdots, a_r$ denote any r integers. Then the congruences displayed above have common solutions. If x_0 is one such solution, then an integer x satisfies the above congruences if and only if $x = x_0 + km, k \in \mathbb{N}$ and $m = \prod_{i=1}^{r} m_i$.

$$\phi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \times \prod_{i=1}^{r}(1 - \frac{1}{p_i})$$

Lemma 2.22: Suppose that m is a positive integer and that $(a, m) = 1$. If k and $\bar{k}$ are positive integers such that $k\bar{k} \equiv 1 \mod \phi(m)$, then $a^{k\bar{k}} \equiv a \mod m$. Proof: $a^{k\bar{k}} = a \times a^{r\phi(m)} = a(a^{\phi(m)})^r \equiv a \times 1^r = a \mod m$.

Corollary 2.27: If $\sum_{i=0}^{n} b_i x^i \equiv 0 \mod p$ has more than n solutions, then all the coefficients b_i are divisible by p.

Corollary 2.30: If $d \mid (p-1)$, then $x^d \equiv 1 \mod p$ has d solutions.

Definition 2.6: Let m denote positive integer and a any integer such that $(a, m) = 1$. Let h be the smallest positive integer such that $a^h \equiv 1 \mod m$. We say that the order of a modulo m is h, or that a belongs to the exponent h modulo m.

Corollary 2.32: If $(a, m) = 1$, then the order of $a \mod m$ divides $\phi(m)$.

Definition 2.7: If g belongs to the exponent $\phi(m)$ modulo m, then g is called a *primitive root* modulo m.

Theorem 2.36: If p is a prime then there exists $\phi(p-1)$ primitive roots modulo p.

3 Quadratic Reciprocity and Quadratic Forms

Definition 3.1: For all a such that $(a, m) = 1$, a is called quadratic residue modulo m if the congruence $x^2 = a \mod m$ has solution. If it has no solution, then a is called quadratic non-residue modulo m.

Definition 3.2: If p denotes an odd prime, then the Legendre symbol $\left(\frac{a}{p}\right)$ is defined to be 1 if a is quadratic residue, -1 if a is quadratic non-residue modulo p, and 0 if $p \mid a$.

Theorem 3.1: Let p be an odd prime:

1. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$
2. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
3. $a \equiv b \mod p \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
4. $(a, p) = 1 \implies \left(\frac{a^2}{p}\right) = 1, \left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$
5. $\left(\frac{1}{p}\right) = 1, \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Theorem 3.4: *The Gaussian reciprocity law.* If p and q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Definition 3.4: *The Jacobi Symbol.* Let Q be positive and odd, so that $q_1 q_2 \cdots q_s$ where q_i are odd primes, not necessarily distinct. $\left(\frac{P}{q_j}\right)$ denotes the Legendre symbol, while Jacobi symbol is denoted as:

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s}\left(\frac{P}{q_j}\right)$$

4 Some Functions of Number Theory

$[x]$ **denotes floor of** x

Theorem 4.2: *de Polignac's formula.* Let p denote a prime. Then the largest exponent e such that $p^e \mid n!$ is $e = \sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right]$.

The Day of the Week from the Date: Let N denote the number of the day in the month, M - the number of the month counting from March(March = 1), C - denote the hundreds in the year and Y the rest($C = 20$ and $Y = 23$). Answer d denotes the day of the week, where $d = 0$ is Sunday. $d = N + [2.6M - 0.2] + Y + [Y/4] + [C/4]$.

Definition 4.1:

1. $d(n)$ is the number of positive divisors of n.
2. $\sigma(n)$ is the sum of the positive divisors of n.
3. $\sigma_k(n)$ is the sum of kth powers of the positive divisors of n.

4. $\omega(n)$ is the number of distinct primes dividing n.

5. $\Omega(n)$ is the number of primes dividing n, counting multiplicity.

6. $p^\alpha \mid\mid n$ means the highest exponent of p dividing n. Mathematically, this can be written as $\text{ord}_p(n) = a$ or $p^\alpha \mid n$, $p^{\alpha+1} \nmid n$.

Definition 4.2: If $f(n)$ is an arithmetic function not identically zero such that $f(mn) = f(m)f(n)$ for every pair of positive integers m, n satisfying $(m, n) = 1$, then $f(n)$ is said to be multiplicative. If $f(mn) = f(m)f(n)$ whether m and n are relatively prime or not, then $f(n)$ is said to be totally multiplicative or completely multiplicative.

