The Class Number Problem

Dylan Nelson

Stellenbosch University

18 October 2019

Table of Contents

Prime Producing Polynomials

Euler noticed that the polynomial $n^2 + n + 41$ is prime for all values of n such that $0 \leq n \leq 39$.

Prime Producing Polynomials

Euler noticed that the polynomial $n^2 + n + 41$ is prime for all values of n such that $0 \leq n \leq 39$.
For $n = 40$, it takes the value $40^2 + 40 + 41 = 41^2$.

Prime Producing Polynomials

Euler noticed that the polynomial $n^2 + n + 41$ is prime for all values of n such that $0 \leq n \leq 39$.
For $n = 40$, it takes the value $40^2 + 40 + 41 = 41^2$.
In general, for the polynomial $n^2 + n + A$ takes on the value A^2 for $n = A - 1$, and so the largest range of values for which it can be prime is $0 \leq n \leq A - 2$.

Prime Producing Polynomials

Euler noticed that the polynomial $n^2 + n + 41$ is prime for all values of n such that $0 \leq n \leq 39$.
For $n = 40$, it takes the value $40^2 + 40 + 41 = 41^2$.
In general, for the polynomial $n^2 + n + A$ takes on the value A^2 for $n = A - 1$, and so the largest range of values for which it can be prime is $0 \leq n \leq A - 2$.
Determining all values of A for which this maximal range of prime numbers is achieved turns out to be equivalent to something called the Class Number 1 problem for imaginary quadratic fields.

Prime Producing Polynomials

Euler noticed that the polynomial $n^2 + n + 41$ is prime for all values of n such that $0 \leq n \leq 39$.
For $n = 40$, it takes the value $40^2 + 40 + 41 = 41^2$.
In general, for the polynomial $n^2 + n + A$ takes on the value A^2 for $n = A - 1$, and so the largest range of values for which it can be prime is $0 \leq n \leq A - 2$.
Determining all values of A for which this maximal range of prime numbers is achieved turns out to be equivalent to something called the Class Number 1 problem for imaginary quadratic fields.
This problem was finally solved by Alan Baker in the 1970's!

Binary Quadratic Forms

Definition (Binary Quadratic Form)

A binary quadratic form is an expression of the form

$$ax^2 + bxy + cy^2$$

for some integers a, b, and c.

Binary Quadratic Forms

Definition (Binary Quadratic Form)

A binary quadratic form is an expression of the form

$$ax^2 + bxy + cy^2$$

for some integers a, b, and c.

Definition (Discriminant)

The discriminant of the binary quadratic form $ax^2 + bxy + cy^2$ is $D = b^2 - 4ac$.

Definition (Positive Definite)

A binary quadratic form $ax^2 + bxy + cy^2$ is called *positive-definite* if $D = b^2 - 4ac < 0$ and $a > 0$.

Definition (Positive Definite)

A binary quadratic form $ax^2 + bxy + cy^2$ is called *positive-definite* if $D = b^2 - 4ac < 0$ and $a > 0$.

Remark

A binary quadratic form $ax^2 + bxy + cy^2$ is positive-definite precisely when $ax^2 + bxy + cy^2$ is positive for all real numbers x and y with $(x, y) \neq (0, 0)$.

Definition (Positive Definite)

A binary quadratic form $ax^2 + bxy + cy^2$ is called *positive-definite* if $D = b^2 - 4ac < 0$ and $a > 0$.

Remark

A binary quadratic form $ax^2 + bxy + cy^2$ is positive-definite precisely when $ax^2 + bxy + cy^2$ is positive for all real numbers x and y with $(x, y) \neq (0, 0)$.

Remark

For our purposes, we will only consider positive-definite binary quadratic forms as these are the forms that are relevant when discussing the class number problem for imaginary quadratic fields, and I was too lazy to figure out what needs to change in order to deal with binary quadratic forms more generally.

Definition (Equivalence)

Two binary quadratic forms are said to be equivalent if there is an invertible linear change of variables which transforms one into the other. In other words, the binary quadratic form $p(x, y) = ax^2 + bxy + cy^2$ is equivalent to precisely the forms $p(sx + ty, ux + vy)$ where

$$\begin{pmatrix} s & t \\ u & v \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

We require the determinant of the matrix to be 1 so that $p(sx + ty, ux + vy)$ remains positive-definite.

Remark

If two binary quadratic forms are equivalent, then they have the same discriminant.

Reduction of Binary Quadratic Forms

Definition

A (positive-definite) binary quadratic form $ax^2 + bxy + cy^2$ is said to be *reduced* if $-a < b \leq a \leq c$, or $0 < b \leq a = c$.

Reduction of Binary Quadratic Forms

Definition

A (positive-definite) binary quadratic form $ax^2 + bxy + cy^2$ is said to be *reduced* if $-a < b \leq a \leq c$, or $0 < b \leq a = c$.

Theorem

Every equivalence class of positive-definite binary quadratic forms contains a reduced element.

Proof

We apply the following procedure to $ax^2 + bxy + cy^2$:
We note that the matrix

$$\begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$$

is in $\mathrm{SL}_2(\mathbb{Z})$, and transforms $ax^2 + bxy + cy^2$ into $a'x^2 + b'xy + c'y^2$ where

$$a' = a \qquad b' = -2an + b \qquad c' = an^2 - bn + c.$$

Proof

We apply the following procedure to $ax^2 + bxy + cy^2$:
We note that the matrix

$$\begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$$

is in $\mathrm{SL}_2(\mathbb{Z})$, and transforms $ax^2 + bxy + cy^2$ into $a'x^2 + b'xy + c'y^2$ where

$$a' = a \qquad b' = -2an + b \qquad c' = an^2 - bn + c.$$

There is a unique value of n such that $(2n-1)a < b \leq (2n+1)a$. We choose this n in the transformation above so that we obtain a binary quadratic form $ax^2 + bxy + cy^2$ where $-a < b \leq a$.

Proof

We apply the following procedure to $ax^2 + bxy + cy^2$:
We note that the matrix

$$\begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$$

is in $\mathrm{SL}_2(\mathbb{Z})$, and transforms $ax^2 + bxy + cy^2$ into $a'x^2 + b'xy + c'y^2$ where

$$a' = a \qquad b' = -2an + b \qquad c' = an^2 - bn + c.$$

There is a unique value of n such that $(2n-1)a < b \leq (2n+1)a$. We choose this n in the transformation above so that we obtain a binary quadratic form $ax^2 + bxy + cy^2$ where $-a < b \leq a$.

Proof

If $a \leq c$, then we are done. Otherwise we apply the transformation given by

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathsf{SL}_2(\mathbb{Z}).$$

Proof

If $a \leq c$, then we are done. Otherwise we apply the transformation given by

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

This has the effect of transforming $ax^2 + bxy + cy^2$ into $cx^2 - bxy + ay^2$.

Proof

If $a \leq c$, then we are done. Otherwise we apply the transformation given by

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

This has the effect of transforming $ax^2 + bxy + cy^2$ into $cx^2 - bxy + ay^2$. We apply these two transformations repeatedly until we obtain a reduced binary quadratic form. Since applying these two operations in succession strictly reduces the coefficient of x^2, this process must terminate.

