The 290 Theorem

Dan Fretwell

SoMaS postgrad seminar
26th October 2014

Outline of talk

Lagrange's four square Theorem

Every positive integer is a sum of four square numbers.

$$7 = 1^2 + 1^2 + 1^2 + 2^2$$
$$1831 = 2^2 + 3^2 + 27^2 + 33^2$$
$$231287 = 1^2 + 3^2 + 306^2 + 371^2$$

A quadratic form over a ring R is a polynomial $Q(x_1, x_2, ..., x_n) \in R[x_1, x_2, ..., x_n]$ of the form:

$$Q(x_1, x_2, ..., x_n) = \sum_{1 \leq i,j \leq n} a_{i,j} x_i x_j.$$

If $R \subseteq \mathbb{R}$ we say that Q is positive definite if $Q(\alpha_1, \alpha_2, ..., \alpha_n) > 0$ whenever $\alpha_1, \alpha_2, ..., \alpha_n \in R \backslash \{0\}$.

For example:

$$x^2 + y^2 + z^2 + w^2$$

$$x^2 - 4xy + 6y^2 = (x - 2y)^2 + 2y^2$$

are positive definite quadratic forms over $\mathbb{Z}$.

A quadratic form over a ring R is a polynomial $Q(x_1, x_2, ..., x_n) \in R[x_1, x_2, ..., x_n]$ of the form:

$$Q(x_1, x_2, ..., x_n) = \sum_{1 \leq i,j \leq n} a_{i,j} x_i x_j.$$

If $R \subseteq \mathbb{R}$ we say that Q is positive definite if $Q(\alpha_1, \alpha_2, ..., \alpha_n) > 0$ whenever $\alpha_1, \alpha_2, ..., \alpha_n \in R \backslash \{0\}$.

For example:

$$x^2 + y^2 + z^2 + w^2$$

$$x^2 - 4xy + 6y^2 = (x - 2y)^2 + 2y^2$$

are positive definite quadratic forms over $\mathbb{Z}$.

Say that a quadratic form Q over $\mathbb{Z}$ represents $m \in \mathbb{N}$ if there exists $a_1, a_2, ..., a_n \in \mathbb{Z}$ such that $Q(a_1, a_2, ..., a_n) = m$.

Question: Is there a simple way to tell if a quadratic form represents all positive integers?

We call such a quadratic form universal. We have already seen that universal forms exist, for example $x^2 + y^2 + z^2 + w^2$ is universal by Lagrange's four square theorem.

Say that a quadratic form Q over $\mathbb{Z}$ represents $m \in \mathbb{N}$ if there exists $a_1, a_2, ..., a_n \in \mathbb{Z}$ such that $Q(a_1, a_2, ..., a_n) = m$.

Question: Is there a simple way to tell if a quadratic form represents all positive integers?

We call such a quadratic form universal. We have already seen that universal forms exist, for example $x^2 + y^2 + z^2 + w^2$ is universal by Lagrange's four square theorem.

Say that a quadratic form Q over $\mathbb{Z}$ represents $m \in \mathbb{N}$ if there exists $a_1, a_2, ..., a_n \in \mathbb{Z}$ such that $Q(a_1, a_2, ..., a_n) = m$.

Question: Is there a simple way to tell if a quadratic form represents all positive integers?

We call such a quadratic form universal. We have already seen that universal forms exist, for example $x^2 + y^2 + z^2 + w^2$ is universal by Lagrange's four square theorem.

The 290 theorem

Let Q be a positive definite quadratic form over $\mathbb{Z}$. Then Q is universal if and only if it represents the 29 integers $1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203, 290$.

The 290 theorem was first proved by Conway and Schneeberger in 1993 but their proof was complicated and so was never published. It wasn't until 2000 that a simpler proof was found by Bhargava, one of the recipients of this years fields medals.