Theorem 4.4: Let $f(n)$ be a multiplicative function and let $F(n) = \sum_{d|n} f(d)$. Then $F(n)$ is multiplicative.

Theorem 4.5: $\forall n \in \mathbb{N}^+$, $\sigma(n) = \prod_{p^\alpha || n} \left(\frac{p^{\alpha+1} - 1}{p - 1} \right)$.

Theorem 4.6: *Gauss's Theorem.* $\forall n \in \mathbb{N}^+$, $\sum_{d|n} \phi(d) = n$.

Definition 4.3: For positive integers n put $\mu(n) = (-1)^{\omega(n)}$ if n is a *square free*, and set $\mu(n) = 0$ otherwise. Then $\mu(n)$ is the Mobius μ function.

Theorem 4.7: The function $\mu(n)$ is multiplicative and $\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1 \\ 0, & n > 1 \end{cases}$

Theorem 4.8: *The Mobius inversion formula.* If $F(n) = \sum_{d|n} f(d)$ for every positive integer n, then $f(n) = \sum_{d|n} \mu(d)F(n/d)$.

Theorem 4.9: If $f(n) = \sum_{d|n} \mu(d)F(n/d)$ for every positive n, then $F(n) = \sum_{d|n} f(d)$.

Recurrence Functions: We say that the arithmetic function f(n) satisfies a linear recurrence (or recursion) if $f(n) = af(n-1) + bf(n-2)$ for $n = 2, 3, \cdots$. Here a and b are fixed numbers, which may be real or even complex. For brevity we write u_n for $f(n)$. In this notation the recurrence under consideration is $u_n = au_{n-1} + bu_{n-2}$.

5 Some Diophantine Equations

Theorem 5.1: Let $a \neq 0, b \neq 0$ and c be integers. If $g = \gcd(a, b) \nmid c$ then equation $ax + by = c$ has no solution in integers, else it has infinitely many solutions. If the pair (x_1, y_1) is one integral solution, then all others are of the form $x = x_1 + \frac{kb}{g}, y = y_1 - \frac{ka}{g}$ where k is an integer.

Definition 5.1: A *Square Matrix* U with integral elements is called unimodular if $\det(U) = \pm 1$.

Theorem 5.3: Let U be an $m \times m$ matrix with integral elements. Then the following are equivalent:

- U is unimodular.
- The inverse matrix U^{-1} exists and has integral elements.
- U may be expressed as a product of elementary row matrices. $U = R_g R_{g-1} \cdots R_2 R_1$.
- U may be expressed as a product of elementary column matrices. $U = C_1 C_2 \cdots C_{h-1} C_h$.

Lemma 5.4: If u and v are relatively prime integers whose product uv is a perfect square, then u and v are both perfect squares.

Theorem 5.5: The positive primitive solutions of $x^2 + y^2 = z^2$ with y even are $x = r^2 - s^2, y = 2rs, z = r^2 + s^2$, where r and s are arbitrary integers of opposite parity with $r > s > 0$ and $(r, s) = 1$.p

Theorem 5.11: Let a, b, c be nonzero integers such that the product abc is *square-free*. Necessary and sufficient conditions that $ax^2 + by^2 + cz^2 = 0$ have a solution in integers x, y, z, not all zero, are that a, b, c do not have the same sign, and that $-be, -ac, -ab$ are quadratic residues modulo a, b, c, respectively.

6 Farey Fractions and Irrational Numbers

A rational number with $\gcd(a, b) = 1$ is said to be in *reduced form* or *lowest terms*. Let us construct a table in the following way. In the first row we write $0/1$ and $1/1$. For $n = 2, 3, \cdots$ we use the rule: Form the nth row by copying the $(n-1)$st in order, but insert the fraction $(a + a')/(b + b')$ between the consecutive fractions a/b and a'/b' of the $(n-1)$st row if $b + b' \leq n$. Thus, since $1 + 1 \leq 2$ we insert$(0 + 1)/(1 + 1)$ between $0/1$ and $1/1$ and obtain $0/1$, $1/2$, $1/1$, for the second row.

Theorem 6.1: If a/b and a'/b' are consecutive fractions in the nth row, say with a/b to the left of a'/b', then $a'b - ab' = 1$.

Definition 6.1: The sequence of all reduced fractions with denominators not exceeding n, listed in order of their size, is called the Farey sequence of order n.

Corollary 6.2: Every a/b in the table is in reduced form.

Corollary 6.3: The fractions in each row are listed in order of their size.

