Introduction

Definition: Natural Numbers, Integers
Natural numbers: $\mathbb{N}=\{0,1,2,\ldots\}$.
Integers: $\mathbb{Z}=\{0,\pm1,\pm2,\ldots\}$.

Definition: Divisor
If $a\in\mathbb{Z}$ can be writeen as $a=bc$ where $b,c\in\mathbb{Z}$, then we say a is divisible by b or, b divides a (denoted $b|a$), or b is a divisor of a .

Definition: Prime
We call a number $p\geq 2$ prime if its only positive divisors are 1 and p .

Definition: Congruent
If $d\geq 2$, $d\in\mathbb{N}$, we say integers a and b are congruent modulo d if $d|(a-b)$ and write it $a\equiv b(\operatorname{mod} d)$.

Examples of Number Theory Questions
1. What are the solutions to $a^2+b^2=c^2$?
   Answer: $a=st$, $b=\frac{s^2-t^2}{2}$, $c=\frac{s^2+t^2}{2}$.
2. Fundamental Theorem of Arithmetic. Each integer can be written as a product of primes; moreover, the representation is unique up to the order of factors.
3. Theorem (Euclid). There are infinitely many prime numbers.
4. Suppose $(a,b)=1$, i.e. a and d have no common divisors except 1. Are there infinitely many primes $p\equiv a(\operatorname{mod} d)$? Equivalently, are there infinitely many prime values of the linear polynomial $dx+a, x\in\mathbb{Z}$?
   Answer: Yes (Dirichlet, 1837).
5. Are there infinitely many primes of the form $p=x^2+1, x\in\mathbb{Z}$?
   Not known, expect yes. It is known that there are infinitely many numbers $n=x^2+1$ such that n is either prime or has 2 prime factors.
6. What primes can be written as $p=a^2+b^2$? Answer: If $p=2$ or $p\equiv 1(\operatorname{mod} 4)$.
   What numbers can be written as $p=a^2+b^2$?
7. For $n\geq 3$, what are the solutions to $a^n+b^n=c^n$?
   Answer: No solution! Fermat's Last Theorem.
8. Are there infinitely many primes p such that $p+2$ is prime?
   Not known, expect yes.
9. Goldbach's Conjectre (1742). Every even number $n\geq 4$ can be written as $n=p_1+p_2$.
   Is every odd number ≥ 7 the sum of three primes? Yes for every n sufficiently large (Vinogruber, 1937).
10. Theorem (Friedlander and Iwaniec, 1998). There exists infinitely many primes of the form $p=a^2+b^4$.
    Theorem (Heath and Brown). There exists infinitely many primes of the form $p=a^2+2b^3$.
11. Prime Number Theorem (1896). Let $\pi(x)=\sum_{p<x,\, p\,\text{prime}} 1$. Then $\pi(x)\sim\frac{x}{\log x}$.

Pythagorean Triple

Definition: Pythagorean Triple
A Pythagorean triple (a,b,c) is integers a , b , c satisfying $a^2+b^2=c^2$.

Definition: Primitive Pythagorean Triple

A Pythagorean triple (a, b, c) is called primitive if a, b, c have no common divisors > 1.

Observations

1. One of a, b, c in a primitive Pythagorean triple must be even, the other two must be odd.
2. Either a or b must be even.
   Proof: Suppose otherwise, i.e a and b are odd and c is even. Then $a=2m+1$, $b=2n+1$, $c=2k$. Then $(2m+1)^2+(2n+1)^2=(2k)^2 \Leftrightarrow 4m^2+4m+4n^2+4n+2=4k^2$. However, $4 \nmid (4m^2+4m+4n^2+4n+2)$ but $4 \mid 4k^2$.
3. Assume b is even. $a^2=(c-b)(c+b)$. $(c-b)$ and $(c+b)$ are relatively prime.
   Proof: Suppose $d \mid (c-b)$ and $d \mid (c+b)$. Then $d \mid a^2$, so d is odd. Also, $d \mid ((c-b)+(c+b))=2c$ and $d \mid ((c+b)-(c-b))=2b$, so $d \mid 2\gcd(c, b)$. So $d \mid 2$ since (a, b, c) primitive. Since d is odd, $d=1$.
4. $(c-b)$ and $(c+b)$ are squares.
   Proof: $a^2=(c-b)(c+b)$ is a square. By fundamental theorem of arithmetic, $a^2=p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_j^{2\alpha_j}$. Since $(c-b)$ and $(c+b)$ are relatively prime, they are squares.

Theorem

Every primitive Pythorean triple (a, b, c) with b even and a and c odd is given by the formulas $a=st$, $b=\dfrac{-s^2+t^2}{2}$, $c=\dfrac{s^2+t^2}{2}$, where $t>s\geq 1$ are relatively prime odd integers.

