Un aperçu des formes quadratiques
An overview of quadratic forms

Siva Sankar Nair

Université de Montréal

$\pi + \varepsilon$ Day, 2023

($\varepsilon = 1$)

Fermat, 1600s

Question: what primes can be written as the sum of two squares?

$$p = a^2 + b^2, \quad \text{where } a \text{ and } b \text{ are integers}$$

Answer: They are $p = 2$ and those primes p which are one more than a multiple of 4:

$$p = 4k + 1$$

Fermat's letter to Mersenne on Xmas Day

cas, si vous ajoutez au quotient de la seconde division, multiplié par la différence des deux diviseurs, le reste de la seconde division, ce qui restera sera mesuré par le premier diviseur.

Exemple : 117 est mesuré par 3. Divisez encore 117 par 4; le quotient sera 29 et le reste de la division 1.

Ajoutez au quotient 29, multiplié par la différence des diviseurs (qui ne change ici rien, parce que c'est l'unité), le reste de la dite division, qui est 1; la somme 30 sera aussi mesurée par 3, premier diviseur.

J'ai déjà trop écrit et il me semble qu'il est temps que vous parliez, après avoir employé si mal votre temps à lire cette longue lettre, qui vous confirmera que je suis etc.

XLV.

FERMAT A MERSENNE.

MARDI 25 DÉCEMBRE 1640.

(A, f^os 12-13 *bis*, B, f^o 19.)

MON RÉVÉREND PÈRE,

1. Je languissois dans l'attente de vos lettres et de M. de Frenicle. Je suis bien aise qu'il approuve ce que j'ai fait (1); et afin qu'il ne soit plus en doute de ce que je lui demande, voici trois questions que je lui propose, pource que les spéculations que j'y ai faites ne me satisfont pas pleinement :

1° La raison essentielle pourquoi 3, 5, 17, 257, etc. à l'infini, sont toujours nombres premiers;

2° Qu'il me donne quelqu'un de ses autres moyens pour trouver

à l'infini des nombres premiers de tels nombres de figures qu'on voudra.

Sur quoi je voudrois être éclairci si une de mes pensées est vraie, qu'en la progression d'un nombre pair, comme 6, toutes les puissances +1 de la progression qui ont pour exposant : 1, 2, 4, 8, 16, etc. sont nombres premiers, si elles ne sont pas mesurées par un de ceux-ci : 3, 5, 17, 257, etc.; laquelle proposition, si elle est vraie, est de très grand usage.

Si je puis une fois tenir la raison fondamentale que 3, 5, 17, etc. sont nombres premiers, il me semble que je trouverai de très belles choses en cette matière, car déjà j'ai trouvé des choses merveilleuses dont je vous ferai part, après que j'aurai eu votre réponse et celle de M. Frenicle.

3° Je lui demande un moyen plus général que celui que j'ai inventé pour savoir quels sont les multiples de l'exposant utiles à la division.

Après cela, je travaillerai aux propositions que vous me demandez.

2. Sur le sujet des triangles rectangles (1), voici mes fondements :

1° Tout nombre premier, qui surpasse de l'unité un multiple du quaternaire, est une seule fois la somme de deux quarrés, et une seule fois l'hypoténuse d'un triangle rectangle.

2° Le même nombre et son quarré sont chacun une fois la somme de deux quarrés;

Son cube et son quarréquarré sont chacun deux fois la somme de deux quarrés;

Son carrécube et son cubecube sont chacun trois fois la somme de deux quarrés;

Etc., à l'infini.

3° Ce même nombre étant une fois l'hypoténuse d'un triangle rectangle, son quarré l'est deux fois, son cube trois, son quarréquarré quatre, etc. à l'infini.

Question: what about any number n? When can we write

$$n = a^2 + b^2 \ ?$$

Answer: If and only if all primes of the form $p = 4k + 3$ that divide n occur to an even power in the prime factorization of n.

Generalizations

Question:

Answer:

QUADRATIC FORMS!