Theorem 6.4: If a/b and a'/b' are consecutive fractions in any row, then among all rational fractions with values between these two, $(a + a')/(b + b')$ is the unique fraction with the smallest denominator.

Theorem 6.5: If $0 \leq x \leq y$, $(x, y) = 1$, then the fraction x/y appears in the yth row and all later rows.

Theorem 6.6: The nth row consists of all reduced fractions a/b such that $0 \leq a/b \leq 1$ and $0 < b \leq n$. These fractions are listed in order of their size.

Theorem 6.7: If a/b and c/d are Farey fractions of order n, such that no other Farey fraction of order n lies between them, then

$$\left| \frac{a}{b} - \frac{a+c}{b+d} \right| = \frac{1}{b(b+d)} \leq \frac{1}{b(n+1)}$$

and

$$\left|\frac{c}{d} - \frac{a+c}{b+d}\right| = \frac{1}{d(b+d)} \leq \frac{1}{d(n+1)}$$

.

Theorem 6.8: If n is a positive integer and x is real, there is a rational number a/b such that $0 < b \leq n$ and $\left|x - \frac{a}{b}\right| \leq \frac{1}{b(n+1)}$.

Theorem 6.9: If ξ is real and irrational, there are infinitely many distinct rational numbers a/b such that $\left|\xi - \frac{a}{b}\right| < \frac{1}{b^2}$.

Lemma 6.11: If x and y are positive integers then *not* both of the inequalities can hold: $\frac{1}{xy} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{x^2} + \frac{1}{y^2}\right)$ and $\frac{1}{x(x+y)} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{x^2} + \frac{1}{(x+y)^2}\right)$.

Theorem 6.11: *Hurwitz.* Given any irrational number ξ, there exist infinitely many different rational numbers h/k such that $\left|\xi - \frac{h}{k}\right| < \frac{1}{\sqrt{5}k^2}$.

Theorem 6.26: *Lagrange.* Every positive integer n can be expressed as the sum of four squares, $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$, where x_i are non-negative integers.

Corollary 6.27: There exist infinitely many positive integers that cannot be written as a sum of four positive perfect squares, but every integer $n > 169$ is a sum of five positive perfect squares.

7 Simple Continued Fractions

If $x_0, x_1, \cdots, x_j$ are all positive, except perhaps, x_0, real numbers then by following notation we denote *continued fraction expansion*:

$$\langle x_0, x_1, \cdots, x_j \rangle = x_0 + \frac{1}{x_1 + \frac{1}{x_2 + \cdots}}$$

$$\cdots + \frac{1}{x_{j-1} + \frac{1}{x_j}}$$

$$\langle x_0, x_1, \cdots, x_j \rangle = x_0 + \frac{1}{\langle x_1, \cdots, x_j \rangle} = \langle x_0, x_1, \cdots, x_{j-2}, x_{j-1} + \frac{1}{x_j} \rangle$$

Such a finite continued fraction is said to be *simple* if all the x_i are integers.

Theorem 7.1: If $\langle a_0, a_1, \cdots, a_j \rangle = \langle b_0, b_1, \cdots, b_n \rangle$ where these finite continued fractions are simple, and if $a_j > 1$ and $b_n > 1$, then $j = n$ and $a_i = b_i$ for $i = 0, 1, \cdots, n$.

Let $a_0, a_1, \cdots$ be an infinite sequence of integers, all positive except perhaps a_0. We define two sequences of integers $\{h_n\}$ and $\{k_n\}$ inductively as follows:

$$h_{-2} = 0,\ h_{-1} = 1,\ h_i = a_i h_{i-1} + h_{i-2},\ i \geq 0$$

$$k_{-2} = 1,\ k_{-1} = 0,\ h_i = a_i k_{i-1} + k_{i-2},\ i \geq 0$$

Note, that $1 = k_0 \leq k_1 < k_2 < \cdots < k_n < \cdots$.

Theorem 7.3: For any positive real number x, $\langle a_0, a_1, \cdots, a_{n-1}, x \rangle = \dfrac{x h_{n-1} + h_{n-2}}{x k_{n-1} + k_{n-2}}$

Theorem 7.4: If we define $r_n = \langle a_0, a_1, \cdots, a_n \rangle$ for all integers $n \geq 0$, then $r_n = \frac{h_n}{k_n}$

Theorem 7.5: The equations

$$h_i k_{i-1} - h_{i-1} k_i = (-1)^{i-1},\ r_i - r_{i-1} = \frac{(-1)^{i-1}}{k_i k_{i-1}}$$

hold for $i \geq 1$. The identities

$$h_i k_{i-2} - h_{i-2} k_i = (-1)^i a_i,\ r_i - r_{i-2} = \frac{(-1)^i a_i}{k_i k_{i-2}}$$

hold for $i \geq 1$. The fraction $\frac{h_i}{k_i}$ is reduced, that is $(h_i, k_i) = 1$.