The 290 theorem

Let Q be a positive definite quadratic form over $\mathbb{Z}$. Then Q is universal if and only if it represents the 29 integers $1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203, 290$.

The 290 theorem was first proved by Conway and Schneeberger in 1993 but their proof was complicated and so was never published. It wasn't until 2000 that a simpler proof was found by Bhargava, one of the recipients of this years fields medals.

Outline of talk

Let $\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_n$ be a basis of $\mathbb{R}^n$. Then a "generic" element $\mathbf{v} = x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + ... + x_n\mathbf{v}_n \in \mathbb{R}^n$ satisfies:

$$\mathbf{v} \cdot \mathbf{v} = \sum_{1 \le i,j \le n} (\mathbf{v}_i \cdot \mathbf{v}_j) x_i x_j.$$

This is a positive definite quadratic form over $\mathbb{R}$!

For example the standard basis $\mathbf{v}_1 = (1, 0, ..., 0), \mathbf{v}_2 = (0, 1, ..., 0), ..., \mathbf{v}_n = (0, ..., 0, 1)$ gives us the quadratic form $x_1^2 + x_2^2 + ... + x_n^2$.

Let $\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_n$ be a basis of $\mathbb{R}^n$. Then a "generic" element $\mathbf{v} = x_1\mathbf{v}_1 + x_2\mathbf{v}_2 + ... + x_n\mathbf{v}_n \in \mathbb{R}^n$ satisfies:

$$\mathbf{v} \cdot \mathbf{v} = \sum_{1 \leq i,j \leq n} (\mathbf{v}_i \cdot \mathbf{v}_j) x_i x_j.$$

This is a positive definite quadratic form over $\mathbb{R}$!

For example the standard basis $\mathbf{v}_1 = (1, 0, ..., 0), \mathbf{v}_2 = (0, 1, ..., 0), ..., \mathbf{v}_n = (0, ..., 0, 1)$ gives us the quadratic form $x_1^2 + x_2^2 + ... + x_n^2$.

The following guarantees that we get quadratic forms over $\mathbb{Z}$.

An integral basis is one such that $\mathbf{v}_i \cdot \mathbf{v}_j \in \mathbb{Z}$ for each i, j.

We also want the variables in our forms to take integer values only. We can make this happen by considering only the integer linear combinations of basis vectors.

The following guarantees that we get quadratic forms over $\mathbb{Z}$.

An integral basis is one such that $\mathbf{v}_i \cdot \mathbf{v}_j \in \mathbb{Z}$ for each i, j.

We also want the variables in our forms to take integer values only. We can make this happen by considering only the integer linear combinations of basis vectors.

Definition

Let $\Lambda \subseteq \mathbb{R}^n$. Then Λ is a lattice if there exists a basis $\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_n$ of $\mathbb{R}^n$ such that:

$$\Lambda = \mathbb{Z}\mathbf{v}_1 \oplus \mathbb{Z}\mathbf{v}_2 \oplus ... \oplus \mathbb{Z}\mathbf{v}_n$$

An integral lattice is one corresponding to an integral basis.

We then have the following correspondence:

Theorem

There is a one-to-one correspondence between integral lattices in $\mathbb{R}^n$ and positive definite quadratic forms in n variables over $\mathbb{Z}$ (up to equivalence of lattices and forms).

Definition

Let $\Lambda \subseteq \mathbb{R}^n$. Then Λ is a lattice if there exists a basis $\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_n$ of $\mathbb{R}^n$ such that:

$$\Lambda = \mathbb{Z}\mathbf{v}_1 \oplus \mathbb{Z}\mathbf{v}_2 \oplus ... \oplus \mathbb{Z}\mathbf{v}_n$$

An integral lattice is one corresponding to an integral basis.

We then have the following correspondence:

Theorem

There is a one-to-one correspondence between integral lattices in $\mathbb{R}^n$ and positive definite quadratic forms in n variables over $\mathbb{Z}$ (up to equivalence of lattices and forms).