Proof: $(c-b)$ and $(c+b)$ are relatively prime, squares, and odd, so $c-b=s^2$, $c+b=t^2$ for some $t>s\geq 1$ relatively prime odd integers. Solving for a, b, c, we get $a=st$, $b=\dfrac{-s^2+t^2}{2}$, $c=\dfrac{s^2+t^2}{2}$.

Lemma

Consider the a line with slope m passing through $(-1, 0)$ of the unit circle. For every $m \in \mathbb{Q}$, we get a rational solution $(x, y)=\left(\dfrac{1-m^2}{1+m^2}, \dfrac{2m}{1+m^2}\right)$. Conversely, given a point (x_1, y_1) with rational coordinates on the unit circle, the slope of the line through (x_1, y_1) and $(-1, 0)$ is a rational number.

Theorem

Every point on the unit circle $x^2+y^2=1$ whose coordinates are rational can be obtained from the formula $(x, y)=\left(\dfrac{1-m^2}{1+m^2}, \dfrac{2m}{1+m^2}\right)$ by substituting rationals numbers for m.

Note: The exception is $(-1, 0)$ which corresponds to the vertical line.

Corollary

Writing $m=\dfrac{u}{v}$ and clearing dominators, we get $(x, y)=\left(\dfrac{u^2-v^2}{u^2+v^2}, \dfrac{2uv}{u^2+v^2}\right)$. Then the solution to the Pythagorean triple is $(a, b, c)=(u^2-v^2, 2uv, u^2+v^2)$.

Greatest Common Divisors and the Euclidean Algorithm

Definition: Greatest Common Divisor

Given $a, b \in \mathbb{N}$, $a, b \geq 1$, we call $d \in \mathbb{N}$ the greastest common divisor of a and b if the following hold:

1. $d|a$ and $d|b$.
2. If $d'|a$ and $d'|b$, then $d'|d$.

Denote such d by $\gcd(a, b)$ or (a, b).

Euclidean Algorithm

Given $a, b \in \mathbb{N}$, $a > b$, can write

$$\begin{gathered} a = q_1 \cdot b + r_1 \quad (*_1) \\ b = q_2 \cdot r_1 + r_2 \quad (*_2) \\ r_1 = q_3 \cdot r_2 + r_3 \quad (*_3) \\ \vdots \\ r_{n-3} = q_{n-1} \cdot r_{n-2} + r_{n-1} \quad (*_{n-1}) \\ r_{n-2} = q_n \cdot r_{n-1} + r_n \quad (*_n) \\ r_{n-1} = q_{n+1} \cdot r_n + 0 \quad (*_{n+1}) \end{gathered}$$

Proof: The algorithm terminates because $r_1 < b$ by $(*_1)$, $r_2 < r_1$ by $(*_2)$, etc. Finally, $r_n < r_{n-1}$ by $(*_n)$.

Claim

r_n, the last non-zero remainder, gives $\gcd(a, b)$.

Proof:

1. $r_n|r_{n-1}$ by $(*_{n+1})$, $r_n|r_{n-2}$ by $(*_n)$, $r_n|r_{n-3}$ by $(*_{n-1})$, etc. So $r_n|b$ by $(*_2)$ and $r_n|a$ by $(*_1)$.
2. Suppose some $d|a$ and $d|b$. Then $d|r_1$ by $(*_1)$, $d|r_2$ by $(*_2)$, etc. Finally, $d|r_n$ by $(*_n)$.

Linear Equations

Given $a, b, c \in \mathbb{Z}$, what are the solutions to $ax + by = c \ \ , x, y \in \mathbb{Z}$?

Claim

Let $S = \{ax + by : x, y \in \mathbb{Z}\}$. Then $S = d\mathbb{Z} \overset{\text{def}}{=} \{dz : z \in \mathbb{Z}\}$ where $d = \gcd(a, b)$.

Factorization and the Fundamental Theorem of Arithmetic

Claim

If p is prime and $p|ab$, then $p|a$ or $p|b$.

Theorem: Prime Divisibility Property

If p is prime and $p|a_1 \cdots a_r$, then $p|a_j$ for some $j = 1, \ldots, r$.

Theorem: Fundamental Theorem of Arithmetic

Any integer $n \geq 2$ can be factored into a product of primes (not necessarily distinct) $n = p_1 \cdots p_r$ in a unique way (up to order of factors).

Congruences

Theorem: Linear Congruence Theorem
Let $a, c, m \in \mathbb{Z}$ and $g = \gcd(a, m)$.

