Division Algorithm

Let $a, b \in \mathbb{Z}$, $b > 0$. Then $\exists$ unique q, r such that

$$a = bq + r, \qquad 0 \le r < b$$

quotient (under q) — remainder (under r)

Corollary

Let $a, b \in \mathbb{Z}$, $b \neq 0$. Then $\exists\ q, r \in \mathbb{Z}$ such that

$$a = bq + r, \qquad 0 \le r \le |b|$$

Well ordering Principle (Axiom)

Every non-empty set of natural numbers contains a least element

Archimedean Principle

If $a, b \in \mathbb{N}$ then $\exists\ n \in \mathbb{N}$ such that $bn > a$

Exercise: use the well ordering principle to prove the division algorithm

Divisors

Let $a, b \in \mathbb{Z}$. We say that a divides b if $\exists\, c \in \mathbb{Z}$ such that

$$b = ca$$

We write $a \mid b$ and say that a is a factor or divisor of b, and b is a multiple of a

Theorem

Let $a, b, c, d \in \mathbb{Z}$ ($\setminus \{0\}$ where necessary)

(1) $a \mid b$ iff $-a \mid b$

(2) $a \mid 0$, $1 \mid a$, $a \mid a$

(3) $a \mid 1$ iff $a = \pm 1$

(4) If $a \mid b$ and $b \mid c$

then $ab \mid cd$

(5) If $a \mid b$ and $b \mid c$ then $a \mid c$

(6) If $a \mid b$ and $b \mid a$ then $a = \pm b$

(7) If $a \mid b$, $b \neq 0$, then $|a| \leq |b|$

(8) If $a \mid b$ and $a \mid c$

then $a \mid (ax + cy)$ $\forall$ $x, y \in \mathbb{Z}$

Definition

Let $a, b \in \mathbb{Z}$. If $c \in \mathbb{Z}$ is such that $c \mid a$ and $c \mid b$ then c is a <u>common divisor</u> of a and b

If d is a common divisor of a and b and $d \geq c$, $\forall$ common divisors c of a and b, then d is the greatest common divisor of a and b. This is denoted

$\gcd(a, b) = \text{hcf}(a, b)$

or more usually (a, b)

Euclid's Algorithm

How to find (a,b)?

Method: Repeated use of division algorithm

Assume $a > b$. $\exists\ q_1, r_1 \in \mathbb{Z}$ st

$$a = bq_1 + r_1 \qquad 0 \leq r_1 < b$$

If $r_1 = 0$ STOP

as $b \mid a$ and $(a,b) = b$

Otherwise consider b and r_1. Find q_2, r_2 st

$$b = q_2 r_1 + r_2, \qquad 0 \leq r_2 < r_1$$

If $r_2 = 0$, STOP

Otherwise continue: find $q_3, r_3 \in \mathbb{Z}$ st

$$r_1 = q_3 r_3 + r_3 \qquad , \quad 0 \leq r_3 < r_2$$

Claim

The last non-zero remainder is (a,b)

Theorem

If $d = (a, b)$, then $\exists \; x, y \in \mathbb{Z}$ st

$d = ax + by$

Proof - Work Euclids Algorithms backwards

Corollary

Let $a, b, x, y \in \mathbb{Z}$, with $d = (a, b)$ then

$ax + by$ is a multiple of d

so $ax + by = n$ has solutions $x, y \in \mathbb{Z}$ iff d / n

Definition

If $(a, b) = 1$ we say a and b are co-prime

Corollary

$(a, b) = 1$ iff $\exists \; x, y \in \mathbb{Z}$ st

$ax + by = 1$

Corollary

If $d = (a,b)$

then $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

Corollary

If $a | c$, $b | c$ and $(a,b) = 1$
then

$$ab | c$$

Euclid's Lemma

If $a | bc$ and $(a,b) = 1$, then $a | c$

Proof

As $(a,b) = 1$

$\exists$ $x, y \in \mathbb{Z}$ st

$$ax + by = 1$$

Hence $cax + cby = c$

and $a | c$

Diophantine Equations

Linear, $a, b, c \in \mathbb{Z}$. Find $x, y \in \mathbb{Z}$ st

$$ax + by = c$$

This has solutions iff $(a,b) \mid c$

Given one solution x_0, y_0 ~~the~~ other solutions are given by

$$x_r = x_0 + \frac{b}{(a,b)} r$$

$$y_r = y_0 - \frac{a}{(a,b)} r$$

Suppose x', y' is another solution

$$c = ax_0 + by_0 = ax' + by'$$

$$a(x_0 - x') = b(y' - y_0)$$

Divide out (a,b) and use Euclid's Lemma

Primes

An integer $p > 1$ is prime if its only divisors are 1 and p

Questions

(1) Is there a largest? NO

(2) Is there a formula for the nth prime? NO

(3) How many primes are less than some given N

$$\sim \frac{N}{\log N}$$

Prime number theorem

Theorem

Let p be prime $a, b \in \mathbb{Z} \setminus \{0\}$

(1) If $p \mid ab$ then $p \mid a$ or $p \mid b$

(2) Let $a_i \in \mathbb{Z}$, $i = 1, \dots, t$. If

$$p \mid \prod_{i=1}^{t} a_i$$

then $\exists\ i \in \{1, \dots, t\}$ st $p \mid a_i$

(3) Let $q_1, \dots, q_t$ be prime.

If $p \mid \prod_{i=1}^{t} q_i$

then $\exists\ i \in \{1, \dots, t\}$

st $p = q_i$

Fundamental Theorem of Arithmetic

Every natural number $n > 1$ can be written as a unique product of primes

Usually we write

$$n = \prod_{i=1}^{t} p_i^{\alpha_i}$$

p_i prime, $p_i \neq p_j$ $i \neq j$, $\alpha_i \in \mathbb{N}$

Theorem

There are infinitely many primes

Proof

Suppose it is not true and there are only finitely many primes

$p_1, p_2, \ldots, p_t$

Let $N = p_1 p_2 \ldots p_t + 1$

Clearly $N > p_i$, $i = 1, \ldots, t$ so

N is composite

Therefore it has a prime divisor q.
It is not possible for $q = p_i$
for any $i \in \{1, \ldots, t\}$. contradiction

Twin primes

Are there infinitely many twin primes? Unknown

is 3, 5 17, 19

It is possible arbitrarily long strings of composite numbers

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

Goldbach's Conjecture (1742)

Every even number is the sum of two ones or two primes

Congruences

Let $a, b \in \mathbb{Z}$, $n \in \mathbb{N} \setminus \{1\}$. We say

$a \equiv b \pmod{n}$ if $n \mid (a-b)$

ie $\exists\ k \in \mathbb{Z}$ st $(a-b) = nk$

Theorems

(1) $a \equiv a \pmod{n}$ (reflexive)

$\forall\ a \in \mathbb{Z}$, $n \in \mathbb{N} \setminus \{1\}$

(2) If $a \equiv b \pmod{n}$ (symmetric)

then $b \equiv a \pmod{n}$

(3) If $a \equiv b \pmod{n}$ (transitive)

and $b \equiv c \pmod{n}$

then $a \equiv c \pmod{n}$

(4) If $a \equiv b \pmod{n}$

and $c \equiv d \pmod{n}$

then $a + c \equiv b + d \pmod{n}$

and $ac \equiv bd \pmod{n}$

(5) If $a \equiv b \pmod{n}$

then $a + c \equiv b + c \pmod{n}$

$ac \equiv bc \pmod{n}$

(6) If $a \equiv b \pmod{n}$

then $a^k \equiv b^k \pmod{n}$ $\quad k \in \mathbb{N}$

Let $a \in \mathbb{Z}$, $n \in \mathbb{N}$. We know $\exists\, b, r \in \mathbb{Z}$ st

$$a = bn + r \quad , \quad 0 \le r < n$$

We say r is ~~the~~ least non-negative residue $\pmod{n}$

Any set of n numbers which are pairwise incongruent (mod n) is called a complete set of residues (mod n)

Linear Composition

I missed a bit

$ax \equiv b \pmod n$

~~the~~ $\exists$ u st

$ax - b = un$

So

$ax - un = b$

(1) When $(a, m) \mid b$

(2) If x_0 is a solution then other solution are

$x_0 + \frac{tm}{(a,m)}$ There are (a,m) incongruent solutions (mod n)

Simultaneous Linear Congruences

When does ~~the~~ systems

$x \equiv a_i \pmod{n_i}$

have solutions

Chinese Remainder Theorem

Let $n_1, \dots, n_t \in \mathbb{N} \setminus \{1\}$

and $a_1, \dots, a_t \in \mathbb{Z}$

Suppose

$(n_i, n_j) = 1, \quad i \neq j$

Then the system

$$x \equiv a_i \pmod{n_i}$$

has a unique solution $\left(\bmod \prod_{i=1}^{t} n_i\right)$

Non Linear Congruences

Let f be a polynomial of degree n,
Aim to solve

$$f(x) \equiv 0 \left(\bmod \prod_{i=1}^{t} p_i^{\alpha_i}\right) \qquad (\otimes)$$

1st reduction: This congruence equation has a solution iff

$f(x) = 0 \pmod{p_i^{\alpha_i}}$

has a solution for $i = 1, \ldots, t$

1 solution is x_i

To determine then a solution to (*)
solve the system

$x \equiv x_i \pmod{p_i^{\alpha_i}}$

using ~~the~~ CRT

2nd reduction:

We will show that solving

$f(x) \equiv 0 \pmod{p^\alpha}$ $\quad p$ a prime

reduces to solving

$f(x) \equiv 0 \pmod{p}$

Suppose x_0 is a solution to

$f(x) \equiv 0 \bmod p^\alpha$

we will use this to construct solutions $\pmod{p^{\alpha+1}}$

Use the Taylor polynomial of f

$$f(x_0 + tp^\alpha) = f(x_0) + tp^\alpha f'(x_0) + \frac{(tp^\alpha)^2}{2} f''(x_0) + \dots + \frac{(tp^\alpha)^n}{n!} f^{(n)}(x_0)$$

$\equiv 0 \pmod{p^{\alpha+1}}$

When is $x_0 + tp^\alpha$ a solution of

$$f(x) \equiv 0 \pmod{p^{\alpha+1}}$$

If $x_0 + tp^\alpha$ solves

$$f(x) \equiv 0 \pmod{p^{\alpha+1}}$$

we must have

$$f(x_0) + tp^\alpha f'(x_0) \equiv 0 \pmod{p^{\alpha+1}}$$

so we must have that

$$p \mid \left(\frac{f(x_0)}{p^\alpha} + tf'(x_0)\right)$$

ie $\dfrac{f(x_0)}{p^\alpha} + t f'(x_0) \equiv 0 \pmod{p}$

so $t f'(x_0) \equiv - \dfrac{f(x_0)}{p^\alpha} \pmod{p}$

If $p \nmid f'(x_0)$ we have a unique solution

Now consider ~~the~~ case $p \mid f'(x_0)$

$$f(x_0 + tp^\alpha) = f(x_0) + tp^\alpha f'(x_0) + \dots + \dots$$

$$\equiv 0 \pmod{p^{\alpha+1}}$$

If $f(x_0) \equiv 0 \pmod{p^{\alpha+1}}$ then

$f(x_0 + tp^\alpha) \equiv 0 \pmod{p^{\alpha+1}}$, $\forall t$

If $f(x_0) \not\equiv 0 \pmod{p^{\alpha+1}}$ then

~~there~~ are no t st

$f(x_0 + tp^\alpha) \equiv 0 \pmod{p^{\alpha+1}}$

Example

Solve,

$f(x) = x^3 - 2x^2 + 3x + 9 \equiv 0 \bmod 27$

(mod 3)

$x \equiv 0$, $x \equiv 2$ are the solutions (mod 3)

(mod 9)

$f(x) = x^3 - 2x^2 + 3x \equiv 0 \bmod 9$

$f'(x) = 3x - 4x + 3$

$x \equiv 0 \pmod 3$

$f'(0) = 3$ so $3 \mid f'(0)$

$x \equiv 0$ is also a solution (mod 9)

Hence, $0 + 3t$ is also a solution (mod 9) for each t. We have $0, 3, 6$

$x \equiv 2$ $\quad f'(2) = 7 \quad 3 \nmid f'(2)$

Find t st $tf'(2) \equiv -\frac{f(2)}{3} \pmod 3$

$7t \equiv -\frac{15}{3} = -5 \pmod 3$

$t \equiv 1 \pmod 3$

Here, $2 + 1 \cdot 3 = 5$ is a solution (mod 9)