Fact

The reduced binary quadratic form in each equivalence class is unique.

Definition (Class Number)

The number of equivalence classes of positive-definite binary quadratic forms with discriminant D is called the *Class Number* of the discriminant D.

Remark

The *Class Number Problem* is the problem of identifying all discriminants D with a given class number.

The Connection with Möbius Transformations

To the binary quadratic form $p(x, y) = ax^2 + bxy + cy^2$ with discriminant D, we assign the complex number

$$\tau(p) = \frac{b + \sqrt{D}}{2a}$$

in the upper half-plane.

The Connection with Möbius Transformations

To the binary quadratic form $p(x, y) = ax^2 + bxy + cy^2$ with discriminant D, we assign the complex number

$$\tau(p) = \frac{b + \sqrt{D}}{2a}$$

in the upper half-plane.

We note that $\mathrm{SL}_2(\mathbb{Z})$ acts on the upper half plane via *Möbius transformations*:

$$\begin{pmatrix} s & t \\ u & v \end{pmatrix} \tau = \frac{s\tau + t}{u\tau + v}.$$

The Connection with Möbius Transformations

To the binary quadratic form $p(x, y) = ax^2 + bxy + cy^2$ with discriminant D, we assign the complex number

$$\tau(p) = \frac{b + \sqrt{D}}{2a}$$

in the upper half-plane.
We note that $\mathrm{SL}_2(\mathbb{Z})$ acts on the upper half plane via *Möbius transformations*:

$$\begin{pmatrix} s & t \\ u & v \end{pmatrix} \tau = \frac{s\tau + t}{u\tau + v}.$$

This action is compatible with the action on binary quadratic forms in the sense that $\tau(\sigma p) = \sigma\tau(p)$ for all $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ and all binary quadratic forms p.

The Connection with Möbius Transformations

To the binary quadratic form $p(x, y) = ax^2 + bxy + cy^2$ with discriminant D, we assign the complex number

$$\tau(p) = \frac{b + \sqrt{D}}{2a}$$

in the upper half-plane.
We note that $\mathrm{SL}_2(\mathbb{Z})$ acts on the upper half plane via *Möbius transformations*:

$$\begin{pmatrix} s & t \\ u & v \end{pmatrix} \tau = \frac{s\tau + t}{u\tau + v}.$$

This action is compatible with the action on binary quadratic forms in the sense that $\tau(\sigma p) = \sigma\tau(p)$ for all $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ and all binary quadratic forms p.

It is well known that under this action, the orbit of every complex number in the upper half-plane contains an element in the so-called *fundamental region* $\mathcal{F}$ given by all complex numbers z in the upper half-plane such that

$$-\frac{1}{2} < \mathfrak{Re}(z) \leq \frac{1}{2} \qquad \text{and} \qquad |z| \geq 1,$$

and where we require that if $|z| = 1$ then $\mathfrak{Re}(z) \geq 0$.

It is well known that under this action, the orbit of every complex number in the upper half-plane contains an element in the so-called *fundamental region* $\mathcal{F}$ given by all complex numbers z in the upper half-plane such that

$$-\frac{1}{2} < \mathfrak{Re}(z) \leq \frac{1}{2} \qquad \text{and} \qquad |z| \geq 1,$$

and where we require that if $|z| = 1$ then $\mathfrak{Re}(z) \geq 0$.
For a number $\tau(p)$ corresponding to a positive-definite binary quadratic form $p(x, y) = ax^2 + bxy + cy^2$, we have that

$$\mathfrak{Re}(\tau) = \frac{b}{2a} \qquad |\tau|^2 = \left(\frac{b+\sqrt{D}}{2a}\right)\left(\frac{b-\sqrt{D}}{2a}\right)$$
$$= \frac{b^2 - (b^2 - 4ac)}{4a^2} = \frac{c}{a}.$$

We thus have that

$$-\frac{1}{2} < \tau \leq \frac{1}{2} \iff -\frac{1}{2} < \frac{b}{2a} \leq \frac{1}{2} \iff -a < b \leq a$$

and

$$|\tau| \geq 1 \iff |\tau|^2 \geq 1 \iff \frac{c}{a} \geq 1 \iff a \leq c.$$

We thus have that

$$-\frac{1}{2} < \tau \leq \frac{1}{2} \iff -\frac{1}{2} < \frac{b}{2a} \leq \frac{1}{2} \iff -a < b \leq a$$

and

$$|\tau| \geq 1 \iff |\tau|^2 \geq 1 \iff \frac{c}{a} \geq 1 \iff a \leq c.$$

We see that $\tau(p)$ lies in the fundamental domain $\mathcal{F}$ if and only if p is reduced!

We thus have that

$$-\frac{1}{2} < \tau \leq \frac{1}{2} \iff -\frac{1}{2} < \frac{b}{2a} \leq \frac{1}{2} \iff -a < b \leq a$$

and

$$|\tau| \geq 1 \iff |\tau|^2 \geq 1 \iff \frac{c}{a} \geq 1 \iff a \leq c.$$

We see that $\tau(p)$ lies in the fundamental domain $\mathcal{F}$ if and only if p is reduced!
The result that the orbit of every complex number in the upper half-plane contains an element in the fundamental domain thus implies our earlier result that every equivalence class of binary quadratic forms contains a reduced form.

We thus have that

$$-\frac{1}{2} < \tau \leq \frac{1}{2} \iff -\frac{1}{2} < \frac{b}{2a} \leq \frac{1}{2} \iff -a < b \leq a$$

and

$$|\tau| \geq 1 \iff |\tau|^2 \geq 1 \iff \frac{c}{a} \geq 1 \iff a \leq c.$$

We see that $\tau(p)$ lies in the fundamental domain $\mathcal{F}$ if and only if p is reduced!

The result that the orbit of every complex number in the upper half-plane contains an element in the fundamental domain thus implies our earlier result that every equivalence class of binary quadratic forms contains a reduced form.

The results are of course not equivalent since we only have a correspondence between binary quadratic forms and quadratic integers, not between binary quadratic forms and complex numbers in the upper half-plane in general.

Fractional Ideals

Definition (Fractional Ideal)

Let R be an integral domain, and let K be its field of fractions. A fractional ideal of R is an R-submodule I of K such that there exists a non-zero $r \in R$ such that $rI \subseteq I$.

Fractional Ideals

Definition (Fractional Ideal)

Let R be an integral domain, and let K be its field of fractions. A fractional ideal of R is an R-submodule I of K such that there exists a non-zero $r \in R$ such that $rI \subseteq I$.

Example

$\frac{1}{2019}\mathbb{Z}$ is a fractional ideal of $\mathbb{Z}$

Fractional Ideals

Definition (Fractional Ideal)

Let R be an integral domain, and let K be its field of fractions. A fractional ideal of R is an R-submodule I of K such that there exists a non-zero $r \in R$ such that $rI \subseteq I$.

Example

$\frac{1}{2019}\mathbb{Z}$ is a fractional ideal of $\mathbb{Z}$

Definition (Principal Fractional Ideals)

Fractional ideals of the form sR for some $s \in K$ are called *Principal Fractional Ideals*.

