The Finite Simple Groups II: Proof of the classification

Nick Gill (OU)

November 15, 2012

A brief recap...

Recall that...

A brief recap...

Recall that...

Definition

A group G is called simple if it has no non-trivial proper normal subgroups.

The Classification of Finite Simple Groups

Today we will prove the following theorem.

The Classification of Finite Simple Groups

Today we will prove the following theorem.

Theorem

Let G be a finite simple group. Then G lies in one (or more) of the following families:

The Classification of Finite Simple Groups

Today we will prove the following theorem.

Theorem

Let G be a finite simple group. Then G lies in one (or more) of the following families:

1. *the cyclic groups of prime order;*

The Classification of Finite Simple Groups

Today we will prove the following theorem.

Theorem

Let G be a finite simple group. Then G lies in one (or more) of the following families:

1. *the cyclic groups of prime order;*
2. *the alternating groups of degree at least 5;*

The Classification of Finite Simple Groups

Today we will prove the following theorem.

Theorem

Let G be a finite simple group. Then G lies in one (or more) of the following families:

1. *the cyclic groups of prime order;*
2. *the alternating groups of degree at least 5;*
3. *the finite groups of Lie type;*

The Classification of Finite Simple Groups

Today we will prove the following theorem.

Theorem

Let G be a finite simple group. Then G lies in one (or more) of the following families:

1. *the cyclic groups of prime order;*
2. *the alternating groups of degree at least 5;*
3. *the finite groups of Lie type;*
4. *the 26 sporadic groups.*

Building groups

Building groups

The simple groups are often described as the 'building blocks' of groups, in the following sense...

Building groups

The simple groups are often described as the 'building blocks' of groups, in the following sense...

Definition

A **composition series** *of a group G is a subnormal series*

$$\{1\} = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$$

such that every quotient H_{i+1}/H_i is a non-trivial simple group.

Building groups

The simple groups are often described as the 'building blocks' of groups, in the following sense...

Definition

A **composition series** *of a group G is a subnormal series*

$$\{1\} = H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$$

such that every quotient H_{i+1}/H_i is a non-trivial simple group.

The quotients H_{i+1}/H_i are called the **composition factors** of G.

Composition series

Composition series

Theorem

Let G be a group with two composition series:

$$\{1\} = G_0 \lhd G_1 \lhd G_2 \cdots \lhd G_m = G;$$

$$\{1\} = H_0 \lhd H_1 \lhd H_2 \cdots \lhd H_n = G.$$

Then the two multisets of composition factors are equal:

$$\{G_1/G_0, \dots G_m/G_{m-1}\} = \{H_1/H_0, \dots, H_n/H_{n-1}\}.$$

Composition series

Theorem

Let G be a group with two composition series:

$$\{1\} = G_0 \lhd G_1 \lhd G_2 \cdots \lhd G_m = G;$$

$$\{1\} = H_0 \lhd H_1 \lhd H_2 \cdots \lhd H_n = G.$$

Then the two multisets of composition factors are equal:

$$\{G_1/G_0, \dots G_m/G_{m-1}\} = \{H_1/H_0, \dots, H_n/H_{n-1}\}.$$

Thus G has associated to it a unique multiset of composition factors. We think of G as being 'built' from this multiset.

Composition series

Theorem

Let G be a group with two composition series:

$$\{1\} = G_0 \lhd G_1 \lhd G_2 \cdots \lhd G_m = G;$$

$$\{1\} = H_0 \lhd H_1 \lhd H_2 \cdots \lhd H_n = G.$$

Then the two multisets of composition factors are equal:

$$\{G_1/G_0, \ldots G_m/G_{m-1}\} = \{H_1/H_0, \ldots, H_n/H_{n-1}\}.$$

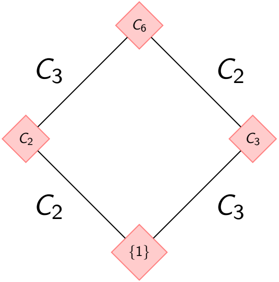
Thus G has associated to it a unique multiset of composition factors. We think of G as being 'built' from this multiset.
If the composition factors are all cyclic of prime order, then we call G **soluble** or **solvable** (after Galois).