For each solution $0, 3, 5, 6 \pmod 9$
we work up to (mod 27)

$f(x) = x^3 - 2x^2 + 3x + 9$

$f'(x) = 3x^2 - 4x + 3$

$\underline{x \equiv 0}$ $\quad f'(0) = 3, \quad 3 \mid f'(0)$

However $f(0) \not\equiv 0 \pmod{27}$

NO SOLUTIONS

$\underline{x \equiv 3}$ In this case $3 \mid f'(3)$

and $f(3) \equiv 0 \pmod{27}$

so we have solutions $3, 3+9, 3+18,$

ω 3, 12, 21 solutions mod 27

$x \equiv 6$ No soluts

$x \equiv 5$ has a unique solution

Definition

- Any solution $f: \mathbb{N} \longrightarrow \mathbb{R}$ is called arithmetic

An arithmetic function f is called multiplicative if

$$f(nm) = f(n) f(m)$$

when $(n, m) = 1$

$\mu(n)$ mobius function

$\pi(n)$ # of primes $\leq n$

$\varphi(n)$ # of numbers co prime to n and less than n

$\tau(n)$ # of divisors of n

$\omega(n)$ # of prime divisors of n

$\sigma(n)$ sum of divisors of n

φ

$\varphi(1) = 1$

$\varphi(2) = 1$

$\varphi(3) = 2$

$\varphi(4) = 2$

$\varphi(5) = 4$

$\varphi(6) = 2$

$\varphi(p) = p-1$, p a prime

Definition

If a is coprime to n then so is any x s.t. $x \equiv a \pmod{n}$. There are $\phi(n)$ equivalence classes coprime to n. Any set of $\phi(n)$ residues which are pairwise incongruent $\pmod{n}$ is called a reduced set of residues $\pmod{n}$

Theorem

If $a_1, \ldots, a_{\phi(n)}$ is a reduced set of residues $\pmod{n}$ and $(k,n) = 1$, then

$$ka_1, \ldots, ka_{\phi(n)}$$

is also a reduced set of residues $\pmod{n}$

Eulers Theorem

Let $n \in \mathbb{N} \setminus \{1\}$, $a \in \mathbb{Z}$, $(a,n) = 1$. Then

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

Proof

Let $r_1, \ldots, r_{\phi(n)}$ be a reduced set of residues (mod n) then $ar_1, \ldots, ar_{\phi(n)}$ is also such a set. Thus

$$ar_1 \ldots ar_{\phi(n)} \equiv r_1 \ldots r_{\phi(n)} \pmod n$$

$$\Rightarrow \quad a^{\phi(n)} \equiv 1 \pmod n$$

Corollary - Fermat's Little Theorem

Let p be a prime and $a \in \mathbb{Z}$, $(a,p)=1$. Then

$$a^{p-1} \equiv 1 \pmod p$$

Also

$$a^p \equiv a \pmod p, \quad \forall a \in \mathbb{Z}$$

Inverses

Suppose $(a,n)=1$

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

$$a \underbrace{a^{\phi(n)-1}}_{\text{Inverse}} \equiv 1 \pmod n$$

Example

$3^{2000000} \pmod{31}$

$2000000 = 30q + r_1$

$q = 66666$

$r = 20$

$\varphi(31) = 30$

We know $3^{30} \equiv 1 \pmod{31}$

$$3^{10^6} \equiv (3^{30})^{66666}\, 3^{20} \pmod{31}$$
$$\equiv 3^{30} \pmod{31}$$

Fact

If p is prime what is

$\varphi(p^t) = p^t - p^{t-1}$

Theorem

Suppose f is arithmetic and define

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

If f is multiplicative then so is F

Proof

We need to show $F(mn) = F(m)F(n)$ when $(m,n)=1$

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

If $d|mn$ and $(m,n)=1$ then we can write $d = d_1 d_2$ st

$$d_1|m, \quad d_2|n \qquad (d_1, d_2) = 1$$

$$F(mn) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2)$$

$$= \sum_{\substack{d_1 | m \\ d_2 | n}} f(d_1) f(d_2)$$

$$= \sum_{d_1 | m} f(d_1) \sum_{d_2 | n} f(d_2)$$

$$= F(m) F(n)$$

Lemma

τ and σ are multiplicative

Formulae for τ and σ

Let $\quad n = \prod_{n=1}^{t} p_i^{\alpha_i}$

Then $\quad \tau(n) = \tau\left(\prod_{n=1}^{t} p_i^{\alpha_i}\right)$

$$= \prod_{i=1}^{t} \tau\left(p_i^{\alpha_i}\right)$$

Similarly

$$\sigma(n) = \prod_{i=1}^{t} \sigma\left(p_i^{\alpha_i}\right)$$

Let p be prime

$\tau(p^k)$, $\sigma(p^k)$

$\tau(p^k) = k+1$

and $\tau(n) = \prod_{i=1}^{t} \tau(p_i^{\alpha_i})$

$= \prod_{i=1}^{t} (\alpha_i + 1)$

$\sigma(p^k) = 1 + p + p^2 + \dots + p^k$

$= \dfrac{p^{k+1} - 1}{p - 1}$

$\sigma(n) = \prod_{i=1}^{t} \dfrac{p_i^{\alpha_i + 1} - 1}{p_i - 1}$

Fact

ϕ is multiplicative

Let $m, n \in \mathbb{N}$, $(m,n)=1$

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

Consider the r^{th} row.

if $(m,r)=d>1$

then no element of the r^{th} row is coprime to m and therefore to mn

We only need to consider rows where $(m,r)=1$. There are $\phi(n)$ such rows.

$\phi(n)$ multiplicative continued

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

$5, 12+5, 24+5, \ldots, 173$
$5, 2, 14, 5, 2,$
$12, 15$
$\frac{60}{12} = 5$ $(12,15)=3$
n / mn
$n / \frac{mn}{d}$
$r \equiv \frac{nm}{d} + r \mod n$

Take the r^{th} row $(r, m) = 1$

$r, m+r, 2m+r, \ldots, (n-1)m+r$

These numbers are pairwise incongruent (mod n)

If $im+r \equiv jm+r \pmod n$ then $i \equiv j \pmod n$. This is a complete set of residues (mod n)

Thus there are $\phi(n)$ elements coprime to n (and also coprime to m)

Thus, there are $\phi(m)\phi(n)$ elements coprime to mn

so $\phi(mn) = \phi(m)\phi(n)$

and ϕ is multiplicative

Formulae for ϕ

We know

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

when p is prime

If $n = \prod_{i=1}^{t} p_i^{\alpha_i}$

~~then~~

$$\phi(n) = \prod_{i=1}^{t} \phi(p_i^{\alpha_i})$$

$$= \prod_{i=1}^{t} p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)$$

$$= n \prod_{i=1}^{t}\left(1 - \frac{1}{p_i}\right)$$

Lemma

Either $d(n) = 1$ or $d(n)$ is even.

Definition

A number n is <u>perfect</u> if it is the sum of its divisors which are less than n

6, 28, 496, 8128 are the only perfect numbers $< 10^6$

It is unknown if odd perfect numbers exist

So far only 48 perfect numbers have been found.

<u>Conjecture</u> - There are infinitely many prime numbers

Definition

p is a <u>Mersenne</u> prime if $2^p - 1$ is also prime

It is unknown if there are infinitely many such primes.

So far only 48 have been found

Theorem

A natural number n is perfect and even if it has the form

$$n = 2^{p-1}(2^p - 1)$$

where both p and $2^p - 1$ are prime, ie exactly one perfect number associated with each Mersenne prime

Proof

Suppose $n = 2^{p-1}(2^p - 1)$

where $2^p - 1$ is prime

($\Rightarrow p$ is prime)

We need to show n is perfect, ie

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

The divisors of n are

$1, 2, \ldots, 2^{p-1},$

$(2^p-1), 2(2^p-1), \ldots, 2^{p-1}(2^p-1)$

$1+2+\ldots 2^{p-1} = 2^p-1$

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

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

$= 2^p(2^p-1) = 2n$

Now suppose

$\sigma(n) = 2n$

We need to show n is of the form

$2^{p-1}(2^p-1)$

Where 2^p-1 and p are prime.
We can write

$n = 2^{k-1}n'$ where n' is odd

We have $\sigma(n) = \sigma(2^{k-1})\sigma(n')$

Also $\sigma(n) = 2n = 2^k n'$

Thus $2^k n' = (2^k - 1)\sigma(n')$

We have

$$2^k - 1 \mid n'$$

We can write

$$n' = (2^k - 1)n''$$

This gives

$$\sigma(n') = 2^k n''$$

Note that

$$n' + n'' = (2^k - 1)n'' + n''$$
$$= 2^k n'' = \sigma(n')$$

This implies $n'' = 1$ and n' is prime

Thus $n' = 2^k - 1$ prime and

$n = 2^{k-1}(2^k - 1)$ as required #

The Möbius Function

(1) $\mu(1) = 1$

(2) If $\exists$ prime p st $p^2 | n$ then $\mu(n) = 0$

(3) Otherwise

$n = \prod_{i=1}^{t} p_i$, p_i prime , $p_i \neq p_j$, $i \neq j$

Then $\mu(n) = (-1)^t$

$\mu(1) = 1$

$\mu(2) = -1$

$\mu(3) = -1$

$\mu(4) = 0$

$\mu(5) = -1$

$\mu(6) = 1$

μ is multiplicative

Lemma

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

Proof

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

As μ is multiplicative so if F

Let p be prime

$$F(p^k) = \sum_{d|p^k} \mu(d)$$

$$= \mu(1) + \mu(p) + \mu(p^2) + \dots + \mu(p^k)$$

$$= 1 - 1 + 0$$

$$= 0$$

Mobius Inversion Formula

Let $f : \mathbb{N} \longrightarrow \mathbb{R}$ and

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

Then

$$f(n) = \sum_{d|n} F(d)\mu\left(\frac{n}{d}\right)$$

$$= \sum_{d|n} F\left(\frac{n}{d}\right)\mu(d)$$

Proof

Consider

$$\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$$

$$= \sum_{d_1 d_2 = n} \mu(d_1) F(d_2)$$

$$= \sum_{d_1 d_2 = n} \mu(d_1) \sum_{d|d_2} f(d)$$

$$= \sum_{dd_1|n} \mu(d_1) f(d)$$

$$= \sum_{d|n} f(d) \underbrace{\sum_{d_1 | \frac{n}{d}} \mu(d_1)}_{\substack{=1 \text{ if } n=d \\ \text{otherwise } 0}}$$

$$= f(n) \quad \text{as required}$$

Lemma

$$\sum_{d|n} \varphi(d) = n \qquad \left(\sum_{d|n} \varphi\left(\tfrac{n}{d}\right) = n \right)$$

Corollary

φ is multiplicative

Proof

Notice that

$$\sum_{d|n} \#\{a \in \{1, \dots, n\} \mid (a,n) = d\}$$

$$= n$$

We have

$$\varphi\left(\frac{n}{d}\right) = \#\left\{a \in \left\{1,\dots,\frac{n}{d}\right\} \mid \left(a,\frac{n}{d}\right)=1\right\}$$