Definition 7.1: An infinite simple continued fraction $\langle a_0, a_1, \cdots \rangle$ is defined to be $\lim_{n \to \infty} \langle a_0, a_1, \cdots, a_n \rangle$.

Theorem 7.7: The value of any infinite simple continued fraction is *irrational*.

Theorem 7.9: Two distinct infinite simple continued fractions converge to different values.

ξ denotes some irrational number.

Theorem 7.11: For $n \geq 0$ we have:

$$\left|\xi - \frac{h_n}{k_n}\right| < \frac{1}{k_n k_{n+1}} \wedge |\xi k_n - h_n| < \frac{1}{k_{n+1}}$$

Theorem 7.12:

$$\left|\xi - \frac{h_n}{k_n}\right| < \left|\xi - \frac{h_{n-1}}{k_{n-1}}\right| \wedge |\xi k_n - h_n| < |\xi k_{n-1} - h_{n-1}|$$

An infinite simple continued fraction $\langle a_0, a_1, \cdots \rangle$ is said to be periodic if there is an integer n such that $a_n = a_n + r$ for all sufficiently large r. Thus a periodic continued fraction can be written in the form:

$$\langle b_0, b_1, \cdots, b_j, a_0, a_1, \cdots, a_n, \cdots \rangle = \langle b_0, b_1, \cdots, \overline{a_0, a_1, \cdots, a_{n-1}} \rangle$$

Theorem 7.21: If the positive integer d is not a perfect square, the simple continued fraction expansion of $\sqrt{d}$ has the form: $\sqrt{d} = \langle a_0, \overline{a_1, a_2, \cdots, a_{r-1}, 2a_0} \rangle$.

The equation $x^2 - dy^2 = N$, with given integers d and N, unknowns x and y, is usually called *Pell's equation*. If d is negative, it can have only a finite number of solutions. If d is a perfect square, say $d = a^2$, the equation reduces to $(x - ay)(x + ay) = N$ and again there is only a finite number of solutions.

Theorem 7.22: If d is a positive integer not a perfect square, then $h_n^2 - dk_n^2 = (-1)^{n-1} q_{n+1}$ for all integers $n \geq -1$, where

$$q_{i+1} = \frac{d - m_{i+1}^2}{q_i},\ m_{i+1} = a_i q_i - m_i$$

8 Primes and Multiplicative Number Theory

Theorem 8.7: *Bertrand's Postulate.* If $x > 1$ is a real number, then there exists at least one prime number in the open interval $(x, 2x)$.

$$\pi(x) \sim \frac{x}{\log x}$$

Corollary 8.10: Let p' is the least prime exceeding p. $\limsup_{p\to\infty} \frac{p'-p}{\log p} \geq 1$ and $\liminf_{p\to\infty} \frac{p'-p}{\log p} \leq 1$.

A *Dirichlet Series* is any series of the form $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$. Here s is a real number, so that the series defines a function $A(s)$ of the real variable s, provided that the series converges. The *Riemann zeta function* is an important example of a Dirichlet series. For $s > 1$: $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.

Theorem 8.11: For each Dirichlet series $A(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ there exists a unique σ_a(abscissa of absolute convergence) such that the series is absolutely convergent for $s > \sigma_a$, but is not absolutely convergent for $s < \sigma_a$. If $c > \sigma_a$, then the series $A(s)$ is uniformly convergent for s in the interval $[c, +\infty)$.

Corollary 8.12: $A(s)$ is a continuous function on the open interval $(\sigma_a, +\infty)$.

Theorem 8.18: *The Euler Product Formula.* Suppose that $f(n)$ is a multiplicative function and put $F(s) = \sum_{n=1}^{\infty} f(n)/n^s$. If s is a real number for which the series is absolutely convergent, $F(s) = \prod_p (1 + f(p)/p^s + f(p^2)/p^{2s} + \cdots)$.

9 Algebraic Numbers

Definition 9.2: A polynomial $f(x)$, not identically zero, is irreducible, or prime, over $\mathbb{Q}$ if there is no factoring, $f(x) = g(x)h(x)$, or $f(x)$ into two polynomials $g(x)$ and $h(x)$ of positive degrees over $\mathbb{Q}$.