More on composition factors

Consider the cyclic group C_6. Here are two composition series:

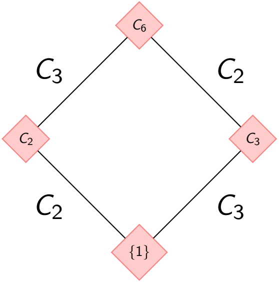
More on composition factors

Consider the cyclic group C_6. Here are two composition series:



More on composition factors

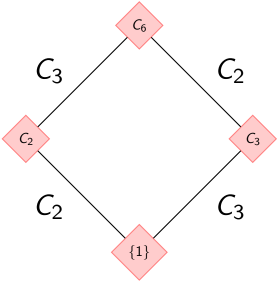
Consider the cyclic group C_6. Here are two composition series:



Clearly the multiset of composition factors of C_6 is $\{C_2, C_3\}$.

More on composition factors

Consider the cyclic group C_6. Here are two composition series:



Clearly the multiset of composition factors of C_6 is $\{C_2, C_3\}$.
Warning: This is also the multiset of composition factors for $\mathrm{Sym}(3)$...

Group cohomology

Group cohomology

In general there may be many ways to construct a group from a multiset of composition factors. Understanding this situation is hard...

Group cohomology

In general there may be many ways to construct a group from a multiset of composition factors. Understanding this situation is hard...

Theorem

Let N be an abelian group, and let Q be any group. Equivalence classes of extensions

$$\{1\} \to N \to G \to Q \to \{1\}$$

are in 1-1 correspondence with the cohomology group $H^2(Q, N)$.

The proof of CFSG

Our story starts, in 1963, with two very clever men and a 255 page paper.

The proof of CFSG

Our story starts, in 1963, with two very clever men and a 255 page paper.

Walter Feit

The proof of CFSG

Our story starts, in 1963, with two very clever men and a 255 page paper.

Walter Feit

John Thompson

The Odd Order Theorem

The Odd Order Theorem

Theorem

If G is a finite simple group of odd order, then G is cyclic.

The Odd Order Theorem

Theorem

If G is a finite simple group of odd order, then G is cyclic.

An equivalent formulation is the following:

Theorem

If G is a finite group of odd order, then G is soluble.

Proving the Odd Order Theorem

Proving the Odd Order Theorem

The basic strategy of the Odd Order Theorem is the same as the basic strategy of the proof of CFSG.

Proving the Odd Order Theorem

The basic strategy of the Odd Order Theorem is the same as the basic strategy of the proof of CFSG.

1. Suppose G is a non-soluble group of odd order.

Proving the Odd Order Theorem

The basic strategy of the Odd Order Theorem is the same as the basic strategy of the proof of CFSG.

1. Suppose G is a non-soluble group of odd order.
2. We may assume that G is a **minimal counter-example**,

Proving the Odd Order Theorem

The basic strategy of the Odd Order Theorem is the same as the basic strategy of the proof of CFSG.

1. Suppose G is a non-soluble group of odd order.
2. We may assume that G is a **minimal counter-example**, i.e. G is a simple group for which every subgroup is soluble.

Proving the Odd Order Theorem

The basic strategy of the Odd Order Theorem is the same as the basic strategy of the proof of CFSG.

1. Suppose G is a non-soluble group of odd order.
2. We may assume that G is a **minimal counter-example**, i.e. G is a simple group for which every subgroup is soluble.
3. Study the **internal structure** of G,

Proving the Odd Order Theorem

The basic strategy of the Odd Order Theorem is the same as the basic strategy of the proof of CFSG.

1. Suppose G is a non-soluble group of odd order.
2. We may assume that G is a **minimal counter-example**, i.e. G is a simple group for which every subgroup is soluble.
3. Study the **internal structure** of G, i.e. use group theory to analyse the possible structure of the maximal subgroups of G.

Proving the Odd Order Theorem

The basic strategy of the Odd Order Theorem is the same as the basic strategy of the proof of CFSG.

1. Suppose G is a non-soluble group of odd order.
2. We may assume that G is a **minimal counter-example**, i.e. G is a simple group for which every subgroup is soluble.
3. Study the **internal structure** of G, i.e. use group theory to analyse the possible structure of the maximal subgroups of G.
4. Derive a **contradiction** somehow(!)

