Primes of the form $x^2 + y^2$

My tour guide in the land of “Number Theory”

CHAN Heng Huat

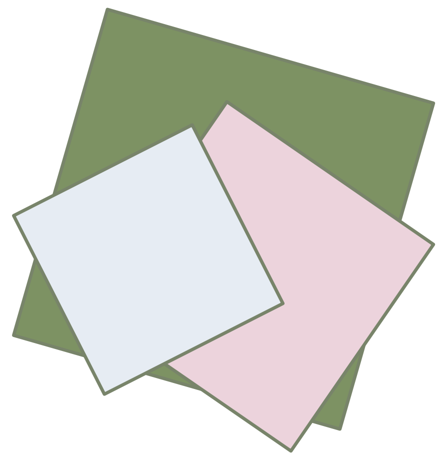
National University of Singapore

Squares

Squares

A square integer is an integer of the form k^2.

The first few examples of squares are $1, 4, 9, 16, 25, \cdots$.



The Division Algorithm

The Division Algorithm

Given any integer b and a positive integer a, there exists unique integers q (quotient) and r (remainder) with $0 \leq r < a$ such that $b = aq + r$.

The Division Algorithm

Let $a = 2$ and N is any integer. Any integer N is of the form $2q$ or $2q + 1$.

Or we say that an integer N is either EVEN (if $N = 2q$) or ODD ($N = 2q + 1$).

Even integers : $0, 2, 4, 6, 8, 12 \cdots$

Odd integers : $1, 3, 5, 7, 9, 11, \cdots$

Given any integer b and a positive integer a, there exists unique integers q (quotient) and r (remainder) with $0 \leq r < a$ such that $b = aq + r$.

The Division Algorithm

Let $a = 4$ and N is any integer.

Any integer N is of the form $4q$, $4q + 1$, $4q + 2$ or $4q + 3$.

Note that an EVEN integer is either of the form $4q$ or $4q + 2$ and an ODD integer is either of the form $4q + 1$ or $4q + 3$.

Even integers : $\{0, 2, 4, 6, 8, 10, 12, \cdots\} = \{0, 4, 8, 12, \cdots\} \cup \{2, 6, 10, 14, \cdots\}$

Integers of the form $4q$ Integers of the form $4q + 2$

Odd integers : $\{1, 3, 5, 7, 9, 11, \cdots\} = \{1, 5, 9, 13, \cdots\} \cup \{3, 7, 11, 15, \cdots\}$

Integers of the form $4q + 1$ Integers of the form $4q + 3$

Given any integer b and a positive integer a, there exists unique integers q (quotient) and r (remainder) with $0 \leq r < a$ such that $b = aq + r$.

Divisors and Primes

Divisors

Given any integer b and a positive integer a, if $b = aq$ (or in other words, $r = 0$), then we say that a divides b or a is a divisor of b.

$2021 = 43 \cdot 47$

43 and 47 divide 2021

Primes

A prime number is a positive integer $p > 1$ that has exactly two DISTINCT divisors, 1 and p.

The first few examples of primes are $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \cdots$.

The number 6 is not a prime. It is composite.

Wilson's Theorem

An important property of Primes

Wilson's Theorem

Let $p > 2$ be a prime. Then $(p-1)! + 1$ is divisible by p.

For $p = 5$, $4! + 1 = 25$ and this is divisible by 5.

Wilson's Theorem

A corollary to this theorem is that if p is a prime of the form $4k + 1$, then there exists an integer u such that p divides $u^2 + 1$.

For $p = 3$, we cannot find u such that $u^2 + 1$ that is divisible by 3.

For $p = 5$, we find that 5 divides $2^2 + 1$.

Primes of the form $x^2 + y^2$

An observation

A. Girard (1595-1632) and P. Fermat (1601-1665)

independently observed that

p is a prime of the form $4k+1$ if and only if p is a sum of two squares

Examples

3 is not a sum of two squares

5 is a sum of two squares $5 = 1^2 + 2^2$

7 is not a sum of two squares

11 is not a sum of two squares

13 is a sum of two squares $13 = 2^2 + 3^2$

Quiz

1. True or False: The number 144169 is a sum of two squares.

   True, because 144169 is a prime of the form $4k+1$.

2. True or False: The number 2021 is a sum of two squares.

   False.

   $2021 = 43 \cdot 47$. It is of the form $4k+1$ but it is NOT a prime. Also it is a product of primes of the form $4k+3$ and so it cannot be a sum of two squares.

L. Euler

According to Gauss, Euler was the first to give a proof of the Girard-Fermat conjecture.

My Tour Guide

p is a prime of the form $4k+1$ if and only if p is a sum of two squares

In my course MA3265 Introduction to Number Theory, my "tour guide" appears in almost everywhere in the land of "number theory".