1. If $g \nmid c$, then the congruence $a x \equiv c \pmod{m}$ has no solutions.
2. If $g \mid c$, then the congruence $a x \equiv c \pmod{m}$ has exactly g congruent solutions They are given by $x = x_0 \frac{c}{g} + k \frac{m}{g},\ k \in \mathbb{Z}$ where (x_0, y_0) is a solution to $a x - m y = g$.

Fermat's Little Theorem

Theorem: Fermat's Little Theorem
If p is prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Euler's Phi Function and Möbius Inversion Formula

Definition: Arithmetic Function
An arithmetic function is a complex valued function defined on $\{1, 2, \ldots\}$.

Examples

1. Möbius function: $\mu(n) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } \exists\, p \text{ such that } p^2 \mid n \\ (-1)^k & \text{if } n = p_1 \cdots p_k \text{ distinct primes} \end{cases}$.
2. $f(n) = 1\ \forall\, n$.
3. Euler's phi function: $\varphi(n) = \#\{j \mid 1 \le j \le n, (j, n) = 1\}$.
4. Von Mangoldt function: $\Lambda(n) = \begin{cases} \log p & \text{if } n = p^\alpha \text{ for some } p \text{ and } \alpha \\ 0 & \text{otherwise} \end{cases}$.

Definition: Multiplicative
An arithmetic function f is called multiplicative if $f(m \times n) = f(m) f(n)\ \forall\, (m, n) = 1$.

Definition: Completely Multiplicative
An arithmetic function f is called completely multiplicative if $f(m \times n) = f(m) f(n)\ \forall\, m, n$.

Note
The product of two (completely) multiplicative functions is (completely) multiplicative.

Examples

1. $f(n) = 1\ \forall\, n$ is multiplicative and completely multiplicative.
2. The Möbius function μ is multiplicative but not completely multiplicative.
3. The von Mangoldt function Λ is not multiplicative.

Lemma
$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{otherwise} \end{cases}$.

Theorem: Möbius Inversion Formula

Suppose f and g are arithmetic functions. Then for all n, $f(n) = \sum_{d|n} g(d) \Leftrightarrow g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$.

Lemma

If g is multiplicative, then $f(n) = \sum_{d|n} g(d)$ is also multiplicative.

Lemma

Euler's phi function is defined as $\varphi(n) = \#\{j | 1 \le j \le n, (j,n)=1\}$. Then $\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$.

Euler's Formula and Chinese Remainder Theorem

Theorem: Euler's Formula
If $(a,m)=1$, then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Note
Since $\varphi(p) = p-1$, Euler's Formula generalizes Fermat's Little Theorem.

Theorem: Chinese Remainder Theorem
If $(m,n)=1$ and $b, c \in \mathbb{Z}$, then $x \equiv b \pmod{m}$ and $x \equiv c \pmod{n}$ are simultaneously satisfied for a unique x with $0 \le x < mn$.

Theorem
There are infinitely many primes $p \equiv 3 \pmod{4}$.

Mersenne Primes and Perfect Numbers

Theorem
If $a^b - 1$ is prime for some $a, b \ge 2$, then $a=2$ and b is prime.

Definition: Mersenne Prime
A Mersenne prime p is a prime of the form $p = 2^q - 1$.

Definition

Define the arithmetic function σ as $\sigma(n) = \sum_{d|n} d$.

Definition: Perfect Number
A number n is perfect if $\sigma(n)=2n$.

Theorem: Euclid's Perfect Number Formula
If 2^p-1 is prime, then $2^{p-1}(2^p-1)$ is perfect.

Theorem: Euler's Perfect Number Theorem
Any even perfect number n is of the form $n=2^{p-1}(2^p-1)$ where 2^p-1 is a Mersenne prime.

Conjectures
1. There are no odd perfect numbers.
2. There are infinitely many Mersenne primes.

Theorem (Lagrange)
If p is prime, and $f(x)=\sum_{i=0}^{n} a_i x^i$ with $(a_n, p)=1$, then $f(x)\equiv 0 \pmod{p}$ has at most n incongruent solutions modulo p.

Powers Modulo *m* and Successive Squaring

Algorithm
To compute $a^k \pmod{m}$,
1. Write k as sums of powers of 2 (binary expansion); so $k=u_0+u_1 2+\cdots+u_r 2^r$ where each $u_i=0$ or 1.
2. Make a table of powers of $a \pmod{m}$ using successive squaring: $a^{2^i}=A_{i-1}^2=A_i$, $i=0,1,\ldots,r$.
3. $a^k\equiv A_0^{u_0}\cdots A_r^{u_r} \pmod{m}$.

Computing k^{th} Roots Modulo *m*
Find x such that $x^k\equiv b \pmod{m}$.