The Gram matrix of a lattice $\Lambda = \mathbb{Z}\mathbf{v}_1 \oplus \mathbb{Z}\mathbf{v}_2 \oplus ... \oplus \mathbb{Z}\mathbf{v}_n$ is the matrix $M_\Lambda = (a_{i,j})$, where:

$$a_{i,j} = \begin{cases} \mathbf{v}_i \cdot \mathbf{v}_j & \text{if } i = j \\ \frac{\mathbf{v}_i \cdot \mathbf{v}_j}{2} & \text{otherwise} \end{cases}$$

If Λ is integral then the entries of this matrix lie in $\frac{1}{2}\mathbb{Z}$.

The Gram matrix encodes within it the quadratic form attached to Λ. In fact the quadratic form is $Q_\Lambda = \mathbf{x} M_\Lambda \mathbf{x}^T$, where $\mathbf{x} = (x_1, x_2, ..., x_n)$.

The Gram matrix of a lattice $\Lambda = \mathbb{Z}\mathbf{v}_1 \oplus \mathbb{Z}\mathbf{v}_2 \oplus \ldots \oplus \mathbb{Z}\mathbf{v}_n$ is the matrix $M_\Lambda = (a_{i,j})$, where:

$$a_{i,j} = \begin{cases} \mathbf{v}_i \cdot \mathbf{v}_j & \text{if } i = j \\ \frac{\mathbf{v}_i \cdot \mathbf{v}_j}{2} & \text{otherwise} \end{cases}$$

If Λ is integral then the entries of this matrix lie in $\frac{1}{2}\mathbb{Z}$.

The Gram matrix encodes within it the quadratic form attached to Λ. In fact the quadratic form is $Q_\Lambda = \mathbf{x} M_\Lambda \mathbf{x}^T$, where $\mathbf{x} = (x_1, x_2, \ldots, x_n)$.

Outline of talk

We will not be able to see a full proof of the 290 theorem but we will be able to see a part of Bhargava's elegant argument.

Let Q be a non-universal positive definite quadratic form over $\mathbb{Z}$. The truant of Q is defined to be the smallest positive integer not represented by Q.

Let Λ be an integral lattice with Q as its quadratic form. Then an escalation of Λ is an integral lattice Λ' generated by Λ and a vector $\mathbf{v}$ such that $\mathbf{v} \cdot \mathbf{v}$ is the truant of Q.

We will not be able to see a full proof of the 290 theorem but we will be able to see a part of Bhargava's elegant argument.

Let Q be a non-universal positive definite quadratic form over $\mathbb{Z}$. The truant of Q is defined to be the smallest positive integer not represented by Q.

Let Λ be an integral lattice with Q as its quadratic form. Then an escalation of Λ is an integral lattice Λ' generated by Λ and a vector $\mathbf{v}$ such that $\mathbf{v} \cdot \mathbf{v}$ is the truant of Q.

Bhargava's idea is to consider chains of escalators that come from the zero dimensional lattice $\{0\}$.

Clearly the truant of $\{0\}$ is 1 so we may escalate by creating the lattice $\Lambda_1 = \mathbb{Z}$. This is the only possible choice.

Now $Q_{\Lambda_1}(x) = x^2$ and so the truant is 2. Thus we may escalate by creating a vector $\mathbf{v} \in \mathbb{R}^2$ such that $\mathbf{v} \cdot \mathbf{v} = 2$ and setting $\Lambda_2 = \mathbb{Z}(1, 0) \oplus \mathbb{Z}\mathbf{v}$.

However there are genuinely different lattices that can arise!

Bhargava's idea is to consider chains of escalators that come from the zero dimensional lattice $\{0\}$.

Clearly the truant of $\{0\}$ is 1 so we may escalate by creating the lattice $\Lambda_1 = \mathbb{Z}$. This is the only possible choice.