Complex numbers, Elementary number theory and Fermat's method of descent

Legendre symbol and the Jacobsthal sum

Binary quadratic forms

Continued fractions

Jacobi's Triple Product Identity and Partition function

Minkowski's Theorem and Geometry of Numbers

Easy Direction

An odd prime is either of the form $4k+1$ or $4k+3$. We will show that if p is of the form $4k+3$ then it cannot be a sum of two squares.

An integer is of the form $2k$ or $2k+1$. Therefore a square is of the form $4k$ or $4k+1$. This means that the sum of two squares is of the form $4k, 4k+1$ or $4k+2$.

Therefore a prime of the form $4k+3$ can never be a sum of two squares.

Hard Direction

It remains to show that if a prime is of the form $4k + 1$, then it is a sum of two primes.

Continued fraction and Hermite's proof

Continued Fractions

A simple continued fraction is of the form $a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{j-1} + \cfrac{1}{a_j}}}}$.

where $a_k, 0 \leq k \leq j$ are positive integers.

The notation for the continued fraction is $< a_0, a_1, \cdots, a_j >$.

Continued Fractions

Find the continued fraction expansion of $4/17$.

The continued fraction is $< 0, 4, 4 >$.

A simple continued fraction is of the form $a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{j-1} + \cfrac{1}{a_j}}}}$.

where $a_k, 0 \leq k \leq j$ are positive integers.

The notation for the continued fraction is $< a_0, a_1, \cdots, a_j >$.

Continued Fractions

Let $(a_n)_{n=0}^{\infty}$ be a sequence of INTEGERS, all positive except possibly a_0.

Define $(h_n)_{n=0}^{\infty}$ and $(k_n)_{n=0}^{\infty}$ by

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

$$k_{-2} = 1, k_{-1} = 0, k_i = a_i k_{i-1} + k_{i-2} \quad \text{for } i \geq 0.$$

Continued Fractions

Note that k_n is increasing. Important property: $\frac{h_{s+1}}{k_{s+1}} - \frac{h_s}{k_s} = \frac{(-1)^s}{k_s k_{s+1}}$

For $0 \leq s \leq j$, it can be shown that $< a_0, a_1, \cdots, a_s >= \frac{h_s}{k_s}$.

The continued fraction of $4/17$ is $< 0, 4, 4 >$.

The convergents are $0, 1/4, 4/17$.

Let $(a_n)_{n=0}^{\infty}$ be a sequence of INTEGERS, all positive except possibly a_0.

Define $(h_n)_{n=0}^{\infty}$ and $(k_n)_{n=0}^{\infty}$ by

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

$$k_{-2} = 1, k_{-1} = 0, k_i = a_i k_{i-1} + k_{i-2} \quad \text{for } i \geq 0.$$

A simple Lemma and primes of the form $x^2 + y^2$

Let $\xi =< a_0, a_1, \cdots, a_j >$. Then for $0 \leq s \leq j$, $\left|\xi - \frac{h_s}{k_s}\right| < \left|\frac{h_s}{k_s} - \frac{h_{s+1}}{k_{s+1}}\right|$.

The above inequality is established using the facts that the sequence $(h_{2j}/k_{2j})_{j=1}^{\infty}$ increases to ξ and $(h_{2j+1}/k_{2j+1})_{j=1}^{\infty}$ decreases to ξ.

Important property: $\frac{h_{s+1}}{k_{s+1}} - \frac{h_s}{k_s} = \frac{(-1)^s}{k_s k_{s+1}}$

A simple Lemma and primes of the form $x^2 + y^2$

Let $\xi =< a_0, a_1, \cdots, a_j >$. Then for $0 \le s \le j$, $\left|\xi - \frac{h_s}{k_s}\right| < \left|\frac{h_s}{k_s} - \frac{h_{s+1}}{k_{s+1}}\right|$.

Let $u > 0$ be such that p divides $u^2 + 1$.

Let $\frac{u}{p} =< a_0, a_1, \cdots, a_j >$.

Choose s such that $k_s < \sqrt{p} < k_{s+1}$.

By the lemma and the important identity, we deduce that $|uk_s - h_s p| < \sqrt{p}$, or $(uk_s - h_s p)^2 < p$.

Important property: $\frac{h_{s+1}}{k_{s+1}} - \frac{h_s}{k_s} = \frac{(-1)^s}{k_s k_{s+1}}$

A simple Lemma and primes of the form $x^2 + y^2$

Let $\alpha = k_s$ and $\beta = uk_s - h_s p$. We check that $\alpha^2 + \beta^2 = p$.

Important property: $$\frac{h_{s+1}}{k_{s+1}} - \frac{h_s}{k_s} = \frac{(-1)^s}{k_s k_{s+1}}$$

Example

The confinued fraction of $23800/144169$ is $< 0, 6, 17, 2, 1, 1, 2, 17, 6 >$.