Proving the Odd Order Theorem

The basic strategy of the Odd Order Theorem is the same as the basic strategy of the proof of CFSG.

1. Suppose G is a non-soluble group of odd order.
2. We may assume that G is a **minimal counter-example**, i.e. G is a simple group for which every subgroup is soluble.
3. Study the **internal structure** of G, i.e. use group theory to analyse the possible structure of the maximal subgroups of G.
4. Derive a **contradiction** somehow(!) In this case Feit and Thompson used the Brauer-Suzuki theory of exceptional characters. This theory connects the characters of a group G to the characters of its maximal subgroups.

Characters, what?

Let G be a finite group.

Characters, what?

Let G be a finite group.

1. A **representation** of G is a homomorphism $\rho : G \to GL(V)$ where V is an n-dimensional vector space over $\mathbb{C}$.

Characters, what?

Let G be a finite group.

1. A **representation** of G is a homomorphism $\rho : G \to GL(V)$ where V is an n-dimensional vector space over $\mathbb{C}$.
2. Each representation $\rho : G \to GL(V)$ yields a **character**:

$$\chi_\rho : G \to \mathbb{C}, g \mapsto \mathrm{trace}(\rho(g)).$$

Characters, what?

Let G be a finite group.

1. A **representation** of G is a homomorphism $\rho : G \to GL(V)$ where V is an n-dimensional vector space over $\mathbb{C}$.
2. Each representation $\rho : G \to GL(V)$ yields a **character**:

$$\chi_\rho : G \to \mathbb{C}, g \mapsto \mathrm{trace}(\rho(g)).$$

3. A representation is called **irreducible** if the matrices representing G do not preserve any non-trivial proper subspace of V.

Characters, what?

Let G be a finite group.

1. A **representation** of G is a homomorphism $\rho : G \to GL(V)$ where V is an n-dimensional vector space over $\mathbb{C}$.
2. Each representation $\rho : G \to GL(V)$ yields a **character**:

$$\chi_\rho : G \to \mathbb{C}, g \mapsto \mathrm{trace}(\rho(g)).$$

3. A representation is called **irreducible** if the matrices representing G do not preserve any non-trivial proper subspace of V.
4. Fact: the irreducible representations (and hence the irreducible characters) of G are in 1-1 correspondence with the conjugacy classes of G.

The Character Table

The Character Table

The characters of a group G can be written down in a square of numbers called the *Character Table of G*.

The Character Table

The characters of a group G can be written down in a square of numbers called the *Character Table of G*.

Char/ CC	1A	2A	3A	5A	5B
χ_1	1	1	1	1	1
χ_2	3	-1	0	$\frac{1}{2}(1+\sqrt{5})$	$\frac{1}{2}(1-\sqrt{5})$
χ_3	3	-1	0	$\frac{1}{2}(1-\sqrt{5})$	$\frac{1}{2}(1+\sqrt{5})$
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

The Character Table

The characters of a group G can be written down in a square of numbers called the *Character Table of G*.

Char/ CC	1A	2A	3A	5A	5B
χ_1	1	1	1	1	1
χ_2	3	-1	0	$\frac{1}{2}(1+\sqrt{5})$	$\frac{1}{2}(1-\sqrt{5})$
χ_3	3	-1	0	$\frac{1}{2}(1-\sqrt{5})$	$\frac{1}{2}(1+\sqrt{5})$
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

If one is given the character table of some mysterious group G, then one can immediately derive a lot of information about G.

The Character Table

The characters of a group G can be written down in a square of numbers called the *Character Table of G*.

Char/ CC	1A	2A	3A	5A	5B
χ_1	1	1	1	1	1
χ_2	3	-1	0	$\frac{1}{2}(1+\sqrt{5})$	$\frac{1}{2}(1-\sqrt{5})$
χ_3	3	-1	0	$\frac{1}{2}(1-\sqrt{5})$	$\frac{1}{2}(1+\sqrt{5})$
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

If one is given the character table of some mysterious group G, then one can immediately derive a lot of information about G. The above character table of a perfect group G of order 60...

The Character Table

The characters of a group G can be written down in a square of numbers called the *Character Table of G*.