Exercise $\quad = \#\{a \in \{1,\dots,n\} \mid (a,n) = d\}$

Also $\varphi(n) = n\sum_{d|n} \frac{\mu(d)}{d}$ $\leftarrow$ Exercise

Size of the arithmetic functions

Notation O, $\ll$

We say $f(x) = O(g(x))$ or

$f(x) \ll g(x)$ if $\exists\, C$

st $f(x) \leq C g(x)$ for all appropriate x

If $f(x) \ll g(x) \ll f(x)$

we say say $f(x) \asymp g(x)$

comparable

Example

$x^2 = O(x^2+x) \qquad x \in [1, \infty)$

$x^2+x = O(x^2)$

$\tau(n)$, # of divisors of n

$$\liminf_{n \to \infty} \tau(n) = 2$$

$60 = 2^2 \cdot 3 \cdot 5$

$\tau(60) = 3 \cdot 2 \cdot 2 = 12$

$\tau(n)$ can be larger than any power of $(\log n)$

Let $\alpha \in \mathbb{R}^+$, then $\exists$ n st

$$\tau(n) \gg (\log n)^\alpha$$

Consider $n = 2^m$ so $\tau(n) = m+1$

$\log n = m \log 2$

$$m = \frac{\log n}{\log 2}$$

$$m+1 \approx \frac{\log n}{\log 2}$$

Consider instead

$$n = (2\cdot 3)^m \quad , \tau(n) = (m+1)^2$$

$$\log n = m \log 6$$

$$m = \frac{\log n}{\log 6}$$

$$\tau(n) = (m+1)^2 \approx \left(\frac{\log n}{\log 6}\right)^2$$

Theorem

$\tau(n) \ll n^{\delta} \quad \forall \ \delta > 0$

Lemma

Let f be multiplicative such that

$f(p^{\alpha}) \longrightarrow 0$

as $p^{\alpha} \longrightarrow \infty$ for p prime

Then $f(n) \longrightarrow 0$ as $n \longrightarrow \infty$

Proof of Lemma

Suppose $f(p^{\alpha}) \longrightarrow 0$ as $p^{\alpha} \longrightarrow \infty$

This implies

(1) $\exists \ A \in \mathbb{R}$ st $|f(p^{\alpha})| < A$

(2) $\exists \ B \in \mathbb{R}$ st $|f(p^{\alpha})| < 1 \quad p^{\alpha} > B$

(3) $\forall \ \varepsilon > 0$, $\exists \ N_{\varepsilon}$ st

$|f(p^{\alpha})| < \varepsilon \ , \quad p^{\alpha} > N_{\varepsilon}$

Let $n = \prod_{i=1}^{t} p_i^{\alpha_i}$

so $f(n) = \prod_{i=1}^{t} f(p_i^{\alpha_i})$

A finite number, C, of elements p^α are $< B$

Hence, $f(n) \le A^C$

For $\varepsilon > 0$ as $n \longrightarrow \infty$, eventually n will have a factor $p^\alpha > N_\varepsilon$ so

$f(n) \le \varepsilon A^C$

Thus $f(n) \longrightarrow 0$ as $n \longrightarrow \infty$

<u>Proof of Theorem</u>

$f(n) = n^{-\delta} \tau(n)$

so f is multiplicative

We have $f(p^\alpha) = p^{-\alpha\delta} \tau(p^\alpha)$

$= (\alpha + 1) p^{-\alpha\delta}$

Hence

$$f(p^\alpha) \leq \frac{2\alpha}{p^{\alpha\delta}} = \frac{2}{p^{\alpha\delta}} \frac{\log p^\alpha}{\log p}$$

$$\leq \frac{2}{\log 2} \frac{\log(p^\alpha)}{(p^\alpha)^\delta} \longrightarrow 0 \text{ as } p^\alpha \longrightarrow \infty$$

Hence $f(n) \longrightarrow 0$ as $n \longrightarrow \infty$

so $\tau(n) n^{-\delta} \longrightarrow 0$

$\Rightarrow \tau(n) \ll n^\delta$

Average order of τ?

$$\frac{1}{N} \sum_{n=1}^{N} \tau(n) \sim \log N$$

Size of $\phi(n)$?

Let $n = p^m$ then

$$\phi(n) = n\left(1 - \frac{1}{p}\right)$$

$$> n(1-\varepsilon) \text{ for } p \text{ sufficiently large}$$

Also, $\dfrac{\phi(n)}{n^{1-\delta}} \longrightarrow \infty$ as $n \longrightarrow \infty$

Average order?

Let $\Phi(N) = \sum_{n=1}^{N} \phi(n)$

Theorem

$$\Phi(N) = \frac{3N^2}{\pi^2} + O(N\log N)$$

Proof

$$\sum_{i=1}^{n} \phi(n) = \sum_{i=1}^{n} \sum_{d \mid i} \frac{i\mu(d)}{d}$$

Let $d' = \dfrac{i}{d}$

$$= \sum_{dd' \le n} d'\mu(d)$$

$$= \sum_{d=1}^{n} \mu(d) \sum_{d'=1}^{\left[\frac{n}{d}\right]} d'$$

$$= \frac{1}{2} \sum_{d=1}^{n} \mu(d)\left(\left[\frac{n}{d}\right]^2 - \left[\frac{n}{d}\right]\right)$$

$$= \frac{1}{2} \sum_{d=1}^{n} \mu(d) \left(\frac{n^2}{d^2} + O\left(\left[\frac{n}{d} \right] \right) \right)$$

$$= \frac{1}{2} n^2 \sum_{d=1}^{n} \frac{\mu(d)}{d^2} + O\left(n \sum_{d=1}^{n} \frac{1}{d} \right)$$

Lemma

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{m=1}^{\infty} \frac{\mu(m)}{m^2} = 1 \qquad , s > 1$$

Proof

Consider

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{m=1}^{\infty} \frac{\mu(m)}{m^s}$$

$$= \sum_{m,n=1}^{\infty} \frac{\mu(m)}{(mn)^s}$$

$$= \sum_{i=1}^{\infty} \frac{1}{i^s} \sum_{d \mid i} \mu(d)$$

$$= 1$$

Back to the theorem

$$= \frac{1}{2} n^2 \sum_{d=1}^{n} \frac{\mu(d)}{d^2} + O\left(n \sum_{d=1}^{n} \frac{1}{d}\right)$$

$$= \frac{1}{2} n^2 \left(\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} - \sum_{d=n+1}^{\infty} \frac{\mu(d)}{d^2} \right) + O(n \log n)$$

$$= \underbrace{\frac{3n^2}{\pi^2}}_{\text{from the lemma}} + n^2 O\left(\int_{n+1}^{\infty} \frac{dx}{x^2} \right) + O(n \log n)$$

$$= \frac{3n^2}{\pi^2} + O(n \log n) \quad \text{as required}$$

Size of $\pi(n)$?

Lemma

Let $n>1$, and for each prime p define $r(p)$ to be the unique integer such that

$$p^{r(p)} \leq 2n \leq p^{r(p)+1}$$

The following hold

(1) $2^n \leq \binom{2n}{n} \leq 2^{2n}$

(2) $\prod_{n<p<2n} p \,\Big|\, \binom{2n}{n}$

(3) $\binom{2n}{n} \,\Big|\, \prod_{p\leq 2n} p^{r(p)}$

(4) If $n>2$ and $\frac{2n}{3} < p \leq n$ then

$$p \nmid \binom{2n}{n}$$

(5) $\prod_{p\leq n} p < 4^n$

Chebychev's Theorem

For $n > 1$,

$$\frac{n}{8\log n} \le \pi(n) \le \frac{6n}{\log n}$$

Prime number theorem

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

Proof

part 2

$$n^{\pi(2n)-\pi(n)} < \prod_{n \le p < 2n} p \le \binom{2n}{n}$$

part 3

$$\le \prod_{p \le 2n} p^{r(p)}$$

def of $r(p)$

$$\le (2n)^{\pi(2n)}$$

From part 1 we have

$$n^{\pi(2n)-\pi(n)} \le 2^{2n}$$

$$2^n \le (2n)^{\pi(2n)}$$

Now let $n = 2^k$

Then $k\left(\pi(2^{k+1}) - \pi(2^k)\right) \le 2^{k+1}$ (1)

and $2^k \le (k+1)\,\pi(2^{k+1})$ (2)

We also have

$$\pi(2^{k+1}) \le 2^k$$

Then

$$(k+1)\pi(2^{k+1}) - k\pi(2^k)$$

$$\le 2^{k+1} + 2^k = 3 \cdot 2^k$$

This implies

$$(k+1)\pi(2^{k+1}) - k\pi(2^k) + k\pi(2^k) - (k-1)\pi(2^{k-1})$$

$$+ \ldots + \pi(2) - \pi(1)$$

$$< 3(2^k + 2^{k-1} + 2^{k-2} + \ldots + 1)$$

$$= 3 \cdot 2^{k+1}$$

Hence

$$\frac{2^{k+1}}{2(k+1)} \le \pi(2^{k+1}) \le \frac{3 \cdot 2^{k+1}}{k+1}$$

from (2)

Rename $k = m$

$$\frac{2^{m+1}}{2(m+1)} < \pi(2^{m+1}) < \frac{3 \cdot 2^{m+1}}{m+1}$$

$$\pi(2^k) \approx \frac{2^k}{\log(2^k)}$$

Now consider general $n \in \mathbb{N}$

Choose m such that

$$2^{m+1} \leq n < 2^{m+2}$$

Note that

$$\frac{k}{2} \leq \log(2^k) \leq k$$

Also note that $\pi(n)$ is a non decreasing function

$$\pi(n) \leq \pi(2^{m+2})$$

$$< \frac{3 \cdot 2^{m+2}}{m+2}$$

Aside

$$\frac{2^{m+1}}{2(m+1)} < \pi(2^{m+1}) < \frac{3 \cdot 2^{m+1}}{m+1}$$

$$2^{m+1} < n < 2^{m+2}$$

$$< \frac{6 \cdot 2^{m+1}}{\log(2^{m+2})} < \frac{6n}{\log n}$$

Also

$$\pi(n) > \pi(2^{m+1})$$

$$> \frac{2^{m+1}}{2(m+1)} = \frac{2^{m+2}}{8\left(\frac{m+2}{2}\right)}$$

$$> \frac{n}{8\log(2^{m+1})}$$

$$> \frac{n}{8\log n}$$

Corallary

$p_n \precsim n \log n$

Bertrand's Postulate

If $n \in \mathbb{N}$, $\exists$ prime satisfying

$$n < p \leq 2n$$

Quadratic Residues

Let $a, b, c \in \mathbb{Z}$. When does the congruence, with p prime

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

have solutions?

Suppose wlog $(a, p) = 1$

Also suppose p is odd

If $(a, p) = 1$ then $(4a, p) = 1$

Then

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

has solution iff

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}$$

$$(2ax + b)^2 - b^2 + 4ac \equiv 0 \pmod{p}$$

Let $y = 2ax + b$

$d = b^2 - 4ac$

The question then becomes

when does

$$y^2 \equiv d \pmod{p}$$

have solutions?

Definition

If $x^2 \equiv a \pmod{p}$ has a solution then we say a is a quadratic residue of p, otherwise a is a quadratic non residue of p

Example

$p = 7$

$$1^2 \equiv 1 \pmod{7}$$

$$2^2 \equiv 4 \pmod{7}$$

$$3^2 \equiv 9 \pmod{7}$$

$$4^2 \equiv (-3)^2 \equiv 2 \pmod{7}$$

$$5^2 \equiv (-2)^2 \equiv 4 \pmod{7}$$

$$6^2 \equiv (-1)^2 \equiv 1 \pmod{7}$$

The quadratic non residues of 7 are 1, 2, 4 and the quadratic non residues are 3, 5, 6

Euler's Criterion

Let p be an odd prime. Let $a \in \mathbb{Z}$, $(a,p)=1$. Then a is a quadratic residue of p

iff $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

Proof

Suppose a is a quadratic residue of p, then $\exists\, x$ st

$$x^2 \equiv a \pmod{p}$$

We have

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \pmod{p}$$

$$\equiv 1 \pmod{p}$$

Fermat's Little theorem

Wilson's Theorem

$$(p-1)! \equiv -1 \pmod{p}$$

Now suppose a is not a quadratic residue of p

For each $c \in \{1, \dots, p-1\}$

$\exists$ $c' \in \{1, \dots, p-1\}$

st $cc' \equiv a \pmod{p}$

and $c \neq c'$

Hence

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

By Wilsons ~~theorem~~ a is not a quadratic residue of p, then

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Example

Can we solve $x^2 \equiv 3 \pmod{31}$?

Euler's Criterion

$3^{15} \pmod{31}$

$3 \equiv 3 \pmod{31}$

$3^2 \equiv 9 \pmod{31}$

$3^4 \equiv 81 \equiv 19 = -12 \pmod{31}$

$3^8 \equiv 144 \equiv 20 \equiv -11 \pmod{31}$

$3^{15} = 3^8 3^4 3^2 3^1$

$\equiv (-11)(-12)(-4)$

$\equiv 13(-12)$

$\equiv -1 \mod (31)$ NO!