The convergents are

$0, 1/6, 17/103, 35/212, 52/315, 87/527, 226/1369, 3929/23800, 23800/144169.$

$$\sqrt{144169} = 379.696\cdots \qquad 315 \leq \sqrt{144169} < 527$$

Therefore, $144169 = 315^2 + 212^2$.

We can read off the solution to $p = x^2 + y^2$ from the continued fraction expansion of u/p where $p|(u^2+1)$ and $u < p$.

Important property: $\dfrac{h_{s+1}}{k_{s+1}} - \dfrac{h_s}{k_s} = \dfrac{(-1)^s}{k_s k_{s+1}}$

Geometry of Numbers

Convex sets

A subset $X \subset \mathbf{R}^n$ is convex if whenever $x, y \in X$, then all points on the straight line segment joining x to y also lie in X.

Convex

NOT Convex

A subset X is centrally symmetric if $x \in X$ implies that $-x \in X$.

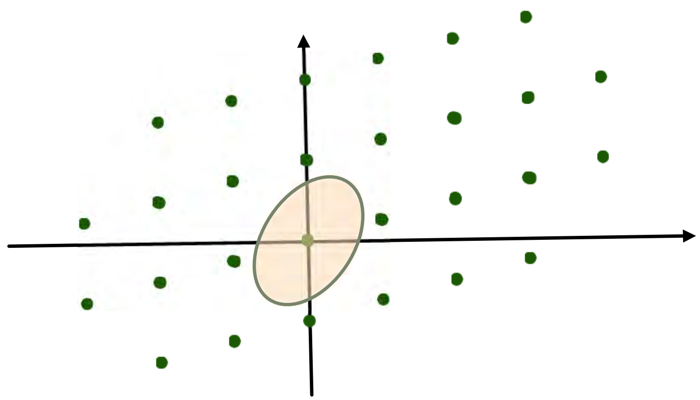
Minkowski's Theorem

We state the result for $n = 2$.

Let L be an 2-dimensional lattice in $\mathbf{R}^2$ with fundamental domain T.

Let X be a bounded centrally symmetric convex subset of $\mathbf{R}^2$.

If $\text{vol}(X) > 2^2\text{vol}(T)$, then X contains a non-zero point of L.

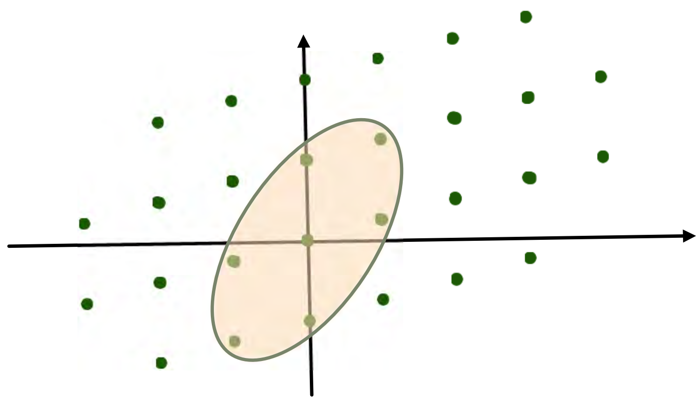


Minkowski's Theorem

Let L be an 2-dimensional lattice in $\mathbf{R}^2$ with fundamental domain T.

Let X be a bounded centrally symmetric convex subset of $\mathbf{R}^2$.

If $\text{vol}(X) > 2^2\text{vol(T)}$, then X contains a non-zero point of L.



Minkowski's Theorem

Recall that if p is a prime of the form $4k + 1$, then there exists an integer u such that $u^2 + 1$ is a multiple of p.

Minkowski's Theorem

Let u be such that p divides $u^2 + 1, 0 < u < p$.

Let L be the lattice generated by $(1, u)$ and $(0, p)$.

The volume of L is p.

Let X be the sphere with radius $\sqrt{3p/2}$.

The volume of X is $3p\pi/2 > 4p = 2^2\text{vol}(L)$.

By Minkowski's Theorem, X contains a non-zero element of L, say (α, β).

Let X be a bounded centrally symmetric convex subset of $\mathbf{R}^n$.

If $\text{vol}(X) > 2^n\text{vol}(\text{T})$, then X contains a non-zero point of L.

Minkowski's Theorem

Claim: $\alpha^2 + \beta^2 = p$

$(\alpha, \beta) = \ell(1, u) + k(0, p) \in L, \ell, k \in \mathbf{Z}$

$\alpha^2 + \beta^2$ is divisible by p

$\alpha^2 + \beta^2 = 3p/2 < 2p$