The Group of Fractional Ideals

Definition (Ideal Product)

Given two fractional ideals I and J, the product of these ideals is defined as

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i \,\middle|\, x_i \in I \text{ and } y_i \in J \right\}.$$

The Group of Fractional Ideals

Definition (Ideal Product)

Given two fractional ideals I and J, the product of these ideals is defined as

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i \,\middle|\, x_i \in I \text{ and } y_i \in J \right\}.$$

Definition (Invertible Ideals)

A fractional ideal I of R is said to be invertible if there exists a fractional ideal J of R such that $IJ = R$.

The Group of Fractional Ideals

Definition (Ideal Product)

Given two fractional ideals I and J, the product of these ideals is defined as

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i \;\middle|\; x_i \in I \text{ and } y_i \in J \right\}.$$

Definition (Invertible Ideals)

A fractional ideal I of R is said to be invertible if there exists a fractional ideal J of R such that $IJ = R$.

Definition (Group of Fractional Ideals)

The set of invertible fractional ideals of an integral domain R form an abelian group under multiplication.

The Class Group

Fact

An integral domain R is a Dedekind domain if and only if every non-zero fractional ideal of R is invertible.

The Class Group

Fact

An integral domain R is a Dedekind domain if and only if every non-zero fractional ideal of R is invertible.

Definition (Class Group)

The quotient of the group of fractional ideals of R by the group of principle ideals of R is called the *Class Group* of R.

The Class Group

Fact

An integral domain R is a Dedekind domain if and only if every non-zero fractional ideal of R is invertible.

Definition (Class Group)

The quotient of the group of fractional ideals of R by the group of principle ideals of R is called the *Class Group* of R.

Definition (Class Number)

The *Class Number* of a ring R is the size of its class group. In particular, we are interested in the case where R is the ring of integers of some number field K, which is always Dedekind.

The Connection with Quadratic Forms

Fact

If $\mathcal{O}_K$ is the ring of integers of some number field K, then every fractional ideal of $\mathcal{O}_K$ can be generated by 2 elements.

The Connection with Quadratic Forms

Fact

If $\mathcal{O}_K$ is the ring of integers of some number field K, then every fractional ideal of $\mathcal{O}_K$ can be generated by 2 elements.

Fact

There is a one-to-one correspondence between the equivalence classes of positive-definite binary quadratic forms with discriminant d, and the class group of the ring of integers of $\mathbb{Q}(\sqrt{d})$. The binary quadratic form $ax^2 + bxy + cy^2$ corresponds to the ideal generated by a and $\frac{b+\sqrt{d}}{2}$.

The Connection with Quadratic Forms

Fact

If $\mathcal{O}_K$ is the ring of integers of some number field K, then every fractional ideal of $\mathcal{O}_K$ can be generated by 2 elements.

Fact

There is a one-to-one correspondence between the equivalence classes of positive-definite binary quadratic forms with discriminant d, and the class group of the ring of integers of $\mathbb{Q}(\sqrt{d})$. The binary quadratic form $ax^2 + bxy + cy^2$ corresponds to the ideal generated by a and $\frac{b+\sqrt{d}}{2}$.

Fact

The number of equivalence classes of positive-definite binary quadratic forms with discriminant d is therefore equal to the size of the class group of $\mathbb{Q}(\sqrt{d})$.

Rabinowitz' Theorem

Theorem

Let A be a positive integer, and let $D = 1 - 4A$. Then the following are equivalent:

1. *The imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ has class number 1.*
2. *The polynomial $p(n) = n^2 + n + A$ is prime for all natural numbers n such that $0 \leq n \leq A - 2$.*
3. *The polynomial $p(n) = n^2 + n + A$ is prime for all natural numbers n such that*
$$0 \leq n \leq \frac{1}{2}\sqrt{\frac{-D}{3}} - \frac{1}{2}.$$
4. *The only reduced binary quadratic form with discriminant D is $x^2 + xy + Ay^2$.*

Proof

We first show that if $\mathbb{Q}(\sqrt{D})$ has class number 1, then $n^2 + n + A$ is prime for all natural numbers n such that $0 \leq n \leq A - 2$.

Proof

We first show that if $\mathbb{Q}(\sqrt{D})$ has class number 1, then $n^2 + n + A$ is prime for all natural numbers n such that $0 \leq n \leq A - 2$.
Let

$$\eta = \frac{1 + \sqrt{D}}{2}.$$

We note that $\mathbb{Z}[\eta]$, which is the ring of integers of $\mathbb{Q}(\sqrt{D})$, is a unique factorisation domain.

Proof

We first show that if $\mathbb{Q}(\sqrt{D})$ has class number 1, then $n^2 + n + A$ is prime for all natural numbers n such that $0 \leq n \leq A - 2$.
Let

$$\eta = \frac{1 + \sqrt{D}}{2}.$$

We note that $\mathbb{Z}[\eta]$, which is the ring of integers of $\mathbb{Q}(\sqrt{D})$, is a unique factorisation domain.
Consider some natural number n such that $0 \leq n \leq A - 2$, and let p be a prime number such that $p \mid n^2 + n + A$.

Proof

We first show that if $\mathbb{Q}(\sqrt{D})$ has class number 1, then $n^2 + n + A$ is prime for all natural numbers n such that $0 \leq n \leq A - 2$.
Let

$$\eta = \frac{1 + \sqrt{D}}{2}.$$

We note that $\mathbb{Z}[\eta]$, which is the ring of integers of $\mathbb{Q}(\sqrt{D})$, is a unique factorisation domain.
Consider some natural number n such that $0 \leq n \leq A - 2$, and let p be a prime number such that $p \mid n^2 + n + A$.
We thus have that p divides $(n + \eta)(n + \bar{\eta})$. However, neither factor is divisible by p, and so p is not a prime in $\mathbb{Z}[\eta]$.

Proof

It follows that there exists α, β in $\mathbb{Z}[\eta]$, neither of which are units, such that $\alpha\beta = p$.

Proof

It follows that there exists α, β in $\mathbb{Z}[\eta]$, neither of which are units, such that $\alpha\beta = p$.
We see that $p^2 = N(p) = N(\alpha)N(\beta)$, where N denotes the norm in $\mathbb{Z}[\eta]$.

Proof

It follows that there exists α, β in $\mathbb{Z}[\eta]$, neither of which are units, such that $\alpha\beta = p$.
We see that $p^2 = N(p) = N(\alpha)N(\beta)$, where N denotes the norm in $\mathbb{Z}[\eta]$.
Since α and β are not units, we have that their norms are not equal to 1, and so we have that $N(\alpha) = N(\beta) = p$.