Legendre Symbol

Let p be an odd prime and $(a,p)=1$, The legendre symbol

$$\left(\frac{a}{p}\right)$$

is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p \\ -1 & \text{otherwise} \end{cases}$$

Theorem

Let p be an odd prime, $a, b \in \mathbb{Z}$
$(a, p) = (b, p) = 1$, then

(1) If $a \equiv b \pmod{p}$

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

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

(3) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

(4) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

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

(6) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$

Corollery

If p is an odd prime then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

Proof

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

Completion exercise

Example

Can we solve $x^2 \equiv -84 \pmod{31}$?

$$\left(\frac{-84}{31}\right) = \left(\frac{-1}{31}\right)\left(\frac{4}{31}\right)\left(\frac{7}{31}\right)\left(\frac{3}{31}\right)$$

$$= -\left(\frac{21}{31}\right)$$

Theorem

There are infinitely many primes congruent to $1 \pmod 4$

Proof

Suppose there are finitely many such primes $p_1, \ldots, p_t$. Consider

$$N = 4 p_1^2 p_2^2 \cdots p_t^2 + 1$$

$$N \equiv 1 \pmod 4, \quad N > p_i, \quad i = 1, \ldots, t$$

Thus, N is composite and $\exists\, p$ prime st $p \mid N$. It should be clear that $p \neq p_i$, $i = 1, \ldots, t$.

We have $N \equiv 0 \mod p$

so $4 p_1^2 \cdots p_t^2 \equiv -1 \pmod p$

Thus

$$\left(\frac{-1}{p}\right) = 1 \implies p \equiv 1 \pmod 4$$

a contradiction. Thus there are infinitely many primes of the form $4K+1$.

Primitive Roots

Remember if $(a, n) = 1$ then

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

Definition

The order of a number $a \pmod{n}$ is the smallest natural number d such that

$$a^d \equiv 1 \pmod{n}$$

If $d = \phi(n)$ then a is a primitive root of n. Clearly if n is prime then $\phi(n) = n-1$. If r is a primitive root of a prime p then $r, r^2, \ldots, r^{p-1}$ is a complete set of residues $\pmod{p}$

$\text{ord}_n\, a$ = order of $a \pmod{n}$

Theorem

If $\operatorname{ord}_n a = d$ then $d \mid \phi(n)$

Proof

From the division algorithm $\exists$ $b, c \in \mathbb{N}$ st

$$\phi(n) = bd + c \qquad 0 \le c < d$$

$$1 \equiv a^{\phi(n)} = a^{bd+c} = (a^d)^b a^c \equiv a^c \pmod n$$

This contradicts $d = \operatorname{ord}_n a$, Therefore

$c = 0$ and $d \mid \phi(n)$

$\square$

Example

Let $p = 17$, $\phi(p) = 16$

possible orders are $1, 2, 4, 8, 16$

- $2 \equiv 2 \pmod{17}$ $\qquad$ $2^8 \equiv 1 \pmod{17}$

$2^2 \equiv 4$ $\qquad$ 2 is not a primitive root of 17

$2^4 \equiv -1$

- $3 \equiv 3 \pmod{17}$

$3^2 \equiv 9 \equiv -8$

$3^4 \equiv 64 \equiv -4$

$3^8 \equiv 16 \equiv -1$

$3^{16} \equiv 1 \quad \Rightarrow \quad 3$ is a primitive root of 17

Lagrange's Theorem

Let $f \in \mathbb{Z}[x]$

$f(x) = a_n x^n + \dots + a_1 x + a_0 \qquad a_i \in \mathbb{Z}$

Let p be a prime, $(a_n, p) = 1$

Then f has at most n incongruent roots $\pmod{p}$

Proof (by induction)

$\underline{n=1}$ $\quad a_1 x + a_0 \equiv 0 \pmod{p} \quad (a_1, p) = 1$

This has a unique solution $\pmod{p}$

Suppose ~~the~~ statement holds for $n=k$ is a k^{th} degree polynomial has a maximum of k incongruent roots $(\bmod p)$

Consider $f(x) = a_{k+1}x^{k+1} + \dots + a_1 x + a_0$

$$(a_{k+1}, p) = 1$$

Assume f has $k+2$ incongruent roots $(\bmod p)$ and ~~these~~ are

$c_0, c_1, c_2, \dots, c_{k+1}$

We have

$$f(x) - f(c_0) = a_{k+1}(x^{k+1} - c_0^{k+1}) + \dots$$

$$\dots + a_1(x - c_0)$$

$$= (x - c_0)\, g(x)$$

where $g(x)$ has degree at most k

$$0 \pmod p \equiv f(c_i) - f(c_0) = \underbrace{(c_i - c_0)}_{\not\equiv 0 \ (\bmod p)}\, g(c_i)$$

Thus
$$g(c_i) \equiv 0 \quad \text{for} \quad i=1,\dots,k+1$$
Contradicts the induction hypothesis

Lemma

Let p be prime, $a \in \mathbb{Z}$, $(a,p)=1$
Let $\text{ord}_p a = d$ and $u \in \mathbb{N}$, Then
$$\text{ord}_p(a^u) = \frac{d}{(d,u)}$$

Proof

Let $t = \text{ord}_p(a^u)$

Let $h = \gcd(d,u)$

then we can write
$$d = hd_1 \qquad (u_1, d_1) = 1$$
$$u = hu_1$$

Then $$(a^u)^{d_1} = (a^{hu_1})^{\frac{d}{h}} = (a^d)^{u_1} \equiv 1 \mod p$$

Hence $t | d_1$

Also, $(a^u)^t \equiv 1 \bmod p$ by definition

Hence, $d | ut$

so $d_1 h | u_1 h t$

By Euclids lemma $d_1 | t$

Therefore $t = d_1 = \frac{d}{(u,d)}$

Lemma

Let p be prime and suppose $d | (p-1)$. Then, the # of integers of order d in the set $\{1, \dots, p-1\}$ is at most $\phi(d)$

Proof

Let $F(d) = \# \{ a \in \{1, \dots, p-1\} \mid \mathrm{ord}_p a = d \}$

If $F(d) = 0$ then $F(d) \leq \phi(d)$

Now suppose $F(d) \geq 1$ so $\exists\ a \in \{1, \dots, p-1\}$

st $\text{ord}_p a = d$, so $a^d \equiv 1 \bmod p$

Note that

$a, a^2, \ldots, a^d$ are incongruent $(\text{mod } p)$

Also if $K = 1, \ldots, d$ then

$(a^K)^d \equiv (a^d)^K \equiv 1 \pmod p$

Thus for each $K \in \{1, \ldots, d\}$, a^K is a root of $x^d \equiv 1 \pmod p$

By Lagrange's theorem these are the only roots of this equation

By the previous lemma we know that a^K has order d iff $(K, d) = 1$. There are $\varphi(d)$ such K. Thus if there is one element of order d there are $\varphi(d)$ such elements

Hence, $F(d) \leq \varphi(d)$

Theorem

Let p be a prime with $d \mid p-1$. Let $F(d)$ be as in the lemma, then

$$F(d) = \phi(d)$$

Proof

$$p-1 = \sum_{d \mid p-1} F(d)$$

We also have

$$p-1 = \sum_{d \mid p-1} \phi(d)$$

so $\sum_{d \mid p-1} \phi(d) = \sum_{d \mid p-1} F(d)$

Also from the lemma $F(d) \leq \phi(d)$

Thus $F(d) = \phi(d)$ for $d \mid p-1$

Corollary

Every prime has a primitive root

Theorem

If p is an odd prime, then

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$$

so there are $\frac{p-1}{2}$ quadratic residues of p and $\frac{p-1}{2}$ quadratic non residues of p

Proof

Let r be a primitive root of p so that $r, r^2, \ldots, r^{p-1}$ form a complete set of residues.

For each $a \in \{1, \ldots, p-1\}$ $\exists$ $k_a \in \{1, \ldots, p-1\}$ such that

$$r^{k_a} \equiv a \pmod{p}$$

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv \left(r^{k_a}\right)^{\frac{p-1}{2}} \equiv \left(r^{\frac{p-1}{2}}\right)^{k_a} = (-1)^{k_a}$$

$$\therefore \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = \sum_{a=1}^{p-1} (-1)^{k_a} = 0$$

Corollary

The quadratic residues of an odd prime p are congruent to the even powers of a primitive root of p

Gauss Lemma

Let p be an odd prime and $a \in \mathbb{Z}$, $(a,p) = 1$. Let t denote the number of elements of the set S

$$S = \left\{ a, 2a, 3a, \ldots \frac{p-1}{2} a \right\}$$

which have remainder greater than $\frac{p}{2}$ after division by p

Then $\left(\frac{a}{p}\right) = (-1)^t \pmod{p}$

Proof

Consider $a, 2a, \ldots, \frac{p-1}{2} a$

Let $r_1, \ldots, r_u$ be remainders which are $< \frac{p}{2}$. Let $s_1, \ldots, s_t$ be the remainders which are $> \frac{p}{2}$

Now consider

$r_1, \dots, r_u, p-s_1, \dots, p-s_t$

If $r_i \equiv r_j \pmod p$ or $s_i \equiv s_j \pmod p$

then $\exists$ $m_i \equiv m_j \pmod p$, $m_i, m_j \in \{1, \dots, \frac{p-1}{2}\}$

If $\exists$ i, j st

$r_i \equiv p - s_j \pmod p$

then $r_i \equiv -s_j \pmod p$

so $\exists$ $m_i, m_j \in \{1, \dots, \frac{p-1}{2}\}$

st

$m_i + m_j \equiv 0 \pmod p$

which is impossible

Hence $\{r_1, \dots, r_u, p-s_1, \dots, p-s_t\}$

$= \{1, 2, \dots, \frac{p-1}{2}\}$

Therefore

$$r_1, r_2 \ldots r_u (p - s_1) \ldots (p - s_t)$$
$$\equiv \left(\frac{p-1}{2}\right)! \pmod p$$

Also

$$r_1 \ldots r_u s_1 \ldots s_t \equiv a \cdot 2a \cdot 3a \cdot \ldots \cdot \left(\frac{p-1}{2}\right)a \pmod p$$
$$\equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p$$

$$\equiv (-1)^t r_1 \ldots r_u s_1 \ldots s_t$$

Thus

$$(-1)^t a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! \pmod p$$

This gives $(-1)^t a^{\frac{p-1}{2}} \equiv 1 \pmod p$

$$a^{\frac{p-1}{2}} \equiv (-1)^t \pmod p$$

Finally, by Euler's Criterion

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^t \pmod p$$ as required

Theorem

p is an odd prime.

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod 8 \\ -1 & p \equiv \pm 3 \pmod 8 \end{cases}$$

Proof

Apply the Gauss Lemma with $a = 2$

In this case

$$S = \left\{ a, 2a, \ldots, \frac{p-1}{2} a \right\}$$
$$= \{ 2, 4, \ldots, p-1 \}$$

How many elements of S are $> \frac{p}{2}$

Suppose $2k < \frac{p}{2}$

$$\Rightarrow k \leq \left[\frac{p}{4} \right]$$

completion exercise

Let $t = \frac{p-1}{2} - \left[\frac{p}{4} \right]$

Example

Does $x^2 \equiv 2 \pmod{11}$ have solutions?

$$\left(\frac{2}{11}\right) = -1$$

Quadratic Law of Reciprocity

Let p, q be distinct odd primes. Then

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

Corollary 2

hehe

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{if } p \text{ and/or } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) & \text{if } p \text{ and } q \equiv 3 \pmod 4 \end{cases}$$

Corollary 1

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p \text{ and/or } q \equiv 1 \pmod 4 \\ -1 & \text{if both } p, q \equiv 3 \pmod 4 \end{cases}$$

(Via Eisenstein's Lemma)

Let p be an odd prime and a an odd integer $(a,p)=1$. Then

$$\left(\frac{a}{p}\right) = (-1)^{\left(\sum_{u=1}^{\frac{p-1}{2}}\left[\frac{ua}{p}\right]\right)}$$

Proof

As in the proof of the Gauss Lemma consider $a, 2a, \ldots, \frac{p-1}{2}a$ and let $r_1, \ldots, r_n$ denote the remainders $< \frac{p}{2}$ after division by p $s_1, \ldots, s_t$ . . . . $> \frac{p}{2}$

By the division Algorithm,

$$ja = p\left[\frac{ja}{p}\right] + \text{remainder}$$

these are the r's and s's

Sum to obtain

$$\sum_{j=1}^{\frac{p-1}{2}} ja = p\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{ja}{p}\right] + \sum_{i=1}^{n} r_i + \sum_{j=1}^{t} s_j \quad \text{①}$$