Algorithm
Assume $\gcd(b, m)=1$ and $\gcd(k, \phi(m))=1$. To solve $x^k\equiv b \pmod{m}$,
1. Compute $\phi(m)$.
2. Find positive integers u and v such that $ku-\phi(m)v=1$.
3. Compute $b^u \pmod{m}$ by successive squaring.

Powers, Roots, and "Unbreakable" Codes

Setup
1. Choose two large primes p and q.

2. Compute $m = pq$ and $\phi(m) = (p-1)(q-1)$.
3. Choose k such that $\gcd(k, \phi(m)) = 1$.
4. Publish k and m.

Encryption
1. Convert message into a string of digits.
2. Break the string of digits into numbers less than m. So the message is a list of numbers $a_{1,} \ldots, a_r$.
3. Use successive squaring to compute $b_i = a_i^k (\operatorname{mod} m)$ for each $i = 1, \ldots, r$. The list $b_{1,} \ldots, b_r$ is the encrypted message.

Decryption
1. Given the list $b_{1,} \ldots, b_r$, solve $x^k = b_i (\operatorname{mod} m)$.
2. Since $\phi(m)$ is known, the original message $a_{1,} \ldots, a_r$ can be recovered easily.

Primality Testing and Carmichael Numbers

Definition: Witness
A number a is a witness for n if $a^n \neq a (\operatorname{mod} n)$.

Note
By Fermat's Little Theorem, if p is prime, $a^p \equiv a (\operatorname{mod} p)$ for all a. Hence, if n prime, n has no witnesses.

Definition: Carmichael Number
A Carmichael number is a composite number which has no witnesses.

Claim
1. Every Carmichael number n is odd.
2. Every Carmichael number is a product of distinct primes.

Theorem: Korselt's Criterion for Carmichael Numbers
n is Carmichael if and only if the following three conditions hold:
1. n is odd.
2. For all primes $p | n$, $p^2 \nmid n$.
3. For all primes $p | n$, $(p-1) \nmid (n-1)$.

Definition: Primitive Root
A primitive root of a number n is a number g such that $g^j \neq 1 (\operatorname{mod} n)$ $\forall 1 \leq j \leq \phi(n) - 1$.

Lemma
Any prime number has a primitive root.

Lemma
Let p be an odd prime. Write $p - 1 = 2^k q$ where q is odd. Let $(a, p) = 1$. Then (at least) one of the following is true:
1. $a^q \equiv 1 (\operatorname{mod} p)$.
2. One of the numbers $a^q, a^{2q}, q^{4q}, \ldots, a^{2^{k-1} q}$ is congruent to -1 modulus p.

Theorem: Rabin-Miller Test for Composite Numbers
Let n be an odd integer and write $n-1=2^k q$ with q is odd. If both of the following are true for some a not divisible by n, then n is composite:

1. $a^q \neq 1 (\mod p)$.
2. $a^{2^i q} \neq -1 (\mod n)$ $\forall\, 0 \leq i \leq k-1$.

Definition: Rabin-Miller Witness
A Rabin-Miller witness for n is a number a for which the Rabin-Miller test proves n is composite.

Notes

- If p is prime, then p has no Rabin-Miller witnesses.
- If n is odd and composite, at least 75% of all numbers between 1 and $n-1$ are Rabin-Miller witnesses for n.
- If the Generalized Riemann Hypothesis holds, Rabin-Miller can provide primality testing in polynomial time.

Powers Modulo *p* and Primitive Roots

Definition: Order
Let a and n be positive integers with $(a, n)=1$. The least positive integer d such that $a^d \equiv 1 (\mod n)$ is called the order of a modulo n, and a is said to belong to d.

Note
By Euler's formula, the order exists and is at most $\phi(n)$. In fact, the order d divides every k such that $a^k \equiv 1 (\mod n)$.

Definition: Primitive Root
A primitive root modulo n is a number that belongs to $\phi(n)$.

Notation
$e_n(a)$ is the smallest exponent $e \geq 1$ such that $a^e \equiv 1 (\mod n)$.

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

Lemma
Let p be prime. For each $d | p-1$, let $\psi(d)$ denote the number of a's with $1 \leq a \leq p-1$ and $e_p(a)=d$ (in particular, $\psi(p-1)$ is the number of primitive roots modulo p). Then $\psi(d)=\phi(d)$ $\forall\, d | p-1$.

Theorem
Every prime p has a primitive root. More precisely, there are exactly $\phi(p-1)$ primitive roots.

Artin's Conjecture
2 is a primitive root for infinitely many primes.

Generalized Artin's Conjecture
Let $a \neq 1$ and not a perfect square. Then there are infinitely many primes p such that a is a primitive root modulo p.