Theorem 9.4: If an irreducible polynomial $p(x)$ divides a product $f(x)g(x)$, then $p(x)$ divides at least one of the polynomials $f(x)$ and $g(x)$.

Definition 9.3: A polynomial $f(x) = a_n x^n + \cdots + a_0$ with integral coefficients a_j is said to be primitive if the greatest common divisor of its coefficients is 1.

Theorem 9.6: The product of two primitive polynomials is primitive.

Theorem 9.7: *Gauss's lemma.* If a monic polynomial $f(x)$ with integral coefficients factors into two monic polynomials with rational coefficients, say $f(x) = g(x)h(x)$, then $g(x)$ and $h(x)$ have integral coefficients.

Definition 9.4: Complex number ξ is called an algebraic number if it satisfies some polynomial equation $f(x) = 0$ where $f(x)$ is a polynomial over $\mathbb{Q}$. Any complex number that is not algebraic is said to be *transcendental.*

Theorem 9.8: An algebraic number ξ satisfies a unique irreducible monic polynomial equation $g(x) = 0$ over $\mathbb{Q}$. Furthermore, every polynomial equation over $\mathbb{Q}$ satisfied by ξ is divisible by $g(x)$.

Theorem 9.10: The minimal equation of an algebraic integer is monic with integral coefficients.

Theorem 9.12: If α and β are algebraic numbers, so are $\alpha + \beta$ and $\alpha\beta$. If α and β are algebraic integers, so are $\alpha + \beta$ and $\alpha\beta$.

Theorem 9.13: The set of all algebraic numbers forms a field. The set of all algebraic integers forms a ring.

Theorem 9.14: If ξ is an algebraic number of degree n, then every number in $\mathbb{Q}(\xi)$ can be written uniquely in the form $a_o + a_1\xi + \cdots + a_{n-1}\xi^{n-1}$ where the a_i are rational numbers.

Theorem 9.15: Let $G(x)$ be a polynomial over $\mathbb{Q}$ of degree $n \geq 1$. The totality of polynomials $r(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ with coefficients in $\mathbb{Q}$ and with addition and multiplication modulo $G(x)$ forms a ring.

Theorem 9.16: The rings of polynomials is a field iff $G(x)$ is an irreducible polynomial. If $G(x)$ is the minimal polynomial of the algebraic number ξ, then this field is isomorphic to $\mathbb{Q}(\xi)$.

Theorem 9.17: If α is an algebraic number, there exists an algebraic integer b such that $b\alpha$ is an algebraic integer.

Theorem 9.20: Every quadratic field is of the form $\mathbb{Q}(\sqrt{m})$, where m is a square-free rational integer not equal to 1. Numbers of the form $a + b\sqrt{m}$ with rational integers a and b are integers of $\mathbb{Q}(\sqrt{m})$. These are the only integers of $\mathbb{Q}(\sqrt{m})$ if $m = 2$ or $3 \mod 4$. If $m \equiv 1 \mod 4$, the numbers $(a + b\sqrt{m})/2$, with odd rational integers a, b are also integers of $\mathbb{Q}(\sqrt{m})$ and there are no further integers.

Definition 9.8: The norm $N(\alpha)$ of a number $\alpha = (a + b\sqrt{m})/c$ in $(\mathbb{Q}(\sqrt{m})$ is the product of α and its conjugate, $\bar{\alpha} = (a - b\sqrt{m})/c$. $N(\alpha) = \alpha\bar{\alpha} = \frac{a^2 - b^2 m}{c^2}$.

Theorem 9.21: $N(\alpha) = 0$ iff $\alpha = 0$. $N(\alpha\beta) = N(\alpha N(\beta))$. The norm of an integer in $\mathbb{Q}(\sqrt{m})$ is a rational integer. If γ is an integer in $\mathbb{Q}(\sqrt{m})$, then $N(\gamma) = \pm 1$ iff γ is a unit.

Definition 9.9: An algebraic integer α, not a unit, in a quadratic field $\mathbb{Q}(\sqrt{m})$ is called a prime if it is divisible only by its associates and the units of the field.

Theorem 9.24: If the norm of an integer α in $\mathbb{Q}(\sqrt{m})$ is $\pm p$, where p is a rational prime, then α is a prime.

Theorem 9.25: Every integer in $\mathbb{Q}(\sqrt{m})$, not zero or a unit, can be factored into a product of primes.