Quadratic Forms

Definition

A (binary) quadratic form is a homogeneous polynomial of degree two in two variables

$$Q(x, y) = ax^2 + bxy + cy^2 \quad a, b \in \mathbb{Z}$$

Given a quadratic form, we would like to know which numbers n are represented by it

$$n = ax^2 + bxy + cy^2$$

For example, if $a = 1, b = 0, c = 1$ then we have

$$n = x^2 + y^2$$

$a = 1, b = 2, c = 2$, then

$$n = x^2 + 2xy + 2y^2$$

Equivalent forms

$n = x^2 + y^2$	$n = x^2 + 2xy + 2y^2$
$n = (x-y)^2 + 2(x-y) + 2y^2$	$n = (x+y)^2 + y^2$
$n = u^2 + 2uy + 2y^2$	$n = v^2 + y^2$

These two quadratic forms represent the same integers.

Definition

Two quadratic forms $Q(x, y)$ and $P(x, y)$ are equivalent if

$$P(u, v) = Q(\alpha u + \beta v, \gamma u + \gamma v)$$

for some $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ such that $\alpha\delta - \beta\gamma = 1$.

Equivalent forms

$n = x^2 + y^2$	$n = x^2 + 2xy + 2y^2$
$n = (x-y)^2 + 2(x-y) + 2y^2$	$n = (x+y)^2 + y^2$
$n = u^2 + 2uy + 2y^2$	$n = v^2 + y^2$

These two quadratic forms represent the same integers.

Definition

Two quadratic forms $Q(x, y)$ and $P(x, y)$ are equivalent if

$$P(u, v) = Q(\alpha u + \beta v, \gamma u + \gamma v)$$

for some $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ such that $\alpha\delta - \beta\gamma = 1$.

Equivalent forms

$n = x^2 + y^2$	$n = x^2 + 2xy + 2y^2$
$n = (x - y)^2 + 2(x - y) + 2y^2$	$n = (x + y)^2 + y^2$
$n = u^2 + 2uy + 2y^2$	$n = v^2 + y^2$

These two quadratic forms represent the same integers.

Definition

Two quadratic forms $Q(x, y)$ and $P(x, y)$ are equivalent if

$$P(u, v) = Q(\alpha u + \beta v, \gamma u + \gamma v)$$

for some $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ such that $\alpha\delta - \beta\gamma = 1$.

Equivalent forms

$n = x^2 + y^2$	$n = x^2 + 2xy + 2y^2$
$n = (x - y)^2 + 2(x - y) + 2y^2$	$n = (x + y)^2 + y^2$
$n = u^2 + 2uy + 2y^2$	$n = v^2 + y^2$

These two quadratic forms represent the same integers.

Definition

Two quadratic forms $Q(x, y)$ and $P(x, y)$ are equivalent if

$$P(u, v) = Q(\alpha u + \beta v, \gamma u + \gamma v)$$

for some $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ such that $\alpha\delta - \beta\gamma = 1$.

Equivalent forms

$n = x^2 + y^2$	$n = x^2 + 2xy + 2y^2$
$n = (x - y)^2 + 2(x - y) + 2y^2$	$n = (x + y)^2 + y^2$
$n = u^2 + 2uy + 2y^2$	$n = v^2 + y^2$

These two quadratic forms represent the same integers.

Definition

Two quadratic forms $Q(x, y)$ and $P(x, y)$ are equivalent if

$$P(u, v) = Q(\alpha u + \beta v, \gamma u + \gamma v)$$

for some $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ such that $\alpha\delta - \beta\gamma = 1$.

Equivalent forms

$$n = x^2 + y^2 \qquad n = x^2 + 2xy + 2y^2$$

$$n = (x - y)^2 + 2(x - y) + 2y^2 \qquad n = (x + y)^2 + y^2$$

$$n = u^2 + 2uy + 2y^2 \qquad n = v^2 + y^2$$

These two quadratic forms represent the same integers.

Definition

Two quadratic forms $Q(x, y)$ and $P(x, y)$ are equivalent if

$$P(u, v) = Q(\alpha u + \beta v, \gamma u + \gamma v)$$

for some $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ such that $\alpha\delta - \beta\gamma = 1$.