Theorem
There are at most three numbers which are not primitive roots for infinitely many primes.

Claim
Let p be an odd prime; let g be a primitive root modulo p. Then there exists $x \in \mathbb{Z}$ such that $g' = g + p x$ is a primitive root modulo p^j for all $j \geq 1$.

Theorem
n has a primitive root if and only if $n = 2$ or $n = 4$ or $n = p^j$ or $n = 2 p^j$ where p is an odd prime and $j \geq 1$.

Primitive Roots and Indices

Definition: Index
Let g be a primitive root modulo p. Then $g, g^{2,} \ldots, g^{p-1}$ represent all numbers $1,2,\ldots, p-1 (\text{mod } p)$, i.e. for all $1 \leq a \leq p-1$, $a \equiv g^k (\text{mod } p)$ for a unique $k (\text{mod } p-1)$. Define $I(a) = k$ to be the index of a modulo p for the base g.

Theorem: Index Rules
- Product rule: $I(a b) \equiv I(a) + I(b) (\text{mod } p-1)$.
- Power rule: $I(a^k) \equiv k\, I(a) (\text{mod } p-1)$.

Squares Modulo *p*
Look at $x^2 \equiv a (\text{mod } p)$.

Note
$(p-b)^2 \equiv b (\text{mod } p)$.

Definition: Quadratic Residue, Quadratic Non-Residue
Let p be odd. A quadratic residue modulo p (QR) is a number congruent to a square modulo p. A quadratic non-residue modulo p (NR) is a number not congruent to a square modulo p.

Theorem
Let p be an odd prime. Then there are exactly $\frac{p-1}{2}$ quadratic residues modulo p and $\frac{p-1}{2}$ quadratic non-residues modulo p.

Note
Let g be a primitive root modulo p. Then $g^2 g^{4,} \ldots g^{p-1}$ are quadratic residues modulo p and $g, g^{3,} \ldots g^{p-2}$ are quadratic non-residues modulo p.

Theorem
Let p be an odd prime. Then
1. The product of two quadratic residues modulo p is a quadratic residue modulo p.
2. The product of a quadratic residue modulo p and a quadratic non-residues modulo p is a quadratic non-residue modulo p.
3. The product of two quadratic non-residues modulo p is a quadratic residue modulo p.

Definition: Legendre Symbol
$\left(\frac{a}{p}\right)=\{\begin{matrix} 1 \text{ if } a \text{ is a QR } (\operatorname{mod} p) \\ -1 \text{ if } a \text{ is a NR } (\operatorname{mod} p) \end{matrix}$.

Theorem
If p is an odd prime, then $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$.

Note
By Fermat's Little Theorem, $a^{p-1}\equiv 1 (\operatorname{mod} p)$. Then $(a^{\frac{p-1}{2}})^2\equiv 1(\operatorname{mod} p)$, so $a^{\frac{p-1}{2}}\equiv\pm 1(\operatorname{mod} p)$.

Theorem: Euler's Criterion
Let p is an odd prime. Then $a^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right)(\operatorname{mod} p)$.

Theorem: Special Case of Quadratic Reciprocity
$\left(\frac{-1}{p}\right)=\{\begin{matrix} 1 \text{ if } p\equiv 1 (\operatorname{mod} 4) \\ -1 \text{ if } p\equiv -1 (\operatorname{mod} 4) \end{matrix}$.

Theorem
There are infinitely many primes $p\equiv 1 (\operatorname{mod} 4)$.

Quadratic Reciprocity

Definition: Numerically Least Residue
Given $a\in\mathbb{Z}$ and $n\geq 1$, define the numerically least residue of $a (\operatorname{mod} n)$ as that integer a' such that $a\equiv a' (\operatorname{mod} n)$ and $-\frac{1}{2}n<a'\leq\frac{1}{2}n$.

Lemma: Gauss's Lemma
Let p be an odd prime and $(a, p)=1$. Let a_j be the numerically least residue of $a\cdot j (\operatorname{mod} p)$ for $j=1,2,\ldots$. Then $\left(\frac{a}{p}\right)=(-1)^l$ where l is the number of $1\leq j\leq\frac{1}{2}(p-1)$ such that $a_j<0$.

Theorem: Law of Quadratic Reciprocity

If p and q are distinct odd primes, then $\left(\frac{1}{q}\right)\left(\frac{q}{p}\right)=(-1)^{(\frac{1}{4}(p-1)(q-1))}$, i.e. $\left(\frac{p}{q}\right)=\begin{cases}-\left(\frac{q}{p}\right), \text{if } p\equiv q\equiv 3 \pmod 4\\ \left(\frac{q}{p}\right), \text{otherwise}\end{cases}$.