We already know from the proof of Gauss Lemma that $r_1, \ldots, r_n, p-s_1, \ldots p-s_t$

are the numbers $1, 2, \ldots, \frac{p-1}{2}$

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{i=1}^{n} r_i + tp - \sum_{i=1}^{t} t_i$$

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = p\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] + 2\sum_{j=1}^{t} s_j - pt$$

Consider this (mod 2)

$$0 \equiv \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] - t \pmod 2$$

Hence

$$\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] \equiv t \pmod 2$$

Gauss Lemma

By the Gauss Lemma

$$\left(\frac{a}{p}\right) \equiv (-1)^{t} \equiv (-1)^{\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{ja}{p}\right]}$$

Let $S(p,q) = \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{jp}{q}\right]$

We know

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

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

Therefore

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S(p,q)+S(q,p)}$$

We need to prove

$$S(p,q) + S(q,p) = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$$

$$y = \frac{qx}{p}$$

We will count the lattice points in the different ways (Don't include the axis)

The obvious answer is $\frac{p-1}{2}\frac{q-1}{2}$

It is easy to show

$$\underbrace{\frac{q-1}{2}}_{\substack{\text{height}\\ \text{of } m}} < \underbrace{\frac{q(p-1)}{2p}}_{\substack{\text{height}\\ \text{of } N}} < \frac{q-1}{2} + 1$$

So there are no integers in the triangle mNR except possibly on MR

There are no lattice points on OC either except O or C. Hence the number of points in OKml is the sum of the number of points in the two triangles OKN and OLR

Height of T is $\frac{qj}{p}$

Thus there are $\left[\frac{qj}{p}\right]$ lattice points on ST

So OKN contains

$$\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{jq}{p}\right] = S(q,p)$$

Similarly it can be shown that the number in QLR is $S(p,q)$

$\square$

Example

Does

$$x^2 \equiv 34 \mod (293)$$

have solutions?

$$\left(\frac{34}{293}\right) = \left(\frac{2}{293}\right)\left(\frac{17}{293}\right)$$

$$= -\left(\frac{17}{293}\right)$$

$$\underset{QLR}{=} -\left(\frac{293}{17}\right)$$

$$= -\left(\frac{4}{17}\right) = -1$$

Does not have solutions

Continued Fractions

$$\frac{279}{112} = 2 + \frac{55}{112}$$

$$= 2 + \frac{1}{\left(\frac{112}{55}\right)}$$

$$= 2 + \frac{1}{2 + \left(\frac{2}{55}\right)}$$

$$= 2 + \frac{1}{2 + \frac{1}{\left(\frac{55}{2}\right)}}$$

$$= 2 + \frac{1}{2 + \frac{1}{27 + \frac{1}{2}}}$$

$$= [2 ; 2, 27, 2]$$

Any expansion of this form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2} + \ddots}$$

is a continued fraction

Denote this

$[a_0 ; a_1, a_2, \ldots]$

if it is infinite

$[a_0 ; a_1, a_2, \ldots, a_N]$

is a finite continued fraction

If $a_i \in \mathbb{N}$, $i \in 1, 2, \ldots$

then the continued fraction is simple

An infinite continued fraction converges if the sequence of finite continued fractions

$[a_0], [a_0 ; a_1], [a_0 ; a_1, a_2], \ldots$ converges

All simple continued fractions converge

Khintchine 1964

A continued fraction converges iff $\sum_{i=0}^{\infty} a_i = \infty$

Book: Khinchin

Note that

$$[a_0, a_1, a_2, \dots a_N, a_{N+1}, \dots]$$
$$= [a_0, a_1, a_2, \dots, a_N, [a_{N+1}, a_{N+2}, \dots]]$$

Theorem

$a_0 \in \mathbb{N} \cup \{0\}$

$a_1, a_2, \ldots \in \mathbb{N}$

and let $p_0 = a_0 \quad p_1 = a_0 a_1 + 1$

$q_0 = 1 \quad q_1 = a_1$

$p_n = a_n p_{n-1} + p_{n-2}, \; q_n = a_n q_{n-1} + q_{n-2}$

If $\alpha \in \mathbb{R}$, $\alpha \geq 1$ then

(i) $[a_0, \ldots, a_n, \alpha] = \dfrac{\alpha p_n + p_{n-1}}{\alpha q_n + q_{n-1}}$

(ii) $[a_0, \ldots, a_n] = \dfrac{p_n}{q_n} \leftarrow$ Called the n^{th} convergent of the continued fraction

follows directly from (i)

Proof

induction

$[a_0, a_1] = a_0 + \dfrac{1}{a_1}$

$$= \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}$$

$$[a_0, a_1, \alpha] = a_0 + \frac{1}{a_1 + \frac{1}{\alpha}}$$

$$= \frac{\alpha p_1 + p_0}{\alpha q_1 + q_0}$$ check !

Assume statement holds for $n = k$

$$[a_0, a_1, \ldots, a_k, \alpha] = \frac{\alpha p_k + p_{k-1}}{\alpha q_k + q_{k-1}}$$

Consider

$$[a_0, a_1, \ldots, a_k, a_{k+1}, \alpha]$$

$$= [a_0, a_1, \ldots, a_k [a_{k+1}, \alpha]]$$

$$= \frac{[a_{k+1}, \alpha] p_k + p_{k-1}}{[a_{k+1}, \alpha] q_k + q_{k-1}}$$

$$= \frac{\alpha p_{k+1} + p_k}{\alpha q_{k+1} + q_k}$$

$$[a_{k+1}, \alpha] = a_{k+1} + \frac{1}{\alpha} = \frac{\alpha a_{k+1} + 1}{\alpha}$$

Lemma

Consider the continued fraction

$[a_0, a_1, \ldots]$

(1) $p_n q_{n+1} - p_{n+1} q_n = (-1)^{n+1}$

$\Rightarrow \dfrac{p_n}{q_n} - \dfrac{p_{n+1}}{q_{n+1}} = \dfrac{1}{q_n q_{n+1}}$

(2) $(p_n, q_n) = 1$ clear

(3) For $n > 0$ $q_{n+1} > q_n \Rightarrow q_n \geq n$ clear

(4) $\dfrac{p_0}{q_0} < \dfrac{p_2}{q_2} < \ldots < \dfrac{p_{2m}}{q_{2m}} < \ldots < \dfrac{p_{2n+1}}{q_{2n+1}} < \dfrac{p_{2n-1}}{q_{2n-1}} < \ldots$

$\ldots < \dfrac{p_3}{q_3} < \dfrac{p_1}{q_1}$

(5) All infinite simple continued fractions converge

Proof

(1) $p_n q_{n+1} - p_{n+1} q_n = p_n(a_{n+1} q_n + q_{n-1})$

$$- (a_{n+1} p_n + p_{n-1}) q_n$$

$$= p_n q_{n-1} - p_{n-1} q_n$$

$$= -(p_{n-1} q_n - q_n p_{n-1})$$

$$= -(-(p_{n-2} q_{n-1} - p_{n-1} q_{n-2}))$$

$$\vdots$$

$$= (-1)^n (p_0 q_1 - p_1 q_0)$$

$$= (-1)^{n+1}$$

(4) $\frac{p_{2n}}{q_{2n}} - \frac{p_{2n+2}}{q_{2n+2}} = \frac{p_{2n}}{q_{2n}} - \frac{p_{2n+1}}{q_{2n+1}} + \frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n+2}}{q_{2n+2}}$

(from 1) $= \frac{(-1)^{2n+1}}{q_{2n} q_{2n+1}} - \frac{(-1)^{2n+2}}{q_{2n+1} q_{2n+2}}$

$$= \frac{1}{q_{2n+1} q_{2n+2}} - \frac{1}{q_{2n} q_{2n+1}} < 0$$

Thus the sequence $\frac{p_{2n}}{q_{2n}}$ is increasing

It can similarly be shown that the sequence

$\frac{p_{2n+1}}{q_{2n+1}}$ is decreasing

Its easy to show $\frac{p_{2n}}{q_{2n}} - \frac{p_{2n+1}}{q_{2n+1}} < 0$

Assume, for contradiction

$\frac{p_{2n}}{q_{2n}} > \frac{p_{2m+1}}{q_{2m+1}}$ for some m, n

If $m > n$ then

$\frac{p_{2m}}{q_{2m}} > \frac{p_{2n}}{q_{2n}} > \frac{p_{2m+1}}{q_{2m+1}}$ contradiction

If $m < n$ then

$\frac{p_{2n+1}}{q_{2n+1}} < \frac{p_{2m+1}}{q_{2m+1}} < \frac{p_{2n}}{q_{2n}}$ contradiction

(5) By the monotone convergence theorem the sequences

$$\left(\frac{p_{2n}}{q_{2n}}\right) \text{ and } \left(\frac{p_{2n+1}}{q_{2n+1}}\right) \text{ both converge}$$

We know

$$\left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| \longrightarrow 0 \quad \text{as } n \longrightarrow \infty$$

Therefore $\left(\frac{p_n}{q_n}\right)$ converges

Fact (fun)

Let $\alpha \in \mathbb{R}$ with integer part $[\alpha]$

$$\alpha = [\alpha] + \frac{1}{\alpha_1}$$

$$\alpha_1 = [\alpha_1] + \frac{1}{\alpha_2} \quad \text{etc}$$

$$\alpha = [\,[\alpha], [\alpha_1], [\alpha_2], \dots\,]$$

Fact

Every rational can be represented in two ways

$$[a_0, \dots, a_n] = [a_0, \dots, a_n - 1, +1]$$

proper

Theorem

Let α be irrational, with continued fraction $[a_0, a_1, \dots]$. Then

(1) $\lim_{n \to \infty} \frac{p_n}{q_n} = \alpha$

(2) $\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}$

Dirichlet Theorem

Proof

(1) Let $\alpha = [a_0, a_1, \dots a_n, \alpha_{n+1}]$

$$= \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}}$$

Therefore

$$\alpha - \frac{p_n}{q_n} = \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}} - \frac{p_n}{q_n}$$

$$= \frac{(-1)^n}{q_n(\alpha_{n+1} q_n + q_{n-1})} \qquad \begin{array}{ll} < 0 & n \text{ odd} \\ > 0 & n \text{ even} \end{array}$$

$\alpha < \frac{p_n}{q_n}$ n odd

$\alpha > \frac{p_n}{q_n}$ n even

Hence $\lim_{n \to \infty} \frac{p_n}{q_n} = \alpha$

Theorem

(1) If $[a_0, a_1, \ldots, a_m] = [a_0', \ldots, a_n']$ $a_i, a_i' \in \mathbb{N}$

then $m = n$ $a_i = a_i'$ $i = 0, \ldots, m$

(2) If $[a_0, a_1, \ldots] = [a_0', a_1', \ldots]$ $a_i, a_i' \in \mathbb{N}$

then $a_i = a_i'$ $i = 0, 1, 2, \ldots$

Example

$$\sqrt{37} = 6 + (\sqrt{37} - 6)$$

$$= 6 + \frac{1}{\left(\frac{1}{\sqrt{37} - 6}\right)}$$

$$= 6 + \frac{1}{\sqrt{37} + 6}$$

$$= 6 + \frac{1}{12 + (\sqrt{37} + 6 - 12)}$$

$$= 6 + \frac{1}{12 + (\sqrt{37} - 6)}$$

$$= 6 + \cfrac{1}{12 + \cfrac{1}{12 + \cfrac{1}{12 + \ddots}}}$$

$$= [6, \overline{12}]$$

Example

$$\sqrt{2} = [1, \overline{2}]$$

Example

Let $\alpha = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}}$

$= [\overline{1}]$

$= 1 + \dfrac{1}{\alpha}$

$$\alpha^2 - \alpha - 1 = 0$$

$$\alpha = \frac{1 \pm \sqrt{5}}{2}$$

$a_i = 1 \qquad i = 0, 1, \ldots$

$p_0 = a_0 = 1$

$p_1 = a_0 a_1 + 1 = 2$

$q_0 = 1$

$q_1 = a_1 = 1$

$p_2 = a_2 p_1 + p_0 = p_1 + p_0 = 3$

$p_3 = p_2 + p_1 = 5$

$p_4 = 8$

$p_5 = 13$

$\vdots$

$q_2 = q_1 + q_0 = 2$

$q_3 = q_2 + q_1 = 3$

$q_4 = 5$

$q_5 = 8$

$\vdots$

Convergence of the Golden ratio are

$$\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}$$

Example

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots]$$

Algebraic number is the root of an integer polynomial

Theorem

The continued fraction expansion of $\alpha \in \mathbb{R}$ is eventually periodic iff α is a quadratic irrational.