Now $Q_{\Lambda_1}(x) = x^2$ and so the truant is 2. Thus we may escalate by creating a vector $\mathbf{v} \in \mathbb{R}^2$ such that $\mathbf{v} \cdot \mathbf{v} = 2$ and setting $\Lambda_2 = \mathbb{Z}(1,0) \oplus \mathbb{Z}\mathbf{v}$.

However there are genuinely different lattices that can arise!

Bhargava's idea is to consider chains of escalators that come from the zero dimensional lattice $\{0\}$.

Clearly the truant of $\{0\}$ is 1 so we may escalate by creating the lattice $\Lambda_1 = \mathbb{Z}$. This is the only possible choice.

Now $Q_{\Lambda_1}(x) = x^2$ and so the truant is 2. Thus we may escalate by creating a vector $\mathbf{v} \in \mathbb{R}^2$ such that $\mathbf{v} \cdot \mathbf{v} = 2$ and setting $\Lambda_2 = \mathbb{Z}(1,0) \oplus \mathbb{Z}\mathbf{v}$.
However there are genuinely different lattices that can arise!

Consider the Gram matrix of such an escalation:

$$M_{\Lambda_2} = \begin{pmatrix} 1 & a \\ a & 2 \end{pmatrix}$$

We know that $a = \frac{(1,0)\cdot\mathbf{v}}{2} \in \frac{1}{2}\mathbb{Z}$ and also by the Cauchy-Schwarz inequality $a^2 \leq 2$ and so $a = 0, \pm\frac{1}{2}, \pm 1$.

Up to equivalence we get the following three possibilities (in reduced form):

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

These give quadratic forms $x^2 + 2y^2, x^2 + xy + 2y^2$ and $x^2 + y^2$ respectively. The truants are then 5, 3 and 3 respectively.

Consider the Gram matrix of such an escalation:

$$M_{\Lambda_2} = \begin{pmatrix} 1 & a \\ a & 2 \end{pmatrix}$$

We know that $a = \frac{(1,0)\cdot\mathbf{v}}{2} \in \frac{1}{2}\mathbb{Z}$ and also by the Cauchy-Schwarz inequality $a^2 \leq 2$ and so $a = 0, \pm\frac{1}{2}, \pm 1$.

Up to equivalence we get the following three possibilities (in reduced form):

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

These give quadratic forms $x^2 + 2y^2, x^2 + xy + 2y^2$ and $x^2 + y^2$ respectively. The truants are then 5, 3 and 3 respectively.

Consider the Gram matrix of such an escalation:

$$M_{\Lambda_2} = \begin{pmatrix} 1 & a \\ a & 2 \end{pmatrix}$$

We know that $a = \frac{(1,0)\cdot \mathbf{v}}{2} \in \frac{1}{2}\mathbb{Z}$ and also by the Cauchy-Schwarz inequality $a^2 \leq 2$ and so $a = 0, \pm\frac{1}{2}, \pm 1$.

Up to equivalence we get the following three possibilities (in reduced form):

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

These give quadratic forms $x^2 + 2y^2, x^2 + xy + 2y^2$ and $x^2 + y^2$ respectively. The truants are then 5, 3 and 3 respectively.

We can play the same game with each Λ_2 (since each has a truant), generating escalator lattices $\Lambda_3 \subseteq \mathbb{R}^3$. We find this time that there are 34 possibilities (up to equivalence).

Each of the 34 forms has a truant and so we continue to play the game.

A crazy thing happens once we reach four dimensions. We now expect some of the quadratic forms to be universal (we know that $x^2 + y^2 + z^2 + w^2$ is by Lagrange).

We can play the same game with each Λ_2 (since each has a truant), generating escalator lattices $\Lambda_3 \subseteq \mathbb{R}^3$. We find this time that there are 34 possibilities (up to equivalence).

Each of the 34 forms has a truant and so we continue to play the game.