Corollary

$\left(\frac{2}{p}\right)=(-1)^{(\frac{1}{8}(p^2-1))}$, i.e. 2 is a QR if $p\equiv\pm 1 \pmod 8$, 2 is a NR if $p\equiv\pm 3 \pmod 8$.

Jacobi Symbol: A Generalization of Legendre Symbol

Let n be odd, $n=p_1\cdots p_r$ (not necessarily distinct). Let $(a,n)=1$. Define $\left(\frac{a}{n}\right)=\left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_r}\right)$ where the symbols on the right hand side are Legendre symbols. If $n=1$, define $\left(\frac{a}{n}\right)=1$ for all a. If $(a,n)\neq 1$, define $\left(\frac{a}{n}\right)=0$.

Properties of the Jacobi Symbol

1. If $a\equiv a' \pmod n$, then $\left(\frac{a}{n}\right)=\left(\frac{a'}{n}\right)$.
2. $\left(\frac{a}{n}\right)=1$ does not imply a is a QR modulo n.
3. $\left(\frac{a}{n}\right)=-1$ does imply a is a NR modulo n.
4. If $(a,b)=1$, then $\left(\frac{ab}{n}\right)=\left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.
5. If $(a,mn)=1$ and m, n odd, then $\left(\frac{a}{mn}\right)=\left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.
6. $\left(\frac{-1}{n}\right)=(-1)^{\frac{1}{2}(n-1)}$, $\left(\frac{2}{n}\right)=(-1)^{\frac{1}{2}(n^2-1)}$.
7. If m, n odd and $(m,n)=1$, then $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=(-1)^{\frac{1}{4}(m-1)(n-1)}$.

Which Numbers Are Sums of Two Squares?

Lemma

Let p be a prime. Then p can be written as $p=a^2+b^2$ if and only if $p=2$ or $p\equiv 1 \pmod 4$.

Theorem

Let $n\in\mathbb{N}$. Then n can be written as $n=a^2+b^2$ if and only if every prime divisor p of n with $p\equiv 3 \pmod 4$ appears to an even power in the standard factorization of n.

Corollary

A number c is the hypotenuse of a primitive Pythagorean triple if and only if c is a product of primes, each of which is congruent to 1 modulo 4.

Theorem: Lagrange
Every natural number is the sum of 4 squares.

Theorem: Legendre, Gauss
n is the sum of 3 squares if and only if $n \neq 4^j(8\mathrm{k}+7)$, $j, k \in \mathbb{N}$.

Theorem
Every natural number is the sum of 3 triangular numbers, 5 pentagonal numbers, 6 hexagonal numbers, etc.

Theorem: Waring's Problem (proved by Hilbert)
Every natural number can be written as a sum of 9 cubes, 19 biquadrates, etc.

Theorem: Fermat' Last Theorem for Exponent 4
The equation $x^4 + y^4 = z^2$ has no solutions in positive integers.

Square-Triangular Numbers

Example
Are there squares that are triangular numbers? Yes! 1 and 36.

Theorem
1. Every solution to $x^2 - 2y^2 = 1$ is obtained by raising $3+2\sqrt{2}$ to powers, i.e. the solutions (x_k, y_k) can be found by multiplying out $x_k + y_k\sqrt{2} = (3+2\sqrt{2})^k$, $k = 1, 2, \ldots$.
2. Every square-triangular number $n^2 = \frac{m(m+1)}{2}$ is given by $n = \frac{x_k - 1}{2}$, $m = \frac{y_k}{2}$ where (x_k, y_k) are solutions to $x^2 - 2y^2 = 1$.

Theorem: Pell's Equation Theorem
Let D be a positive integer that is not a perfect square. Then Pell's equation $x^2 - Dy^2 = 1$ always has solutions in positive integers. If (x_1, y_1) is the solution with the smallest x_1 , then every solution (x_k, y_k) can be obtained by taking powers $x_k + y_k\sqrt{D} = (x_1 + y_1\sqrt{D})^k$, $k = 1, 2, \ldots$.

Diophantine Approximation

Theorem: Pigeonhole Principle (or Dirichlet Box Principle)
If there are more pigeons than pigeonholes, then there exists one hole that contains (at least) two pigeons.

Theorem: Dirichlet's Diophantine Approximation Theorem
Let D be a positive integer that is not a perfect square. Then there exists infinitely many pairs $(x, y) \in \mathbb{N}^2$ such that $|x - y\sqrt{D}| < \frac{1}{y}$.

Theorem: Dirichlet's Diophantine Approximation Theorem (version 2)

Let $\alpha>0$ be an irrational number. Then there exists infinitely many pairs $(x, y)\in\mathbb{N}^2$ such that $\left|\frac{x}{y}-\alpha\right|<\frac{1}{y^2}$.