Proof

Convergents are $\frac{p_n}{q_n}$

Suppose $\alpha = [a_0, a_1, \ldots, a_{k-1}, \overline{a_k, \ldots, a_{k+n-1}}]$

Then we can write $\alpha = [a_0, a_1, \ldots, a_{k-1}, \alpha_k]$

Convergents are $\frac{p_n'}{q_n'}$

Where $\alpha_k = [a_k, a_{k+1}, \ldots, a_{k+n-1}, \alpha_k]$

Then $\alpha = \dfrac{\alpha_k p_{k-1} + p_{k-2}}{\alpha_k q_{k-1} + q_{k-2}} \Rightarrow \alpha_k = \dfrac{p_{k-2} - \alpha q_{k-2}}{\alpha q_{k-1} - p_{k-1}}$

and $\alpha_k = \dfrac{\alpha_k p_{n-1}' + p_{n-2}'}{\alpha_k q_{n-1}' + q_{n-2}'}$

Putting these together

$$\left(\frac{p_{k-2} - \alpha q_{k-2}}{\alpha q_{k-1} - p_{k-1}}\right)^2 q_{n-1}' + \left(\frac{p_{k-2} - \alpha q_{k-2}}{\alpha q_{k-1} - p_{k-1}}\right)(q_{n-1}' - p_{n-1}') - p_{n-2}' q_{n-2}' = 0$$

Is quadratic in α

Conversely, Suppose

$\alpha = [a_0, a_1, a_2, \ldots, a_{n-1}, \alpha_n] \in \mathbb{R} \setminus \mathbb{Q}$

and $\exists$ $a, b, c \in \mathbb{Z}$ st

$$a\alpha^2 + b\alpha + c = 0$$

As before

$$\alpha = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}$$

We obtain $A_n \alpha_n^2 + B_n \alpha_n + C_n = 0$

$A_n = a p_{n-1}^2 + b p_{n-1} q_{n-1} + c q_{n-1}^2$

$B_n = 2a p_{n-1} p_{n-2} + b(p_{n-1} q_{n-2} + p_{n-2} q_{n-1}) + 2c q_{n-1} q_{n-2}$

$C_n = a p_{n-2}^2 + b p_{n-2} q_{n-2} + c q_{n-2}^2 = A_{n-1}$

If $A_n = 0$ then $\frac{p_{n-1}}{q_{n-1}}$ is a root of $ax^2 + bx + c$

Note that $B_n^2 - 4A_nC_n = b^2 - 4ac$

We know

$$\left| \alpha - \frac{p_{n-1}}{q_{n-1}} \right| < \frac{1}{q_{n-1}}$$

Hence, $\exists\ \delta_{n-1}$ $|\delta_{n-1}| < 1$ st

$$\alpha - \frac{p_{n-1}}{q_{n-1}} = \frac{\delta_{n-1}}{q_{n-1}^2}$$

$$p_{n-1} = \alpha p_{n-1} + \frac{\delta_{n-1}}{q_{n-1}}$$

Put this into A_n to obtain

$$A_n = q_{n-1}^2 + \underbrace{\left(a\alpha^2 + b\alpha + c \right)}_{=0} + 2a\alpha\,\delta_{n-1}$$

$$+ \frac{a\,\delta_{n-1}^2}{q_{n-1}^2} + b\,\delta_{n-1}$$

$$= \delta_{n-1}(2a\alpha + b) + \frac{a\,\delta_{n-1}^2}{q_{n-1}^2}$$

Then

$$|A_n| < |2a\alpha + b| + |a|$$

$\Rightarrow |C_n| < |2a\alpha + b| + |a|$

Finally

$B_n^2 - 4A_nC_n = b^2 - 4ac$

$B_n^2 = b^2 - 4ac + 4A_nC_n$

$B_n^2 < |b^2 - 4ac| + 4(|2a\alpha + b| + |a|)^2$

$(A_N), \ (B_N), \ (C_N)$

$\forall N \quad (A_n) \leq d$

$(B_N) \leq K_1$

$(C_N) \leq d$

Eventually, $\exists$ two triples

$(A_{n_1}, B_{n_1}, C_{n_1}) = (A_{n_2}, B_{n_2}, C_{n_2})$

$\Rightarrow \alpha_{n_1} = \alpha_{n_2}$

$a_{n_1} = a_{n_2}$

$a_{n_1+1} = a_{n_2+1}$

$\vdots$

This also implies that in the continued fraction the a_i are bounded

Open Question

Are the entries $2^{\frac{1}{3}}$ bounded ?

Fact

The set of continued fractions with bounded entries has Lebesgue measure zero

Theorem

Let $n > 1$, $0 < q \leq q_n$ $\frac{p}{q} \neq \frac{p_n}{q_n}$

Where $\frac{p_n}{q_n}$ are the convergents of a real number α

Then $|p_n - q_n \alpha| < |p - q\alpha|$

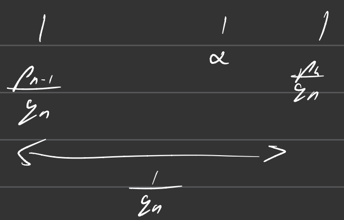
$$\Rightarrow \left|\alpha - \frac{p_n}{q_n}\right| < \left|\alpha - \frac{p}{q}\right|$$

Proof

(1) Let $q = q_n$

Then $\left|\frac{p_n}{q_n} - \frac{p}{q_n}\right| \geq \frac{1}{q_n}$

However $\left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n q_{n+1}} \leq \frac{1}{2 q_n}$



$\Rightarrow \left|\alpha - \frac{p_n}{q_n}\right| < \left|\alpha - \frac{p}{q_n}\right|$

(2) Now suppose

$q_{n-1} < q < q_n$

and $\frac{p}{q} \neq \frac{p_n}{q_n}, \frac{p_{n-1}}{q_{n-1}}$

We can find $\mu, \nu \in \mathbb{R}$ such that

$\mu p_{n-1} + \nu p_{n-1} = p$

$\mu q_n + \nu q_{n-1} = q$

Solving for μ and ν gives

$$\mu = \pm(p q_{n-1} - q p_{n-1}) \in \mathbb{Z} \setminus \{0\}$$

$$\nu = \pm(p q_n - q p_n) \in \mathbb{Z} \setminus \{0\}$$

We have

$$q = \mu p_n + \nu q_{n-1}$$

So μ, ν have opposite signs

We also know that

$$(p_n - q_n \alpha) \text{ and } (p_{n-1} - q_{n-1}\alpha)$$

also have different signs

Therefore

$$\mu(p_n - q_n\alpha) \text{ and } \nu(p_{n-1} - q_{n-1}\alpha)$$

have the same sign

However

$$p - q\alpha = \mu(p_n - q_n\alpha) + \nu(p_{n-1} - q_{n-1}\alpha)$$

Thus

$$|p - q\alpha| \geq \max\left(|\mu||p_n - q_n\alpha|, |\nu||p_{n-1} - q_{n-1}\alpha|\right)$$

$$\geq \max\left(|p_n - q_n\alpha|, |p_{n-1} - q_{n-1}\alpha|\right)$$

as required

Complete by induction

Theorem

Let $\frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}}$ be consecutive convergents

of $\alpha \in \mathbb{R}$. Then at least one of

$|\alpha - \frac{p_i}{q_i}| < \frac{1}{2q_i^2}$ holds $i = n, n+1$

This implies there are infinitely many rationals satisfying

$|\alpha - \frac{p}{q}| < \frac{1}{2q^2}$ for each $\alpha \in \mathbb{R} \setminus \mathbb{Q}$

Proof

Assume this does not hold, ie

$$\left|\alpha - \frac{p_i}{q_i}\right| \geq \frac{1}{2q_i^2} \qquad i = n, n+1$$

We have

$$\frac{1}{q_n q_{n+1}} = \left|\frac{p_{n+1}q_n - p_n q_{n+1}}{q_n q_{n+1}}\right|$$

$$= \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right|$$

$$= \left|\frac{p_n}{q_n} - \alpha\right| + \left|\frac{p_{n+1}}{q_{n+1}} - \alpha\right|$$

$$\geq \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2}$$

Rearranging gives that

$$(q_{n+1} - q_n)^2 \leq 0$$

Impossible unless

$n = 0 \quad q_1 = 1 \qquad q_0 = q_1 = 1$

Even in this case the result still holds

Theorem

If $\alpha = \dfrac{P\beta + R}{Q\beta + S}$

$\beta > 1$ $P, Q, R, S \in \mathbb{Z}$ such that

$Q > S \geq 0$, $PS - QR = \pm 1$

Then, $\dfrac{R}{S}, \dfrac{P}{Q}$ are consecutive convergents of α

Theorem

Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$

$\dfrac{p}{q} \in \mathbb{Q}$ such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$$

Then $\dfrac{p}{q}$ is a convergent of α

Question

For which functions f do infinitely many rationals exist such that

$$\left|\alpha - \frac{p}{q}\right| < f(q) \ ?$$

Hurwitz Theorem

There are infinitely many convergents $\frac{p_n}{q_n}$ of an irrational number α such that

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{\sqrt{5}\, q_n^2}$$

This is sharp (cannot be improved) in the sense that $\exists\ \alpha \in \mathbb{R} \setminus \mathbb{Q}$ such that

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{(\sqrt{5}+\varepsilon)\, q_n^2}$$

does not hold for infinitely many n

Proof

We will show that at least one of every three consecutive convergents satisfies

$$\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{\sqrt{5}\, q_n^2}$$

We have

$$\left| \alpha - \frac{p_n}{q_n} \right| = \frac{1}{q_n(\alpha_{n+1} q_n + q_{n-1})}$$

$$= \frac{1}{q_n^2 \left(\alpha_{n+1} + \frac{q_{n-1}}{q_n} \right)}$$

We will show that

$$\alpha_i + \frac{q_{i-2}}{q_{i-1}} \leq \sqrt{5} \qquad (*)$$

Cannot hold for three consecutive i

Suppose $(*)$ holds for $i = n-1$ and $i = n$

$$\alpha_{n-1} + \frac{q_{n-3}}{q_{n-2}} \leq \sqrt{5}$$

$$\alpha_n + \frac{q_{n-2}}{q_{n-1}} \le \sqrt{5}$$

Also $\quad \alpha_{n-1} = a_{n-1} + \dfrac{1}{\alpha_n}$

$$\frac{q_{n-1}}{q_{n-2}} = \frac{a_{n-1}q_{n-2} + q_{n-3}}{q_{n-2}}$$

$$= a_{n-1} + \frac{q_{n-3}}{q_{n-2}}$$

$$\frac{1}{\alpha_n} + \frac{q_{n-1}}{q_{n-2}} = \alpha_{n-1} + \frac{q_{n-3}}{q_{n-2}} \le \sqrt{5} \quad \text{from } (✱)$$

$$1 = \frac{\alpha_n}{\alpha_n} \le \left(\sqrt{5} - \frac{q_{n-1}}{q_{n-2}}\right)\Big(\sqrt{5} - \overbrace{\frac{q_{n-2}}{q_{n-1}}}^{\text{from } (❀)}\Big)$$

$$\Rightarrow \frac{q_{n-1}}{q_{n-2}} + \frac{q_{n-2}}{q_{n-1}} \le \sqrt{5}$$

$$\Rightarrow \frac{q_{n-1}}{q_{n-2}} + \frac{q_{n-2}}{q_{n-1}} < \sqrt{5} \qquad (✱)(❀)$$

$$1 - \frac{q_{n-2}^2}{q_{n-1}^2} \leq \sqrt{5}\,\frac{q_{n-2}}{q_{n-1}}$$

$$\Rightarrow \quad \frac{\sqrt{5}-1}{2} < \frac{q_{n-2}}{q_{n-1}} < \frac{1+\sqrt{5}}{2}$$