Ideas of Gauss

Discriminant: $D = b^2 - 4ac$. Gauss studied forms with $D < 0$ and $a > 0$.

Definition

$Q(x, y) = ax^2 + bxy + y^2$ is reduced if

$$-a < b \leq a < c \quad \text{or} \quad 0 \leq b \leq a = c$$

Gauss' algorithm: shows that there is a unique reduced form in each equivalence class of quadratic forms!

The class number

For a given discriminant, there are only finitely many reduced quadratic forms with that discriminant!
This means that there are only finitely many equivalence classes of quadratic forms with discriminant D.

Definition

The class number, denoted $h(D)$, is the number of equivalence classes of quadratic forms with discriminant D.

For example, if $D = -4$, then $a \leq 1$ which forces $a = 1, b = 0$ and $c = 1$. Therefore, $x^2 + y^2$ is the only equivalence class with discriminant -4, and $h(-4) = 1$.
$D = -20$ has two equivalence classes corresponding to:

$$x^2 + 5y^2 \quad \text{and} \quad 2x^2 + 2xy + 3y^2$$

Gauss' class number problem

Gauss came up with nine $D < 0$ which have $h(D) = 1$:

$$D = -3, -4, -7, -8, -11, -19, -43, -67, -163,$$

and conjectured that these are all. Proved by Heegner, Stark and Baker in the 1950s and 1960s. These are called Heegner numbers.
Gauss' class number problem: for $m \geq 1$, list all discriminants such that $h(D) = m$.

1. $m = 2$: Baker, Stark 1970s
2. $m = 3$: Oesterlé 1985
3. $m = 4$: Arno 1992
4. $m = 5, 6, 7$: Wagner 1996.
5. $m \leq 100$: Watkins 2004.

Composition laws and group structure

1. Gauss described a set of composition laws on the forms that gave rise to a group structure (early 1800s)!
2. Dirichlet related them to ideals in a ring in $\mathbb{Q}(\sqrt{D})$ to give cleaner composition rules (1890s) Bhargava gave a new description of the composition laws using what is now called Bhargava's cubes (2004)

MATHEMATICAL GAMES

Six sensational discoveries that somehow or another have escaped public attention

In number theory the most exciting discovery of the past year is that when the transcendental number e is raised to the power of π times $\sqrt{163}$, the result is an integer. The Indian mathematician Srinivasa Ramanujan had conjectured that e to the power of $\pi\sqrt{163}$ is integral in a note in the *Quarterly Journal of Pure and Applied Mathematics* (Volume 45, 1913–14, page 350). Working by hand, he found the value to be 262,537,412,-640,768,743.999,999,999,999,.... The calculations were tedious, and he was unable to verify the next decimal digit. Modern computers extended the 9's much farther; indeed, a French program of 1972 went as far as two million 9's. Unfortunately no one was able to prove that the sequence of 9's continues forever (which, of course, would make the number integral) or whether the number is irrational or an integral fraction.

In May, 1974, John Brillo of the University of Arizona found an ingenious way of applying Euler's constant to the calculation and managed to prove that the number exactly equals 262,537,412,-640,768,744. How the prime number 163 manages to convert the expression to an integer is not yet fully understood.

The j-function

For $\tau \in \mathbb{C}$ such that $\mathrm{Im}(\tau) > 0$, we have

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots,$$

where $q = e^{2\pi i \tau}$.

It is an important and deep theorem in algebraic number theory that for the Heegner numbers D and

$$\tau = \frac{-1 + \sqrt{D}}{2},$$

$j(\tau)$ is an integer!

$$j\left(\frac{-1 + \sqrt{-163}}{2}\right) = -(640320)^3 = -262537412640768000.$$

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999925\ldots$$

$$e^{\pi\sqrt{67}} = 147197952743.999998\ldots$$

$$e^{\pi\sqrt{43}} = 884736743.9998\ldots$$

$$e^{\pi\sqrt{19}} = 885479.7777\ldots$$

C'EST TOUT!
MERCI!