Proof

It follows that there exists α, β in $\mathbb{Z}[\eta]$, neither of which are units, such that $\alpha\beta = p$.
We see that $p^2 = N(p) = N(\alpha)N(\beta)$, where N denotes the norm in $\mathbb{Z}[\eta]$.
Since α and β are not units, we have that their norms are not equal to 1, and so we have that $N(\alpha) = N(\beta) = p$.
Let $\alpha = s + t \cdot \eta$ for some integers s and t. Then

$$p = N(\alpha) = s^2 + st + At^2 = \left(s + \frac{t}{2}\right)^2 + \left(A - \frac{1}{4}\right) t^2 \geq A - \frac{1}{4}.$$

Proof

It follows that there exists α, β in $\mathbb{Z}[\eta]$, neither of which are units, such that $\alpha\beta = p$.
We see that $p^2 = N(p) = N(\alpha)N(\beta)$, where N denotes the norm in $\mathbb{Z}[\eta]$.
Since α and β are not units, we have that their norms are not equal to 1, and so we have that $N(\alpha) = N(\beta) = p$.
Let $\alpha = s + t \cdot \eta$ for some integers s and t. Then

$$p = N(\alpha) = s^2 + st + At^2 = \left(s + \frac{t}{2}\right)^2 + \left(A - \frac{1}{4}\right) t^2 \geq A - \frac{1}{4}.$$

Since p is an integer, this implies that $p \geq A$.

Proof

We now note that since $0 \leq n \leq A - 2$, we have that

$$n^2 + n + A < (A-1)^2 + (A-1) + A = A^2.$$

Proof

We now note that since $0 \leq n \leq A - 2$, we have that

$$n^2 + n + A < (A-1)^2 + (A-1) + A = A^2.$$

Recall that p was an arbitrary prime factor of $n^2 + n + A$, and was shown to be greater than or equal to A.

Proof

We now note that since $0 \leq n \leq A-2$, we have that

$$n^2+n+A < (A-1)^2+(A-1)+A = A^2.$$

Recall that p was an arbitrary prime factor of n^2+n+A, and was shown to be greater than or equal to A.
It follows that every prime factor of n^2+n+A is larger than the square-root of n^2+n+A, and so n^2+n+A is prime.

It is clear that if $n^2 + n + A$ is prime for all n such that $0 \leq n \leq A - 2$, then this is also true for all n is the smaller range

$$0 \leq n \leq \frac{1}{2}\sqrt{\frac{-D}{3}} - \frac{1}{2}.$$

It is clear that if $n^2 + n + A$ is prime for all n such that $0 \leq n \leq A - 2$, then this is also true for all n is the smaller range

$$0 \leq n \leq \frac{1}{2}\sqrt{\frac{-D}{3}} - \frac{1}{2}.$$

We also recall that there is a bijection between classes of binary quadratic forms with discriminant D, and ideal classes in the imaginary quadratic field $\mathbb{Q}(\sqrt{D})$.

It is clear that if $n^2 + n + A$ is prime for all n such that $0 \leq n \leq A - 2$, then this is also true for all n is the smaller range

$$0 \leq n \leq \frac{1}{2}\sqrt{\frac{-D}{3}} - \frac{1}{2}.$$

We also recall that there is a bijection between classes of binary quadratic forms with discriminant D, and ideal classes in the imaginary quadratic field $\mathbb{Q}(\sqrt{D})$.
Thus the only thing that remains to be proved in Rabinowitz' Theorem is that if $n^2 + n + A$ is prime for all n such that

$$0 \leq n \leq \frac{1}{2}\sqrt{\frac{-D}{3}} - \frac{1}{2},$$

then the only reduced binary quadratic form with discriminant D is $x^2 + xy + Ay^2$.

Proof

Suppose that $ax^2 + bxy + cy^2$ is a reduced binary quadratic form such that $b^2 - 4ac = D$.

Proof

Suppose that $ax^2 + bxy + cy^2$ is a reduced binary quadratic form such that $b^2 - 4ac = D$.
Since D is odd, this implies that b is odd. Let $b = 2n + 1$. Then we have that

$$1 - 4A = D = b^2 - 4ac = 4n^2 + 4n + 1 - 4ac,$$

and so

$$ac = n^2 + n + A.$$

Proof

Suppose that $ax^2 + bxy + cy^2$ is a reduced binary quadratic form such that $b^2 - 4ac = D$.

Since D is odd, this implies that b is odd. Let $b = 2n + 1$. Then we have that

$$1 - 4A = D = b^2 - 4ac = 4n^2 + 4n + 1 - 4ac,$$

and so

$$ac = n^2 + n + A.$$

We note that since $b \leq a \leq c$,

$$-D = 4ac - b^2 \geq 4b^2 - b^2 = 3b^2$$

and so

$$2n + 1 = b \leq \sqrt{\frac{-D}{3}}.$$

Proof

By assumption, this implies that $ac = n^2 + n + A$ is prime.

Proof

By assumption, this implies that $ac = n^2 + n + A$ is prime.
Since $a \leq c$, this implies that $a = 1$.

Proof

By assumption, this implies that $ac = n^2 + n + A$ is prime.
Since $a \leq c$, this implies that $a = 1$.
Since $-a < b \leq a$, this implies that $b \in \{0, 1\}$. We recall that b is odd, and so $b = 1$.

Proof

By assumption, this implies that $ac = n^2 + n + A$ is prime.
Since $a \leq c$, this implies that $a = 1$.
Since $-a < b \leq a$, this implies that $b \in \{0, 1\}$. We recall that b is odd, and so $b = 1$.
Finally, we have that

$$1 - 4A = D = b^2 - 4ac = 1 - 4c,$$

and so $c = A$.

$\square$

Some of the Ingredients

I will now provide a rough overview of Baker's method of solving the Class Number 1 problem. We leave out the technical details, but will pay attention to some of the concepts that go into the proof. The proof relies on Dirichlet L-series for the Kronecker symbol, some Fourier analysis, and a bound on linear forms in logarithms. We will look at these in varying levels of detail.

Dirichlet Characters

Definition (Dirichlet Characters)

A *Dirichlet character modulo n* is a group homomorphism

$$\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$$

from the multiplicative group of integers modulo n which are relatively prime to n to the multiplicative group of non-zero complex numbers.

Remark

A Dirichlet character modulo n given by χ can be extended to a function from $\mathbb{Z}$ to $\mathbb{C}$ by setting

$$\chi(m) = \chi(m \bmod n)$$

if m is relatively prime to n, and letting $\chi(m) = 0$ otherwise.

The Kronecker Symbol

Definition (Legendre Symbol)

For a prime p, the *Legendre symbol* $\left(\frac{n}{p}\right)$ is a Dirichlet character modulo p given by

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \text{ is a square modulo } p \\ -1 & \text{otherwise.} \end{cases}$$

The Kronecker Symbol

Definition (Legendre Symbol)

For a prime p, the *Legendre symbol* $\left(\frac{n}{p}\right)$ is a Dirichlet character modulo p given by

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{if } n \text{ is a square modulo } p \\ -1 & \text{otherwise.} \end{cases}$$

Not Quite a Definition (Kronecker Symbol)

The *Kronecker symbol* $\left(\frac{n}{m}\right)$ is a Dirichlet character modulo both m and n. It is an extension of the Legendre symbol to arbitrary integers m and is defined essentially as the product of the Legendre symbols corresponding to the prime factors of m, but with some technicalities that I don't want to discuss.

Dirichlet L-series

Definition (L-series)

For a function $\chi : \mathbb{N} \to \mathbb{C}$, the *Dirichlet L-series* associated to χ is defined by

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

wherever this series converges.

Fact

If χ is a Dirichlet character (or more generally, any function that only takes values on the unit circle), then the series defining $L(\chi, s)$ converges absolutely on the right half-plane $\mathfrak{Re}(s) > 1$, and defines an analytic function there.