Now assume (*) holds for $i = n+1$ and by precisely the same argument we obtain

$$\frac{q_{n-1}}{q_n} > \frac{\sqrt{5}-1}{2}$$

Now

$$a_n = \frac{q_n - q_{n-2}}{q_{n-1}} = \frac{q_n}{q_{n-1}} - \frac{q_{n-2}}{q_{n-1}}$$

$$< \left(\sqrt{5} - \frac{q_{n-1}}{q_n}\right) - \frac{q_{n-2}}{q_{n-1}}$$

from (+)(*)

$$< \sqrt{5} - (\sqrt{5}-1) = 1$$

Contradiction

Hence there exists one of $i = n-1, n, n+1$ such that

$$\frac{q_{i-2}}{q_{i-2}} > \sqrt{5}$$

Proof that this is sharp

We will show that there exist $\gamma \in \mathbb{R} \setminus \mathbb{Q}$ such that if $a > \sqrt{5}$ then

$$\left| \gamma - \frac{p}{q} \right| < \frac{1}{a q^2}$$

has at most finitely many solutions, $\frac{p}{q}$

Let $\gamma = \frac{\sqrt{5}-1}{2}$

and suppose the inequality has infinitely many solutions and we choose q arbitrarily large

We have

$$\frac{\sqrt{5}-1}{2} = \frac{p}{q} + \frac{\delta}{q^2} \qquad |\delta| < a < \frac{1}{\sqrt{5}}$$

$$\frac{\sqrt{5} q}{2} - \frac{\delta}{q} = p + \frac{q}{2}$$

Square both sides to obtain

$$\frac{5q^2}{4} + \frac{\delta^2}{q} - \sqrt{5}\,\delta = p^2 + \frac{q^2}{4} + pq$$

$$\left|\frac{\delta^2}{q^2} - \sqrt{5}\,\delta\right| = \left|p^2 + pq - q^2\right| = \left(\frac{q}{2} + p\right)^2 - \frac{5q^2}{4}$$

$$Z \quad = 0$$

Choose q such that

$$\left|\frac{\delta^2}{q^2} - \sqrt{5}\,\delta\right| < 1 \qquad \Rightarrow$$

Therefore

$$\left(\frac{q}{2} + p\right)^2 = \frac{5q^2}{4}$$

$$\underbrace{\frac{q}{2} + p}_{\in \mathbb{Q}} = \underbrace{\pm\frac{\sqrt{5}\,q}{2}}_{\notin \mathbb{Q}} \qquad \text{contradiction}$$

Definition

A real number α is approximable to a degree $n \in \mathbb{R}^+$ if $\exists$ infinitely many rationals such that

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^n}$$

Liouville's Theorem (1844)

A real algebraic number of degree d is not approximable to any degree larger than d.

Proof

Suppose $\alpha \in \mathbb{R}$ is algebraic of degree d. Then $\exists$ $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$, $\deg(f) = d$.

Then $\exists$ M such that

$$|f'(x)| < M \qquad x \in (\alpha - 1, \alpha + 1)$$

$\{$ Pell's Equation will not be on the Exam

Liouville's Theorem

α algebraic degree d minimal polynomial $f \in \mathbb{Z}[x]$

$$f(x) = a_d x^d + \dots + a_1 x + a_0$$

$$f(\alpha) = 0$$

$\exists\ M$ st $|f'(x)| \leq M \quad x \in (\alpha - 1, \alpha + 1)$

Let $\frac{p}{q} \in (\alpha - 1, \alpha + 1)$ and suppose α is ~~the~~ closest root of f to $\frac{p}{q}$.
We have

$$\left|f\left(\frac{p}{q}\right)\right| = \left|\frac{a_d p^d + a_{d-1} p^{d-1} q + \dots + a_1 p q^{d-1} + a_0 q^d}{q^d}\right|$$

$$\geq \frac{1}{q^d}$$

Also $f\left(\frac{p}{q}\right) = f\left(\frac{p}{q}\right) - f(\alpha)$

$$\underset{(MVT)}{=} \left(\frac{p}{q} - \alpha\right) f'(\xi)$$

ξ lies between $\frac{p}{q}$ and α

Hence

$$\left|\alpha - \frac{p}{q}\right| = \frac{\left|f\left(\frac{p}{q}\right)\right|}{\left|f'(\xi)\right|}$$

$$\geq \frac{1}{Mq^d}$$

Thus, α cannot be approximated to any order greater $> d$. In particular, if α is a quadratic irrational,

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{Mq^2}$$

α is badly approximable

Liouville's Number is Transcendental

$$\alpha = \sum_{i=1}^{\infty} 10^{-i!} = 0.110001000 0\ldots$$

Let $N > 2$, and suppose $n > N$

$$\alpha_n = \sum_{i=1}^{n} 10^{-i!} = \frac{p}{10^{n!}} = \frac{P}{Q}$$

$$|\alpha - \alpha_n| = \alpha - \frac{P}{Q} = \sum_{i=n+1}^{\infty} 10^{-i!}$$

$$\leq \sum_{i=(n+1)!}^{\infty} 10^{-i} \quad \text{geometric series}$$

$$= \frac{10^{-(n+1)!}}{\left(\frac{9}{10}\right)}$$

$$= \frac{10}{9} 10^{-(n+1)!}$$

$$\leq 2 \cdot 10^{-(n+1)!}$$

$$= 2 \cdot Q^{-n+1}$$

$$< 2 \cdot Q^{-N}$$

So α is approximable to every degree and cannot be algebraic by Liouville's Theorem

Roth's Theorem (1964)

Let α be algebraic. Then the inequality

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}$$

has at most finitely many solutions $\forall \varepsilon > 0$

Diophantine Equations

Fermat Last Theorem

$x^n + y^n = z^n \qquad (x, y, z) \in \mathbb{Z}^3$

only has solutions for $n \leq 2$

Conjectured for 350 years, proved by Andrew Wiles

First reduced to showing only need to consider odd primes

- $n = 3$, 1770 Euler, Legendre

If p and $2p+1$ are odd prime

$x^p + y^p = z^p$ has no solution

1805 Sophie

- $n = 5$, 1825 Dirichlet, Legendre
- $n = 7$, Lamé, 1839 infinite descent

- 1850's Kummer proved result for all regular primes (infinitely many primes)

  "Birth of algebraic number theory"

- Frey 1983 proved $x^n + y^n = z^n$ has finitely many solutions, $n \geq 2$

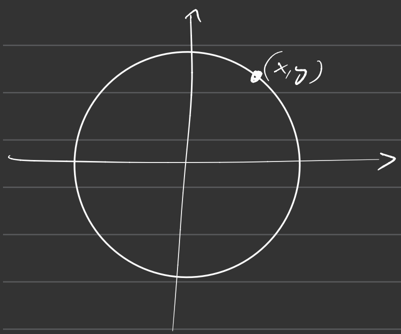
  "elliptic curves"

- 1993 Wiles

Pythagorean Triples

$x^2 + y^2 = z^2$ eg 3, 4, 5

If $hcf(x,y,z) = 1$ then it is a primitive Pythagorean triple.



Lemma 1

If $(x,y,z)=1$ and (x,y,z) is a primitive pythagorean triple (PPT) then

$$(x,y)=(x,z)=(y,z)$$

Lemma 2

If (x,y,z) is a PPT then

$$x \not\equiv y \pmod 2$$

Lemma 3

If $r,s,t \in \mathbb{N}$, $(r,s)=1$ and $rs=t^2$ then $\exists\ m,n \in \mathbb{N}$ st $r=m^2$, $s=n^2$

Theorem

Let $x,y,z \in \mathbb{N}$ with y even. Then (x,y,z) is a PPT iff $\exists\ m,n \in \mathbb{N}$ $m>n$, $(m,n)=1$, $m \not\equiv n \pmod 2$ such that

$$x=m^2-n^2 \qquad y=2mn \qquad z=m^2+n^2$$

$\cos^2\theta+\sin^2\theta=1$, $\sin 2\theta = 2\sin\theta\cos\theta$, $\cos 2\theta = \cos^2\theta - \sin^2\theta$

Proof

Let (x, y, z) be a PPT with y even so x and z are odd

Therefore

$$z + x \quad \text{and} \quad z - x$$

are even

Let

$$r = \frac{z+x}{2}, \quad s = \frac{z-x}{2}$$

We have

$$x^2 + y^2 = z^2$$

$$\Rightarrow y^2 = z^2 - x^2 = (z-x)(z+x)$$

$$= 4rs$$

If $d | r$ and $d | s$ then

$d | (r+s)$ and $d | (r-s)$

Therefore

$z+x$ and $z-x$

so $d \mid x$ and $d \mid z$

Hence, $d=1$ so $(r,s)=1$

Using Lemma 3 we know $\exists\ m,n \in \mathbb{N}$ st

$r=m^2$, $s=n^2$

and $(m,n)=1$

$$\left.\begin{aligned} z &= r+s = m^2+n^2 \\ x &= r-s = m^2-n^2 \end{aligned}\right\} \Rightarrow m,n \text{ cannot both be odd}$$

$y = \sqrt{4rs} = 2mn$

opposite direction is an exercise

Theorem

The Diophantine equation

$$x^4 + y^4 = z^2$$

has no solutions

Proof (Infinite descent)

Assume a solution

$$(x_0, y_0, z_0) \in \mathbb{N}^3$$

exists. We will show this implies there is a second solution $(x_1, y_1, z_1) \in \mathbb{N}^3$ such that $z_1 < z_0$

We have

$$(x_0^2)^2 + (y_0^2)^2 = z_0^2$$

{ Wlog assume $(x, y) = 1$ (exercise)

This implies

$$(x_0^2, y_0^2, z_0^2)$$

is a PPT

Hence $\exists$ m, n st $m > n$ $(n, m) = 1$
and $m \not\equiv n \pmod 2$

$x_0^2 = m^2 - n^2 \Rightarrow m^2 = x_0^2 + n^2$

$y_0^2 = 2mn$ so (x_0, n, m) is another PPT

$z_0 = m^2 + n^2$

$\exists$ r, s, $(r, s) = 1$, $r \not\equiv s \pmod 2$

$$\left.\begin{aligned} n &= 2rs \\ m &= r^2 + s^2 \end{aligned}\right\}$$

As $m \equiv 1 \pmod 2$

and $(m, n) = 1$ we have

$(m, 2n) = 1$

Hence by Lemma 3 $\exists$ z_1, w st

$m = z_1^2$

$2n = w^2$

Thus w is even, so $\exists$ v st

$w = 2v$

$$v^2 = \frac{w^2}{4} = \frac{n}{2} = rs$$

Using Lemma 3 corollary, $\exists$ x_1, y_1 st

$$r = x_1^2$$

$$s = y_1^2$$

$$(x_1, y_1) = 1$$

$$x_1^4 + y_1^4 = r^2 + s^2 = m = z_1^2$$

It remains to show that $z_1 < z_0$

$$z_1 < z_1^4 = m^2 < m^2 + n^2 = z_0$$

This gives an infinite sequence of ~~solutions~~

$(x_n, y_n, z_n) \in \mathbb{N}^3$ with $z_0 > z_1 > z_2 > \dots$

which contradicts the well ordering principle.

Beal's Conjecture

$$x^a + y^b = z^c$$

has no solutions $(x, y, z) \in \mathbb{Z}^3$ with $a, b, c \geq 3$

$(x,y) = (y,z) = (x,z) = 1$

Unsolved \$100,000

Catalan Conjecture

$x^m - y^n = 1$ $\quad x, y, m, n \in \mathbb{N}$, $m, n \geq 1$

has no solutions except for $x = 3$, $m = 2$, $y = 2$, $n = 3$

(14th) Gerson showed $3^n - 2^m \neq \pm 1$ unless $m = 3$, $n = 2$, $m, n > 1$

(18th) Euler showed

$x^3 - y^2 \neq \pm 1$ except for previous solutions

(1976) Tijdeman showed at most a finite number of solutions.

(2002) Mihailescu

ABC - Conjecture

Definition

if $n = \prod_{i=1}^{t} p_i^{a_i}$

then $rad(n) = \prod_{i=1}^{t} p_i$

$\forall\ \varepsilon > 0\ \exists\ K_\varepsilon$ st $a, b, c \in \mathbb{Z}$ with

$a + b = c \qquad (a, b) = 1$

Then

$$\max\{|a|, |b|, |c|\} < K_\varepsilon\, rad(abc)^{1+\varepsilon}$$

(2012) Mochizuki

Sum of Squares

Lemma

If a prime $p = 4m+1$, $m \in \mathbb{N}$, then $\exists$ $x, y \in \mathbb{Z}$ st

$$x^2 + y^2 = kp$$

for some $k \in \mathbb{N}$, $k < p$

Proof

If $p \equiv 1 \pmod 4$

then $\left(\frac{-1}{p}\right) = 1$

Hence, $\exists$ $a < p$ st

$$a^2 \equiv -1 \pmod p$$

so $\exists$ k st

$$a^2 + 1 = kp$$

$$kp = a^2 + 1 < (p-1)^2 + 1$$

$\Rightarrow k < p$ $\square$

Theorem

Let p be a prime, $p \not\equiv 3 \pmod 4$
Then $\exists\ x, y \in \mathbb{Z}$ st

$$x^2 + y^2 = p$$

Proof

$1 + 1 = 2$ (sum of two squares)

Now assume $p \equiv 1 \pmod 4$.