Continued Fractions and Pell's Equation

Continued Fraction Expansion Algorithm

Given $\theta\in\mathbb{R}, \theta>0$, let $a_0=\lfloor\theta\rfloor$. If $\theta\neq a_0$, write $\theta=a_0+\frac{1}{\theta_1}$ and let $a_1=\lfloor\theta_1\rfloor$. If $\theta\neq a_0+\frac{1}{a_1}$, write $\theta_1=a_1+\frac{1}{\theta_2}$ and let $a_2=\lfloor\theta_2\rfloor$. Continue.

Notation

$$[a_0, a_1, \ldots, a_n]=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cdots}}.$$

Definition: Convergents

Let $\theta\in\mathbb{R}, \theta>0$. Define the n -th convergent to $\frac{b_n}{c_n}=[a_0, \ldots, a_n]$ in lowest terms.

Theorem

Let $\frac{b_n}{c_n}=[a_0, \ldots, a_n]$ (think of the a_i 's as variables; want to solve for b_n and c_n). Then

- the numerators $b_0, b_1, \cdots$ are given by the recursion formula $\begin{cases} b_0=a_0 \\ b_1=a_1 a_0+1 \\ b_n=a_n b_{n-1}+b_{n-2} \quad, n\geq 2\end{cases}$, and
- the denominators $c_0, c_1, \cdots$ are given by the recursion formula $\begin{cases} c_0=1 \\ c_1=a_1 \\ c_n=a_n c_{n-1}+c_{n-2} \quad, n\geq 2\end{cases}$.

Theorem

$b_{n-1}c_n-c_{n-1}b_n=(-1)^n$ for $n=1,2,\ldots$. Equivalently, $\frac{b_{n-1}}{c_{n-1}}-\frac{b_n}{c_n}=(-1)^n\frac{1}{c_n c_{n-1}}$

Note

- $\frac{b_{n-1}}{c_{n-1}}-\frac{b_n}{c_n}=(-1)^n\frac{1}{c_n c_{n-1}}$. By the recursion formula, $c_n\to\infty$. Hence $\left\{\frac{b_n}{c_n}\right\}_{n=1}^{\infty}$ is a Cauchy sequence and therefore converges.
- Since $\theta=[a_0, \ldots, a_{n-1}, \theta_n]\ \forall n$ and $0<\frac{1}{\theta_n}\leq\frac{1}{a_n}$, hence $\frac{1}{a_{n-1}}>\frac{1}{a_{n-1}+\frac{1}{\theta}}\geq\frac{1}{a_{n-1}+\frac{1}{a_n}}$, and so

  $a_{n-2}+\frac{1}{a_{n-1}}>a_{n-2}+\frac{1}{a_{n-1}+\frac{1}{\theta}}\geq a_{n-2}+\frac{1}{a_{n-1}+\frac{1}{a_n}}$. By continuing to a_0, we see that θ is in between $\frac{b_n}{c_n}$ and $\frac{b_{n-1}}{c_{n-1}}$.

Therefore the sequence $\left\{\frac{b_n}{c_n}\right\}_{n=1}^{\infty}$ converges to θ.

- There exists a bijective correspondence between rational numbers and finite continued fractions. Also, there is a bijection between irrational numbers and infinite continued fractions.

Lemma

Let $A=[a,\overline{b}]=[a,b,b,b,\ldots]$. Let $B=[\overline{b}]=[b,b,b,\ldots]$. Then $A=a+\frac{1}{B}$ and $B=b+\frac{1}{B}$.

Proposition

For any positive integers a and b, we have $\frac{2a-b}{2}+\frac{\sqrt{b^2+4}}{2}=[a,b,b,b,\ldots]$. In particular, $\frac{b+\sqrt{b^2+4}}{2}=[b,b,b,\ldots]$ and $\sqrt{a^2+1}=[a,2a,2a,2a,\ldots]$.

Theorem: Periodic Continued Fractions Theorem

1. Suppose the number A has periodic continued fraction $A=[a_1,\ldots,a_l,\overline{b_1,\ldots,b_m}]$. Then $A=\frac{r+s\sqrt{D}}{t}$ for some integers r, s, t, D, with $D>0$.
2. Let r, s, t, D be integers with $D>0$ and D not a square. Then the number $\frac{r+s\sqrt{D}}{t}$ has a periodic continued fraction.

Theorem

Let $D\in\mathbb{Z}$, $D>0$, and D not a square. Let $\sqrt{D}=[a,\overline{b_1,\ldots,b_m}]$. Let $\frac{\beta}{\gamma}=[a,b_1,\ldots,b_{m-1}]$. Then (β,γ) is the smallest solution to $x^2-Dy^2=(-1)^m$.