Some L-series formulae

Fact

Let k and d be relatively prime positive integers, and let $\chi(n) = \left(\frac{k}{n}\right)$ and $\chi'(n) = \left(\frac{-d}{n}\right)$ be the corresponding Kronecker symbols. Then for all $s \in \mathbb{C}$ with $\mathfrak{Re}(s) > 1$, we have that

$$L(\chi, s)L(\chi\chi', s) = \frac{1}{2}\sum_{f}\sum_{(x,y)\neq(0,0)} \chi(f(x,y))f(x,y)^{-s}$$

where f ranges over representatives of the equivalence classes of binary quadratic forms with discriminant $-d$.

Some L-series formulae

Fact (Dirichlet's Class Number Formula)

Let d be a positive integer, and let h be the class number of $\mathbb{Q}(\sqrt{-d})$. Let w be the number of roots of unity in $\mathbb{Q}(\sqrt{-d})$, and let $\chi(n) = \left(\frac{-d}{n}\right)$ be a Kronecker symbol. Then we have that

$$L(\chi, 1) = \frac{2\pi h}{w\sqrt{d}}.$$

Some L-series formulae

Fact (Dirichlet's Other Class Number Formula)

Let d be a positive integer, let h be the class number of $\mathbb{Q}(\sqrt{d})$, let $\chi(n) = \left(\frac{d}{n}\right)$ be a Kronecker symbol, and let ϵ be the fundamental unit in $\mathbb{Q}(\sqrt{d})$. Then we have that

$$L(\chi, 1) = \frac{h \log \epsilon}{\sqrt{d}}.$$

Obtaining a Bound on the Discriminant

- We start with the formula

$$L(\chi, s)L(\chi\chi', s) = \frac{1}{2}\sum_{f}\sum_{(x,y)\neq(0,0)} \chi(f(x,y))f(x,y)^{-s}.$$

Obtaining a Bound on the Discriminant

- We start with the formula

$$L(\chi, s)L(\chi\chi', s) = \frac{1}{2}\sum_{f}\sum_{(x,y)\neq(0,0)} \chi(f(x,y))f(x,y)^{-s}.$$

- We split off the terms of the sum corresponding to $y = 0$. It turns out that this is equal to

$$\frac{\pi^2}{6}\prod_{p|k}\left(1 - \frac{1}{p^2}\right)\sum_{f}\frac{\chi(f(1,0))}{f(1,0)^{-s}}.$$

Obtaining a Bound on the Discriminant

- We start with the formula

$$L(\chi, s)L(\chi\chi', s) = \frac{1}{2}\sum_{f}\sum_{(x,y)\neq(0,0)} \chi(f(x,y))f(x,y)^{-s}.$$

- We split off the terms of the sum corresponding to $y = 0$. It turns out that this is equal to

$$\frac{\pi^2}{6}\prod_{p|k}\left(1-\frac{1}{p^2}\right)\sum_{f}\frac{\chi(f(1,0))}{f(1,0)^{-s}}.$$

- In particular, note that if $\mathbb{Q}(\sqrt{-d})$ has class number 1, then the only f which appears in this sum is $f(x,y) = x^2 + xy + \frac{1-d}{4}y^2$, and so the sum is equal to 1.

Here be Dragons

- We express the remaining sum over non-zero y in a Fourier series

$$\sum_{f} \sum_{x,y\in\mathbb{Z},y\neq 0} \chi(f(x,y))f(x,y)^{-s} = \sum_{f} \sum_{r=-\infty}^{\infty} A_{r,f}(s) \exp\left\{\frac{2\pi i r b_f}{2a_f k}\right\}$$

where $f(x,y) = a_f x^2 + b_f xy + c_f y^2$.

Here be Dragons

- We express the remaining sum over non-zero y in a Fourier series

$$\sum_{f} \sum_{x,y\in\mathbb{Z},y\neq 0} \chi(f(x,y))f(x,y)^{-s} = \sum_{f} \sum_{r=-\infty}^{\infty} A_{r,f}(s) \exp\left\{\frac{2\pi i r b_f}{2a_f k}\right\}$$

  where $f(x,y) = a_f x^2 + b_f xy + c_f y^2$.
- We use some dark magic/very scary analysis to obtain bounds on the Fourier coefficients as $s \to 1$.

Here be Dragons

- We express the remaining sum over non-zero y in a Fourier series

$$\sum_{f} \sum_{x,y\in\mathbb{Z},y\neq 0} \chi(f(x,y))f(x,y)^{-s} = \sum_{f} \sum_{r=-\infty}^{\infty} A_{r,f}(s) \exp\left\{\frac{2\pi i r b_f}{2a_f k}\right\}$$

where $f(x,y) = a_f x^2 + b_f xy + c_f y^2$.

- We use some dark magic/very scary analysis to obtain bounds on the Fourier coefficients as $s \to 1$.
- In particular, we find that

$$|A_{r,f}(1)| \leq \frac{2\pi}{\sqrt{d}} |r| e^{-\pi|r|\sqrt{d}/(ka_f)},$$

and

$$A_{0,f}(1) = -\frac{2\pi}{k\sqrt{d}} \chi(a_f) \log p$$

if k is a power of the prime p, and 0 otherwise.

Nearly There

- We assume that $\mathbb{Q}(\sqrt{-d})$ has class number 1, and apply the above results with this value of d, and for $k = 21$, and $k = 33$.

Nearly There

- We assume that $\mathbb{Q}(\sqrt{-d})$ has class number 1, and apply the above results with this value of d, and for $k = 21$, and $k = 33$.
- Since $\mathbb{Q}(\sqrt{-d})$ has class number 1, there is only 1 equivalence class of binary quadratic forms with discriminant $-d$.

Nearly There

- We assume that $\mathbb{Q}(\sqrt{-d})$ has class number 1, and apply the above results with this value of d, and for $k = 21$, and $k = 33$.
- Since $\mathbb{Q}(\sqrt{-d})$ has class number 1, there is only 1 equivalence class of binary quadratic forms with discriminant $-d$.
- Since each value of k which we consider is not a prime power, we have that $A_{0,f}(1) = 0$ in each case.