Let m be the smallest number
st $\exists\ x, y$

$$x^2 + y^2 = mp$$

Assume, $m > 1$

Find integers

a and b such that

$$x \equiv a \pmod m$$

$y \equiv b \pmod m$

$-\frac{m}{2} < a \leq \frac{m}{2}$

$-\frac{m}{2} < b \leq \frac{m}{2}$

Then

$$\begin{aligned} a^2 + b^2 &\equiv x^2 + y^2 \\ &\equiv mp \\ &\equiv 0 \pmod m \end{aligned}$$

Hence $\exists$ k st

$a^2 + b^2 = km$

We have

$(a^2+b^2)(x^2+y^2) = km^2p$

and

$(a^2+b^2)(x^2+y^2) = (ax+by)^2 + (ay-bx)^2$

$ax + by \equiv x^2 + y^2 \pmod{n}$

Similarly

$ay - bx \equiv xy - yx \equiv 0 \pmod{n}$

Thus

$\frac{ax+by}{m}, \frac{ay-bx}{m} \in \mathbb{Z}$

Also

$\left(\frac{ax+by}{m}\right)^2 + \left(\frac{ay-bx}{m}\right)^2 = kp$

We need to show $k < m$

$0 \le km = a^2 + b^2 < \frac{2m^2}{4} = \frac{m^2}{2}$

$k < \frac{m}{2}$

Contradiction

If $k = 0$

$a^2 + b^2 = 0$

$\Rightarrow a = b = 0$

$\Rightarrow x \equiv y \equiv 0 \pmod m$

$\Rightarrow x^2 + y^2 = mp$

Then $m | p$, impossible unless $m = 1$

Theorem

Let $n \in \mathbb{N}$. Then $\exists\, x, y \in \mathbb{N}$ st

$x^2 + y^2 = n$

iff (each prime factor of n of ~~the~~ form

$4u + 3$

occurs ~~to~~ an even power.) (*)

~~Proof~~

Suppose n satisfies (*), then

$n = t^2 u$

where t is divisible by all factors of n are congruent to 3 (mod 4) and and u containing to the rest

Each prime in u can be written as the sum of two squares. Hence $\exists$ x, y st

$$u = x^2 + y^2$$

and $n = t^2(x^2 + y^2)$

Now suppose $\exists$ prime $p \mid n$ st

$$p \equiv 3 \pmod 4$$

and p is raised to an odd power $(2j+1)$ and assume $\exists$ x, y st

$$n = x^2 + y^2$$

If $(x, y) = d$

let $a = \frac{x}{d}$, $b = \frac{y}{d}$ so

$$(a, b) = 1$$

Let $m = \frac{n}{d^2}$, then

$$a^2 + b^2 = m$$

Let p^k be the largest power of p that divides d. Then m is divisible by $p^{2j+1-2k}$

so m is divisible by p

We may assume wlog that $p \nmid a$

As otherwise $p | b$ and $(a, b) \geq p$.

Hence the linear congruence

$$az \equiv b \pmod{p}$$

has a solution

Then

$$a^2 + b^2 \equiv a^2 + az^2$$

$$\equiv a^2(1 + z^2)$$

$$\equiv 0 \pmod{p}$$

$$\Rightarrow \quad z^2 \equiv -1 \pmod{p}$$

$$\Rightarrow \left(\frac{-1}{p}\right) = 1$$

$$\Rightarrow p \equiv 1 \pmod 4$$

contradiction

Legendre 3 squares Theorem

Let $n \in \mathbb{N}$. Then $\exists\ x, y, z \in \mathbb{N}$ st

$$x^2 + y^2 + z^2 = n$$

iff n is not of the form

$$n = 4^k(8t+7), \quad k, t \in \mathbb{N} \cup \{0\}$$

4 squares Theorem

Let $n \in \mathbb{N}$. Then $\exists\ x, y, z, t \in \mathbb{N} \cup \{0\}$ st

$$n = x^2 + y^2 + z^2 + t^2$$

Lemma

If m and n can be written as the sum of 4 squares then so can m, n.

Lemma

If p is an odd prime then $\exists$ $k \le p$ st $\exists$ x, y, z, t st

$$x^2 + y^2 + z^2 + t^2 = kp$$

Proof

We will prove that $\exists$ x, y st

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}$$

Consider the two sets

$$S = \{0, 1^2, 2^2, \ldots, \left(\tfrac{p-1}{2}\right)^2\}$$

and $T = \{-1-0, -1-1^2, -1-2^2, \ldots, -1-\left(\tfrac{p-1}{2}\right)^2\}$

It should be clear that if $x, y \in S$ or $x, y \in T$

then $x \not\equiv y \pmod{p}$

However there are

$\frac{p-1}{2} + 1$ elements in each set

Thus, $S \cup T$ has

$p-1+2 = p+1$ elements

Therefore by the pigeonhole principle
$\exists\ x, y \in S \cup T$ st

$x \equiv y \pmod{p}$

one in S and one in T

Hence $\exists\ K, m$

st $x = n^2$, $y = -1-m^2$

Hence

$$n^2 \equiv -1-m^2 \pmod{p}$$

$$m^2+n^2+1 \equiv 0 \pmod{p}$$

so $m^2+n^2+1 = Kp$ for some K

We have

$$n^2 + m^2 + 1 \leq \left(\frac{p-1}{2}\right)^2 + \left(\frac{p-1}{2}\right)^2 + 1$$

$$< p^2$$

Theorem

Let p be prime. Then $\exists$ $x, y, z, t \in \mathbb{N} \cup \{0\}$ st

$$p = x^2 + y^2 + z^2 + t^2$$

Proof

$$1 + 1 + 0 + 0 = 2$$

From now on assume p is an odd prime.

Let m be the smallest natural number st

$$x^2 + y^2 + z^2 + t^2 = mp$$

has a solution $x, y, z, t \in \mathbb{N} \cup \{0\}$

We will prove $m=1$ by showing that if $m>1$ then there is a smaller such natural number

Case 1, m is even

Either x, y, z, t are all even, all odd or two are even and two are odd.

Rearrange if necessary to get

$x \equiv y \pmod 2$

$z \equiv t \pmod 2$

Then

$\frac{x+y}{2}, \frac{x-y}{2}, \frac{z-t}{2}, \frac{z+t}{2}$ are all integers

and

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z-t}{2}\right)^2 + \left(\frac{z+t}{2}\right)^2$$

$$= \frac{mp}{2}$$

a contradiction as $\frac{m}{2} \in \mathbb{N}$ and $\frac{m}{2} < m$

From now on assume m is odd

Find $a, b, c, d \in \mathbb{Z}$ st

$a \equiv x \pmod m$

$b \equiv y \pmod m$

$c \equiv z \pmod m$

$d \equiv t \pmod m$

$\frac{-m}{2} < a, b, c, d < \frac{m}{2}$

Then,

$$x^2 + y^2 + z^2 + t^2 \equiv a^2 + b^2 + c^2 + d^2 \pmod m$$

$$\equiv 0 \pmod m$$

so $\exists$ K st

$$a^2 + b^2 + c^2 + d^2 = Km$$

Also

$$a^2 + b^2 + c^2 + d^2 \leq 4\left(\frac{m}{2}\right)^2 = m^2$$

$\Rightarrow k < m$

$a = b = c = d = 0$

$\Rightarrow x \equiv y \equiv z \equiv t \equiv 0 \pmod{m}$

So $m^2 \mid (x^2+y^2+z^2+t^2)$

$\Rightarrow m^2 \mid mp \Rightarrow m \mid p$

Impossible

~~Therefore~~ $k > 0$

We have

$$(x^2+y^2+z^2+t^2)(a^2+b^2+c^2+d^2) = km^2p$$

and

$$(x^2+y^2+z^2+t^2)(a^2+b^2+c^2+d^2)$$
$$= \overbrace{(ax+by+cz+dt)^2}^{(mx)^2} + \overbrace{(bx-ay+dz-ct)^2}^{(my)^2}$$
$$+ \overbrace{(cx-dy-az+bt)^2}^{(mz)^2} + \overbrace{(dx+cy-bz-at)^2}^{(mt)^2}$$

Each of the latter 4 terms is divisible by m^2

Then

$$x^2+y^2+z^2+t^2=kp$$

Contradicts definition of m. Therefore $m=1$

Waring's problem

Let $k \in \mathbb{N}$. Then $\exists$ an integer $g(k)$ s.t. every integer can be written as a sum of $g(k)$, kth powers

$$g(2)=4$$

Hilbert (1906) showed existence

$$g(3)=9$$

$$g(4)=19$$

$$g(5)=37$$

$$g(k) = \left[\left(\tfrac{3}{2}\right)^{k}\right] + 2^{k} - 2$$

Last checked up to

$$6 \leq k \leq 471{,}600{,}000$$

Only two numbers

23 239

Cannot be represented as a sum of eight cubes

Define

$G(k)$ to be the smallest natural number such that all sufficiently large natural numbers can be written as a sum of $G(k)$ k^{th} powers.

$$4 \leq G(3) \leq 7$$

Pell's Equation

$d, n \in \mathbb{Z}$

Find $x, y \in \mathbb{Z}$ s.t

$$x^2 - dy^2 = n$$

$d < 0$, $n < 0$

No solutions

$d < 0$, $n > 0$

finite # of solutions

If $d = D^2$

$$x^2 - D^2 y^2 = (x - Dy)(x + Dy) = n$$

Finite # of solutions

From now on assume $d > 0$ and $d \neq D^2$

Theorem

Let $d \in \mathbb{N}$, $n \in \mathbb{Z}$

$d \neq \square^2$, $|n| < d$

If $x^2 - dy^2 = n$ $\quad x, y \in \mathbb{Z}$

Then $\frac{x}{y}$ is a convergent of $\sqrt{d}$

Proof

Assume $n > 0$, we have

$$(x - \sqrt{d}\,y)(x + \sqrt{d}\,y) = n$$

Then $x > \sqrt{d}\,y$

so $\frac{x}{y} > \sqrt{d}$

$$\frac{x}{y} - \sqrt{d} = \frac{x - \sqrt{d}\,y}{y}$$

$$= \frac{x^2 - \sqrt{d}\,y^2}{y(x + \sqrt{d}\,y)}$$

$$= \frac{n}{y(x + \sqrt{d}y)}$$

$$< \frac{n}{y(2\sqrt{d}y)}$$

$$< \frac{1}{2y^2}$$

Thus $\frac{x}{y}$ is a convergent of $\sqrt{d}$

<u>$n < 0$</u>

$$x^2 - dy^2 = n$$

$$y^2 - \frac{x^2}{d} = -\frac{n}{d} > 0$$

Then, by the same argument

$\frac{y}{x}$ is a convergent of $\frac{1}{\sqrt{d}}$ and

therefore of $\sqrt{d}$

When $n=1$, this is called pell's equation

Archimedes and Diophantus considered special cases

12th century Bhaskara

developed a method of solution

1657 Fermat proposed the problem

1767 Euler provided some formal theory

1768 Lagrange produced a result

Pell's Theorem

Let $d \in \mathbb{N}$, $d \neq n^2$

Let $\frac{p_k}{q_k}$ be the kth

convergent of $\sqrt{d}$

Let t be the period length of the continued fraction expansion of $\sqrt{d}$

- When t is even, the solution of

$$x^2 - dy^2 = -1$$

has no solution

The solution of

$$x^2 - dy^2 = 1$$

$x = p_k$, $y = q_k$ where

$$k = jt - 1, \quad j \in \mathbb{N}$$

- When t is odd the solution of

$$x^2 - dy^2 = 1$$

are $x = p_k$, $y = q_k$

where $k = 2jt - 1$ $j \in \mathbb{N}$

The solutions of

$$x^2 - dy^2 = -1$$

are $x = p_k$ $y = q_k$

where $k = (2j-1)t - 1$ $j \in \mathbb{N}$