A crazy thing happens once we reach four dimensions. We now expect some of the quadratic forms to be universal (we know that $x^2 + y^2 + z^2 + w^2$ is by Lagrange).

We can play the same game with each Λ_2 (since each has a truant), generating escalator lattices $\Lambda_3 \subseteq \mathbb{R}^3$. We find this time that there are 34 possibilities (up to equivalence).

Each of the 34 forms has a truant and so we continue to play the game.

A crazy thing happens once we reach four dimensions. We now expect some of the quadratic forms to be universal (we know that $x^2 + y^2 + z^2 + w^2$ is by Lagrange).

Indeed we get a collection of 6560 possibilities for escalators Λ_4 of Λ_3 (up to equivalence).

- Luckily 6402 of these are universal! (Non-trivial, needs modular forms etc).
- 153 happen to represent all but 3 or less positive integers and so become universal after at most 3 escalations!
- The other 5 forms are problematic but all have truant 14 and came from an escalation of a Λ_3 that has truant 10. Swapping the order of these truants turns out to give escalations that fall into the second case above.

Indeed we get a collection of 6560 possibilities for escalators Λ_4 of Λ_3 (up to equivalence).

- Luckily 6402 of these are universal! (Non-trivial, needs modular forms etc).
- 153 happen to represent all but 3 or less positive integers and so become universal after at most 3 escalations!
- The other 5 forms are problematic but all have truant 14 and came from an escalation of a Λ_3 that has truant 10. Swapping the order of these truants turns out to give escalations that fall into the second case above.

Indeed we get a collection of 6560 possibilities for escalators Λ_4 of Λ_3 (up to equivalence).

- Luckily 6402 of these are universal! (Non-trivial, needs modular forms etc).
- 153 happen to represent all but 3 or less positive integers and so become universal after at most 3 escalations!
- The other 5 forms are problematic but all have truant 14 and came from an escalation of a Λ_3 that has truant 10. Swapping the order of these truants turns out to give escalations that fall into the second case above.

Indeed we get a collection of 6560 possibilities for escalators Λ_4 of Λ_3 (up to equivalence).

- Luckily 6402 of these are universal! (Non-trivial, needs modular forms etc).
- 153 happen to represent all but 3 or less positive integers and so become universal after at most 3 escalations!
- The other 5 forms are problematic but all have truant 14 and came from an escalation of a Λ_3 that has truant 10. Swapping the order of these truants turns out to give escalations that fall into the second case above.

Result

The zero dimensional lattice can be escalated at most seven times (producing collections of lattices Λ_i for $i = 1, 2, ..., 7$).

So how does this prove the 290 theorem?

Facts:

- Every integral lattice Λ must contain one of the escalators Λ_i for some i.
- If Λ is non-universal then its truant is the truant of one of the non-universal Λ_i.

Since we know all truants for the Λ_i we know that exactly these numbers must be represented for Λ to be universal. This list of numbers matches the one in the 290 theorem.

Result

The zero dimensional lattice can be escalated at most seven times (producing collections of lattices Λ_i for $i = 1, 2, ..., 7$).

So how does this prove the 290 theorem?

Facts:

- Every integral lattice Λ must contain one of the escalators Λ_i for some i.
- If Λ is non-universal then its truant is the truant of one of the non-universal Λ_i.

Since we know all truants for the Λ_i we know that exactly these numbers must be represented for Λ to be universal. This list of numbers matches the one in the 290 theorem.

Result

The zero dimensional lattice can be escalated at most seven times (producing collections of lattices Λ_i for $i = 1, 2, ..., 7$).

So how does this prove the 290 theorem?

Facts:

- Every integral lattice Λ must contain one of the escalators Λ_i for some i.
- If Λ is non-universal then its truant is the truant of one of the non-universal Λ_i.

Since we know all truants for the Λ_i we know that exactly these numbers must be represented for Λ to be universal. This list of numbers matches the one in the 290 theorem.

Thanks for listening!