Nearly There

- We assume that $\mathbb{Q}(\sqrt{-d})$ has class number 1, and apply the above results with this value of d, and for $k = 21$, and $k = 33$.
- Since $\mathbb{Q}(\sqrt{-d})$ has class number 1, there is only 1 equivalence class of binary quadratic forms with discriminant $-d$.
- Since each value of k which we consider is not a prime power, we have that $A_{0,f}(1) = 0$ in each case.
- We find that

$$\left| \sum_{f} \sum_{r=-\infty}^{\infty} A_{r,f}(1) \exp\left\{ \frac{2\pi i r b_f}{2a_f k} \right\} \right| \leq \sum_{r=-\infty}^{\infty} |A_{r,f}(1)|.$$

Nearly There

- We assume that $\mathbb{Q}(\sqrt{-d})$ has class number 1, and apply the above results with this value of d, and for $k = 21$, and $k = 33$.
- Since $\mathbb{Q}(\sqrt{-d})$ has class number 1, there is only 1 equivalence class of binary quadratic forms with discriminant $-d$.
- Since each value of k which we consider is not a prime power, we have that $A_{0,f}(1) = 0$ in each case.
- We find that

$$\left| \sum_f \sum_{r=-\infty}^{\infty} A_{r,f}(1) \exp\left\{ \frac{2\pi i r b_f}{2a_f k} \right\} \right| \leq \sum_{r=-\infty}^{\infty} |A_{r,f}(1)|.$$

- Using the bound for $|A_{r,f}(1)|$ from earlier, it is then possible to derive that this is bounded above by

$$\frac{16\pi e^{-\pi\sqrt{d}/k}}{\sqrt{d}}.$$

Nearly There

- We assume that $\mathbb{Q}(\sqrt{-d})$ has class number 1, and apply the above results with this value of d, and for $k = 21$, and $k = 33$.
- Since $\mathbb{Q}(\sqrt{-d})$ has class number 1, there is only 1 equivalence class of binary quadratic forms with discriminant $-d$.
- Since each value of k which we consider is not a prime power, we have that $A_{0,f}(1) = 0$ in each case.
- We find that

$$\left| \sum_{f} \sum_{r=-\infty}^{\infty} A_{r,f}(1) \exp\left\{ \frac{2\pi i r b_f}{2a_f k} \right\} \right| \leq \sum_{r=-\infty}^{\infty} |A_{r,f}(1)|.$$

- Using the bound for $|A_{r,f}(1)|$ from earlier, it is then possible to derive that this is bounded above by

$$\frac{16\pi e^{-\pi\sqrt{d}/k}}{\sqrt{d}}.$$

Hopefully I Had Enough Sense to Skip Some of the Slides

- Noting that $\mathbb{Q}(\sqrt{k})$ has class number 1 for $k \in \{21, 33\}$, Dirichlet's Class Number Formula tells us that

$$L(\chi, 1)L(\chi\chi', 1) = \frac{2\pi h_k \log \epsilon_k}{k\sqrt{d}}$$

where h_k is the class number of $\mathbb{Q}(\sqrt{-kd})$, and ϵ_k is the fundamental unit in $\mathbb{Q}(\sqrt{k})$.

Last Boring Slide (In This Stretch) Hopefully

- For $k = 21$, we derive that

$$\frac{2\pi h_{21} \log \epsilon_{21}}{21\sqrt{d}} = \frac{\pi^2}{6} \prod_{p|21} \left(1 - \frac{1}{p^2}\right) + \sum_{r=-\infty}^{\infty} A_{r,f}(1) e^{\pi i r/k},$$

and so

$$\left| \frac{64\pi^2}{441} - \frac{2\pi h_{21} \log \epsilon_{21}}{21\sqrt{d}} \right| < \frac{16\pi e^{-\pi\sqrt{d}/21}}{\sqrt{d}}.$$

Last Boring Slide (In This Stretch) Hopefully

- For $k = 21$, we derive that

$$\frac{2\pi h_{21} \log \epsilon_{21}}{21\sqrt{d}} = \frac{\pi^2}{6} \prod_{p|21} \left(1 - \frac{1}{p^2}\right) + \sum_{r=-\infty}^{\infty} A_{r,f}(1) e^{\pi i r/k},$$

and so

$$\left| \frac{64\pi^2}{441} - \frac{2\pi h_{21} \log \epsilon_{21}}{21\sqrt{d}} \right| < \frac{16\pi e^{-\pi\sqrt{d}/21}}{\sqrt{d}}.$$

- This simplifies to

$$\left| h_{21} \log \epsilon_{21} - \frac{32}{21}\pi\sqrt{d} \right| < 168 e^{-\pi\sqrt{d}/21}.$$

Alas

- We can obtain a similar bound for $k = 33$. With some manipulation, these bounds can be combined to obtain

$$|35h_{21}\log\epsilon_{21} - 22h_{33}\log\epsilon_{33}| < e^{-C\pi\sqrt{d}}$$

for some constant $C < \frac{1}{33}$, and for all large enough d where "large enough" depends on how close to $\frac{1}{33}$ we choose C to be.

Alas

- We can obtain a similar bound for $k = 33$. With some manipulation, these bounds can be combined to obtain

$$|35h_{21}\log\epsilon_{21} - 22h_{33}\log\epsilon_{33}| < e^{-C\pi\sqrt{d}}$$

  for some constant $C < \frac{1}{33}$, and for all large enough d where "large enough" depends on how close to $\frac{1}{33}$ we choose C to be.
- The quantity $35h_{21}\log\epsilon_{21} - 22h_{33}\log\epsilon_{33}$ is a *linear form in logarithms*, and there are known results for how close such a thing can be to 0 without being equal to 0.

Alas

- We can obtain a similar bound for $k = 33$. With some manipulation, these bounds can be combined to obtain

$$|35h_{21}\log\epsilon_{21} - 22h_{33}\log\epsilon_{33}| < e^{-C\pi\sqrt{d}}$$

  for some constant $C < \frac{1}{33}$, and for all large enough d where "large enough" depends on how close to $\frac{1}{33}$ we choose C to be.
- The quantity $35h_{21}\log\epsilon_{21} - 22h_{33}\log\epsilon_{33}$ is a *linear form in logarithms*, and there are known results for how close such a thing can be to 0 without being equal to 0.
- Baker used such a bound to obtain that $d < 10^{500}$.

Alas

- We can obtain a similar bound for $k = 33$. With some manipulation, these bounds can be combined to obtain

$$|35h_{21}\log\epsilon_{21} - 22h_{33}\log\epsilon_{33}| < e^{-C\pi\sqrt{d}}$$

  for some constant $C < \frac{1}{33}$, and for all large enough d where "large enough" depends on how close to $\frac{1}{33}$ we choose C to be.
- The quantity $35h_{21}\log\epsilon_{21} - 22h_{33}\log\epsilon_{33}$ is a *linear form in logarithms*, and there are known results for how close such a thing can be to 0 without being equal to 0.
- Baker used such a bound to obtain that $d < 10^{500}$.
- A more modern bound, assuming that I applied it correctly, allows one to obtain $d < 2 \times 10^{15}$.

Testing the Remaining Possibilities

Baker notes that Stark had shown in 1966 that if $d > 10^4$ and $\mathbb{Q}(\sqrt{-d})$ has class number 1, then d must satisfy $d > e^{10^7}$.

Testing the Remaining Possibilities

Baker notes that Stark had shown in 1966 that if $d > 10^4$ and $\mathbb{Q}(\sqrt{-d})$ has class number 1, then d must satisfy $d > e^{10^7}$.
It is possible to show that $e^{10^7} > 10^{500} > 2 \times 10^{15}$, so we need not check the remaining possible values of d: we can instead follow Baker's lead and appeal to Stark's result.

Testing the Remaining Possibilities

Baker notes that Stark had shown in 1966 that if $d > 10^4$ and $\mathbb{Q}(\sqrt{-d})$ has class number 1, then d must satisfy $d > e^{10^7}$.
It is possible to show that $e^{10^7} > 10^{500} > 2 \times 10^{15}$, so we need not check the remaining possible values of d: we can instead follow Baker's lead and appeal to Stark's result.
But that's no fun!