Theorem

Let $\sqrt{D}=[a,\overline{b_1,\ldots,b_m}]$. Let $\frac{\beta}{\gamma}=[a,b_1,\ldots,b_{m-1}]$. Then the smallest solution in positive integers to Pell's Equation $x^2-Dy^2=1$ is given by $(x_1,y_1)=\begin{cases}(\beta,\gamma) & \text{if } m \text{ even}\\ (\beta^2+\gamma^2 D,2\beta\gamma) & \text{if } m \text{ odd}\end{cases}$.

Irrational and Transcendental Numbers

Definition: Rational Number

A number x is rational if $ax+b=0$ for some $(a,b)\in\mathbb{Z},a^2+b^2>0$.

Definition: Algebraic Number

A number x is algebraic if there exists a polynomial P with integer coefficients such that $P(x)=0$.

Definition: Transcendental Number

A number x is transcendental if it is not algebraic.

Note

The real numbers are uncountable, i.e. there is no bijection between $\mathbb{N}$ and $\mathbb{R}$. On the other hand, the set of algebraic numbers is countable because the set of finite tuples $(a_{1,} \ldots, a_j)$ is countable. Hence there exists transcendental numbers (in fact, uncountably many).

Lemma

$\sqrt{2}$ is irrational.

Theorem: Liouville's Inequality

Let α be a root of the polynomial $f(x)=c_0 x^d + c_1 x^{d-1} + \cdots + c_{d-1} x + c_d$ with integer coefficients. Let $D > d$. Then there are only finitely many rationals $\frac{a}{b}$ such that $\left|\frac{a}{b}-\alpha\right| \le \frac{1}{b^D}$.

Note: Equivalent formulation is that there is a constant K_D such that $\left|\frac{a}{b}-\alpha\right| > \frac{K_D}{b^D}$ for all $\frac{a}{b} \in \mathbb{Q}$.

Lemma

Let $\beta = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$. Then for all $D > 1$ there are infinitely many rationals $\frac{a}{b}$ such that $\left|\frac{a}{b}-\beta\right| \le \frac{1}{b^D}$.

Corollary

β is transcendental.

Binomial Coefficients and Pascal's Triangle

Theorem

Let p be a prime. Then

1. $\binom{p}{k} = \begin{cases} 1 \pmod{p} & \text{if } k=0 \text{ or } k=p \\ 0 \pmod{p} & \text{if } 1 \le k \le p-1 \end{cases}$.
2. $(A+B)^p \equiv A^p + B^p \pmod{p}$.

Fibonacci Numbers

Definition: Fibonacci Numbers

$F_1 = 1$, $F_2 = 1$, $F_n = F_{n-1} + F_{n-2}$ for $n \ge 2$.

Theorem: Binet's Formula

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

Note

$[\bar{1}] = [1, 1, \ldots] = \frac{1+\sqrt{5}}{2}$. The n -th convergent is $\frac{F_{n+1}}{F_n}$.

Generating Functions and Sums of Powers

Definition: Generating Function

A sequence $\{a_n\}_{n=0}^{\infty}$ can be "packed" into a power series $A(x)=\sum_{n=0}^{\infty} a_n x^n$. This is called the generating function for $\{a_n\}_{n=0}^{\infty}$.

Examples

1. $a_n=1 \quad \forall n$. Then $G(x)=\sum_{n=0}^{\infty} x^n$ is the geometric series. $G(x)-x\,G(x)=1$, so $G(x)=\frac{1}{1-x}$.
2. $a_n=n \quad \forall n$. Then $N(x)=\sum_{n=0}^{\infty} n\,x^n$. By differentiating $G(x)$ and multiplying by x, we get $N(x)=\frac{x}{(1-x)^2}$.
3. $a_n=n^2 \quad \forall n$. Then $S(x)=\sum_{n=0}^{\infty} n^2 x^n$. By differentiating $N(x)$ and multiplying by x, we get $S(x)=\frac{x^2+x}{(1-x)^3}$.

Example

The generating function for the Fibonacci sequence is $F(x)=\frac{x}{1-x-x^2}=\sum_{n=1}^{\infty}\frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right)x^n$. This gives another proof to Binet's Formula.

Theorem

Let $F_k(n)=1^k+2^k+\cdots+n^k$.

- $F_1(n)=1+\ldots+n=\frac{n^2+n}{2}$.
- $F_{k-1}(n)=\frac{(n+1)^k-1}{k}-\frac{1}{k}\sum_{j=0}^{k-2}\binom{k}{j}F_j(n)$ (a linear recursive formula).