10 The Partition Function

Definition 10.1: The partition function $p(n)$ is defined as the number of ways that the positive integer n can be written as a sum of positive integers, as in $n = a_1 + a_2 + \ + a_r$. The summands a_i are called the parts of the partition. Although the parts need not be distinct, two partitions are not considered as different if they differ only in the order of their parts. It is convenient to define $p(0) = 1$.

Definition 10.2:
$p_m(n)$: the number of partitions of n into parts no larger than m.
$p^o(n)$: the number of partitions of n into odd parts.
$p^d(n)$: the number of partitions of n into distinct parts.
$q^e(n)$: the number of partitions of n into an even number of distinct parts.
$q^o(n)$: the number of partitions of n into an odd number of distinct parts.
By convention, $p_m(0) = p^o(0) = p^d(0) = q^e(0) = 1, q^o(0) = 0$.

Theorem 10.1: We have

1. $p_m(n) = p(n), n \leq m$,
2. $p_m(n) \leq p(n), \forall n \geq 0$,
3. $p_m(n) = p_{m-1}(n) + p_m(n-m)$ if $n \geq m > 1$,
4. $p^d(n) = q^e(n) + q^o(n)$.

Theorem 10.2: For $n \geq 1$ we have $p^d(n) = p^o(n)$.

Theorem 10.3: The number of partitions of n into m parts is the same as the number of partitions of n having largest part m. Similarly, the number of partitions of n into at most m parts is equal to $p_m(n)$, the number of partitions of n into parts less than or equal to m.

Theorem 10.4: If $n \geq 0$:

$$q^e(n) = q^o(n) = \begin{cases} (-1)^j, & \text{if } n = (3j^2 \pm j)/2,\ j \in \mathbb{N}_0 \\ 0, & \text{otherwise} \end{cases}$$

Generating function for $p(n)$ is:

$$\prod_{n=1}^{\infty}(1-x^n)^{-1}=\sum_{n=0}^{\infty}p(n)x^n$$

Theorem 10.5: *Euler's identity.* For any positive integer n:

$$p(n)=\sum_j(-1)^{j+1}p\left(n-\frac{1}{2}\left(3j^2+j\right)\right)+\sum_j(-1)^{j+1}p\left(n-\frac{1}{2}\left(3j^2-j\right)\right)$$

Theorem 10.6: Suppose $0\leq x<1$ and let $\phi_m(x)=\prod_{n=1}^{m}(1-x^n)$. Then $\sum_{n=0}^{\infty}p_m(n)x^n$ converges and $\displaystyle\sum_{n=0}^{\infty}p_m(n)x^n=\frac{1}{\phi_m(x)}$.

Theorem 10.14: If p is a prime and $0\leq x<1$, then

$$\frac{\phi(x^p)}{\phi(x)^p}=1+p\sum_{j=1}^{\infty}a_jx^j$$

where every a_j is an integer.

11 The Density of Sequences of Integers

The number of positive integers in a set $\mathcal{A}$ that are less than or equal to x is denoted by $A(x)$.

Definition 11.1: The asymptotic density of a set $\mathcal{A}$ is $\delta_1(\mathcal{A})=\lim\limits_{n\to\infty}\inf\frac{A(n)}{n}$. In case the sequence $\frac{A(n)}{n}$ has a limit, we say that $\mathcal{A}$ has a natural density $\delta(\mathcal{A})$. If $\mathcal{A}$ is a finite sequence, $\delta(\mathcal{A})=0$.

Theorem 11.1: If $\mathcal{A}$ is an infinite sequence, then $\delta_1(\mathcal{A})=\lim\limits_{n\to\infty}\inf\frac{n}{a_n}$. If $\delta(\mathcal{A})$ exists, then $\delta(\mathcal{A})=\lim\limits_{n\to\infty}\frac{n}{a_n}$.

Theorem 11.2: every integer greater than 1 ca be written as a sum of two square-free integers.

Lemma 11.3: For every positive integer n, if $Q(n)$ denotes the number of square-free integers among $1, 2, \cdots, n$, then $Q(n) > n/2$.

Definition 11.2: The Schnirelmann density $d(\mathcal{A})$ of a set $\mathcal{A}$ of non-negative integers is $d(\mathcal{A}) = \inf_{n \geq 1} \frac{A(n)}{n}$.

Definition 11.3: Assume that $0 \in \mathcal{A}$ and $0 \in \mathcal{B}$. The sum of $\mathcal{A} + \mathcal{B}$ of the sets A and B is the collection of all integers of the form $a + b$ where $a \in A$ and $b \in B$.