Some Facts About Computers

An average modern consumer computing device, such as the laptop that these slides were created on, can perform on the order of 10^9 to 10^{10} basic calculations per CPU core per second.

Some Facts About Computers

An average modern consumer computing device, such as the laptop that these slides were created on, can perform on the order of 10^9 to 10^{10} basic calculations per CPU core per second.

Actually, this depends very much on what one considers a basic operation, and on a variety of factors such as whether the required data is in cache or needs to be fetched from memory, how much branching the processor needs to do and how effective the branch predictor is at mitigating this effect, and other architectural concerns.

Some Facts About Computers

An average modern consumer computing device, such as the laptop that these slides were created on, can perform on the order of 10^9 to 10^{10} basic calculations per CPU core per second.

Actually, this depends very much on what one considers a basic operation, and on a variety of factors such as whether the required data is in cache or needs to be fetched from memory, how much branching the processor needs to do and how effective the branch predictor is at mitigating this effect, and other architectural concerns.

Nevertheless, let us assume that this laptop can perform 10^{10} to 10^{11} operations per second, which equates to 10^{15} to 10^{16} operations per day.

Some Facts About Computers

An average modern consumer computing device, such as the laptop that these slides were created on, can perform on the order of 10^9 to 10^{10} basic calculations per CPU core per second.

Actually, this depends very much on what one considers a basic operation, and on a variety of factors such as whether the required data is in cache or needs to be fetched from memory, how much branching the processor needs to do and how effective the branch predictor is at mitigating this effect, and other architectural concerns.

Nevertheless, let us assume that this laptop can perform 10^{10} to 10^{11} operations per second, which equates to 10^{15} to 10^{16} operations per day.

This, coincidentally, is approximately the upper bound for the absolute values for the discriminants d that we obtained above.

Some Facts About Computers

An average modern consumer computing device, such as the laptop that these slides were created on, can perform on the order of 10^9 to 10^{10} basic calculations per CPU core per second.

Actually, this depends very much on what one considers a basic operation, and on a variety of factors such as whether the required data is in cache or needs to be fetched from memory, how much branching the processor needs to do and how effective the branch predictor is at mitigating this effect, and other architectural concerns.

Nevertheless, let us assume that this laptop can perform 10^{10} to 10^{11} operations per second, which equates to 10^{15} to 10^{16} operations per day.

This, coincidentally, is approximately the upper bound for the absolute values for the discriminants d that we obtained above.

Unfortunately, the x86 instruction set does not include an instruction for calculating class numbers.

How Not To Test the Remaining Possibilities

We recall that the class number for the discriminant $-d$ is the number of reduced positive-definite binary quadratic forms with discriminant $-d$.

How Not To Test the Remaining Possibilities

We recall that the class number for the discriminant $-d$ is the number of reduced positive-definite binary quadratic forms with discriminant $-d$. We thus wish to find all solutions (a, b, c) to the equation $b^2 - 4ac = -d$ satisfying $-a < b \leq a \leq c$, or $0 < b \leq a = c$.

How Not To Test the Remaining Possibilities

We recall that the class number for the discriminant $-d$ is the number of reduced positive-definite binary quadratic forms with discriminant $-d$.

We thus wish to find all solutions (a, b, c) to the equation $b^2 - 4ac = -d$ satisfying $-a < b \leq a \leq c$, or $0 < b \leq a = c$.

We could loop through values of b, and for each b factorise $d + b^2$ to find possibilities for a and c. This requires us to factorise $O(\sqrt{d})$ numbers for each d, and so requires $O(n^{3/2})$ factorisations to test every d below n.

Factorising 10^{22} integers is infeasible even if we could factorise 10^{16} integers per day. Notably, the x86 instruction set also doesn't include an instruction to factorise integers.

How Not To Test the Remaining Possibilities

We recall that the class number for the discriminant $-d$ is the number of reduced positive-definite binary quadratic forms with discriminant $-d$.
We thus wish to find all solutions (a, b, c) to the equation $b^2 - 4ac = -d$ satisfying $-a < b \leq a \leq c$, or $0 < b \leq a = c$.
We could loop through values of b, and for each b factorise $d + b^2$ to find possibilities for a and c. This requires us to factorise $O(\sqrt{d})$ numbers for each d, and so requires $O(n^{3/2})$ factorisations to test every d below n.
Factorising 10^{22} integers is infeasible even if we could factorise 10^{16} integers per day. Notably, the x86 instruction set also doesn't include an instruction to factorise integers.

How Not To Test the Remaining Possibilities

Of course we don't really need to test every possible value of d since we know that d must be prime, but to exploit this we would need a way to only test prime values of d. First checking if d is prime would then require us to do 10^{15} primality tests, and then still test the remaining 3×10^{13} numbers that remain.

How Not To Test the Remaining Possibilities

Of course we don't really need to test every possible value of d since we know that d must be prime, but to exploit this we would need a way to only test prime values of d. First checking if d is prime would then require us to do 10^{15} primality tests, and then still test the remaining 3×10^{13} numbers that remain.

The Sieve of Eratosthenes is quite efficient for finding all prime numbers below a given bound, but requires us to maintain a list of all of the numbers below that given bound, and storing a flag for each of 10^{15} natural numbers takes hopelessly too much memory.

How Not To Test the Remaining Possibilities

Of course we don't really need to test every possible value of d since we know that d must be prime, but to exploit this we would need a way to only test prime values of d. First checking if d is prime would then require us to do 10^{15} primality tests, and then still test the remaining 3×10^{13} numbers that remain.

The Sieve of Eratosthenes is quite efficient for finding all prime numbers below a given bound, but requires us to maintain a list of all of the numbers below that given bound, and storing a flag for each of 10^{15} natural numbers takes hopelessly too much memory.

We could instead loop through the $O(\sqrt{d})$ possible values for a, and for each of these loop through either the $O(a)$ possible values of b (in which case we test if $d + b^2$ is divisible by $4a$), or the $O(d/a)$ possible values of c (in which case we test if $4ac - d$ is a square), but this still requires us to process at least $\sqrt{d}$ numbers for each d, and so remains infeasible.

A Slightly Better Idea?

We don't actually need to know what the class number for the discriminant d is, we just need to know whether it is equal to 1.

A Slightly Better Idea?

We don't actually need to know what the class number for the discriminant d is, we just need to know whether it is equal to 1.
Using Rabinowitz' Theorem, we could test whether $m^2 + m + \frac{d+1}{4}$ is prime for all m in the range $0 \leq m \leq \sqrt{d/12}$.

A Slightly Better Idea?

We don't actually need to know what the class number for the discriminant d is, we just need to know whether it is equal to 1.

Using Rabinowitz' Theorem, we could test whether $m^2 + m + \frac{d+1}{4}$ is prime for all m in the range $0 \leq m \leq \sqrt{d/12}$.

This doesn't seem to gain us anything since it still requires us to do $O(\sqrt{d})$ primality tests for each d, and we already decided that this many operations per value of d is infeasible.

A Slightly Better Idea?

We don't actually need to know what the class number for the discriminant d is, we just need to know whether it is equal to 1.

Using Rabinowitz' Theorem, we could test whether $m^2 + m + \frac{d+1}{4}$ is prime for all m in the range $0 \leq m \leq \sqrt{d/12}$.

This doesn't seem to gain us anything since it still requires us to do $O(\sqrt{d})$ primality tests for each d, and we already decided that this many operations per value of d is infeasible.

I decided to go with this approach anyway. It is significantly faster than any of the previous approaches mentioned, and in the majority of cases we can stop after 1 or 2 primality checks.

Another Improvement

Primality tests are quite slow if we wish to use a deterministic primality test.

Another Improvement

Primality tests are quite slow if we wish to use a deterministic primality test.
Can we get away with using a probabilistic method to gain speed at the cost of accuracy?

Another Improvement

Primality tests are quite slow if we wish to use a deterministic primality test.

Can we get away with using a probabilistic method to gain speed at the cost of accuracy?

As long as the method we use doesn't give any false negatives (i.e. reports that a number is not prime when it actually is), we could use the probabilistic method as a fast pass over all of the numbers, and then use a deterministic test on the numbers it identifies to check whether they are true or false positives.

Another Improvement

Primality tests are quite slow if we wish to use a deterministic primality test.

Can we get away with using a probabilistic method to gain speed at the cost of accuracy?

As long as the method we use doesn't give any false negatives (i.e. reports that a number is not prime when it actually is), we could use the probabilistic method as a fast pass over all of the numbers, and then use a deterministic test on the numbers it identifies to check whether they are true or false positives.

This is a significant improvement as long as the number of false positives is quite small. There are a number of probabilistic primality tests that we can use, such as the Fermat primality test.

Another Improvement

Primality tests are quite slow if we wish to use a deterministic primality test.

Can we get away with using a probabilistic method to gain speed at the cost of accuracy?

As long as the method we use doesn't give any false negatives (i.e. reports that a number is not prime when it actually is), we could use the probabilistic method as a fast pass over all of the numbers, and then use a deterministic test on the numbers it identifies to check whether they are true or false positives.

This is a significant improvement as long as the number of false positives is quite small. There are a number of probabilistic primality tests that we can use, such as the Fermat primality test.

We could even just test whether the number is divisible by any prime in some small fixed list of primes, but it's probably too much to hope for that this would only have a small number of false positives.

Another Improvement

Primality tests are quite slow if we wish to use a deterministic primality test.

Can we get away with using a probabilistic method to gain speed at the cost of accuracy?

As long as the method we use doesn't give any false negatives (i.e. reports that a number is not prime when it actually is), we could use the probabilistic method as a fast pass over all of the numbers, and then use a deterministic test on the numbers it identifies to check whether they are true or false positives.

This is a significant improvement as long as the number of false positives is quite small. There are a number of probabilistic primality tests that we can use, such as the Fermat primality test.

We could even just test whether the number is divisible by any prime in some small fixed list of primes, but it's probably too much to hope for that this would only have a small number of false positives.

Or is it?

Embracing Wishful Thinking

For each (small) prime p, we require that $n^2 + n + d$ is not divisible by p.

Embracing Wishful Thinking

For each (small) prime p, we require that $n^2 + n + d$ is not divisible by p. The expression $n^2 + n$ takes exactly $\frac{p+1}{2}$ values for an odd prime p, and so there are precisely $\frac{p-1}{2}$ allowable remainders for d modulo p.

Embracing Wishful Thinking

For each (small) prime p, we require that $n^2 + n + d$ is not divisible by p.
The expression $n^2 + n$ takes exactly $\frac{p+1}{2}$ values for an odd prime p, and so there are precisely $\frac{p-1}{2}$ allowable remainders for d modulo p.
Heuristically, each additional small prime p that we include in the test approximately halves the number of possible values for d.

Embracing Wishful Thinking

For each (small) prime p, we require that $n^2 + n + d$ is not divisible by p.

The expression $n^2 + n$ takes exactly $\frac{p+1}{2}$ values for an odd prime p, and so there are precisely $\frac{p-1}{2}$ allowable remainders for d modulo p.

Heuristically, each additional small prime p that we include in the test approximately halves the number of possible values for d.

Since $2^{50} \approx 10^{15}$, we expect a very small number of false positives if we use the first 50 small primes.

Embracing Wishful Thinking

For each (small) prime p, we require that $n^2 + n + d$ is not divisible by p.
The expression $n^2 + n$ takes exactly $\frac{p+1}{2}$ values for an odd prime p, and so there are precisely $\frac{p-1}{2}$ allowable remainders for d modulo p.
Heuristically, each additional small prime p that we include in the test approximately halves the number of possible values for d.
Since $2^{50} \approx 10^{15}$, we expect a very small number of false positives if we use the first 50 small primes.
As an implementation note, we do not actually loop through n and test whether $n^2 + n + d$ is divisible by p. Instead, we precompute the allowable remainders modulo p, store them in a lookup table, and then check whether the remainder of d modulo p is allowable.

A Final Optimisation

We still have the problem that we are doing this for 10^{15} values of d. Fortunately for each d we are only doing 50 computations, but we would still expect this calculation to take a couple of months.

A Final Optimisation

We still have the problem that we are doing this for 10^{15} values of d.
Fortunately for each d we are only doing 50 computations, but we would still expect this calculation to take a couple of months.
We really need a way to only test those d that are likely to work, for example by somehow only looping through the prime values of d.

A Final Optimisation

We still have the problem that we are doing this for 10^{15} values of d. Fortunately for each d we are only doing 50 computations, but we would still expect this calculation to take a couple of months.
We really need a way to only test those d that are likely to work, for example by somehow only looping through the prime values of d.
One possible avenue for optimisation is to notice that since d must be a twin prime, and so $d \equiv 5 \pmod 6$. We can thus start with $d = 5$, and add 6 to d on each iteration. This divides our search space by 6.

A Final Optimisation

We still have the problem that we are doing this for 10^{15} values of d. Fortunately for each d we are only doing 50 computations, but we would still expect this calculation to take a couple of months.

We really need a way to only test those d that are likely to work, for example by somehow only looping through the prime values of d.

One possible avenue for optimisation is to notice that since d must be a twin prime, and so $d \equiv 5 \pmod 6$. We can thus start with $d = 5$, and add 6 to d on each iteration. This divides our search space by 6.

We can take this idea even further. For each of the first 11 primes, we loop over the allowable remainders modulo that prime, and use the Chinese Remainder Theorem Algorithm to generate a value of d that has an allowable remainder modulo each of these primes.

A Final Optimisation

We still have the problem that we are doing this for 10^{15} values of d. Fortunately for each d we are only doing 50 computations, but we would still expect this calculation to take a couple of months.

We really need a way to only test those d that are likely to work, for example by somehow only looping through the prime values of d.

One possible avenue for optimisation is to notice that since d must be a twin prime, and so $d \equiv 5 \pmod 6$. We can thus start with $d = 5$, and add 6 to d on each iteration. This divides our search space by 6.

We can take this idea even further. For each of the first 11 primes, we loop over the allowable remainders modulo that prime, and use the Chinese Remainder Theorem Algorithm to generate a value of d that has an allowable remainder modulo each of these primes.

On the computer that I hired from Amazon Cloud Services, this approach took a little over 1 minute to run. On my current laptop, it takes around half an hour.