Char/ CC	1A	2A	3A	5A	5B
χ_1	1	1	1	1	1
χ_2	3	-1	0	$\frac{1}{2}(1+\sqrt{5})$	$\frac{1}{2}(1-\sqrt{5})$
χ_3	3	-1	0	$\frac{1}{2}(1-\sqrt{5})$	$\frac{1}{2}(1+\sqrt{5})$
χ_4	4	0	1	-1	-1
χ_5	5	1	-1	0	0

If one is given the character table of some mysterious group G, then one can immediately derive a lot of information about G. The above character table of a perfect group G of order 60... So G must be $\mathrm{Alt}(5)$.

Characters and simple groups

Characters and simple groups

Characters had already been used, to spectacular effect, to prove a famous theorem about simple groups.

Characters and simple groups

Characters had already been used, to spectacular effect, to prove a famous theorem about simple groups.

William Burnside

Characters and simple groups

Characters had already been used, to spectacular effect, to prove a famous theorem about simple groups.

William Burnside

Theorem

(Burnside 1904) *If G is a finite simple group of order $p^a q^b$, for primes p and q, then G is cyclic.*

Characters and simple groups

Characters had already been used, to spectacular effect, to prove a famous theorem about simple groups.

William Burnside

Theorem

(Burnside 1904) *If G is a finite simple group of order $p^a q^b$, for primes p and q, then G is cyclic.*

Character theory would play a significant role in many of the results leading to CFSG.

What was that 'internal structure' nonsense?

What was that 'internal structure' nonsense?

Suppose that G is a minimal counter-example to the odd-order theorem. Here's an example of the sort of analysis used (due to Suzuki).

What was that 'internal structure' nonsense?

Suppose that G is a minimal counter-example to the odd-order theorem. Here's an example of the sort of analysis used (due to Suzuki).

1. **Special case**: the centralizer of every non-trivial element of G is abelian.

What was that 'internal structure' nonsense?

Suppose that G is a minimal counter-example to the odd-order theorem. Here's an example of the sort of analysis used (due to Suzuki).

1. **Special case**: the centralizer of every non-trivial element of G is abelian.
2. Then the elements of $G\backslash\{1\}$ break up into equivalence classes, such that each equivalence class is the set of non-identity elements of a maximal abelian subgroup of G.

What was that 'internal structure' nonsense?

Suppose that G is a minimal counter-example to the odd-order theorem. Here's an example of the sort of analysis used (due to Suzuki).

1. **Special case**: the centralizer of every non-trivial element of G is abelian.
2. Then the elements of $G \backslash \{1\}$ break up into equivalence classes, such that each equivalence class is the set of non-identity elements of a maximal abelian subgroup of G.
3. The normalizers of these maximal abelian subgroups turn out to be exactly the maximal proper subgroups of G.

What was that ‘internal structure’ nonsense?

Suppose that G is a minimal counter-example to the odd-order theorem. Here’s an example of the sort of analysis used (due to Suzuki).

1. **Special case**: the centralizer of every non-trivial element of G is abelian.
2. Then the elements of $G\backslash\{1\}$ break up into equivalence classes, such that each equivalence class is the set of non-identity elements of a maximal abelian subgroup of G.
3. The normalizers of these maximal abelian subgroups turn out to be exactly the maximal proper subgroups of G.
4. What is more these normalizers are Frobenius groups, i.e. they have a very special, very well understood structure.

What was that 'internal structure' nonsense?

Suppose that G is a minimal counter-example to the odd-order theorem. Here's an example of the sort of analysis used (due to Suzuki).

1. **Special case**: the centralizer of every non-trivial element of G is abelian.
2. Then the elements of $G \backslash \{1\}$ break up into equivalence classes, such that each equivalence class is the set of non-identity elements of a maximal abelian subgroup of G.
3. The normalizers of these maximal abelian subgroups turn out to be exactly the maximal proper subgroups of G.
4. What is more these normalizers are Frobenius groups, i.e. they have a very special, very well understood structure.
5. One can work out the characters of G by *inducing* from the characters of these Frobenius groups.

Lessons to be learnt

Lessons to be learnt

- Notice that, in the special case we just discussed, all of the maximal subgroups of G are normalizers of a p-group for some prime p.

Lessons to be learnt

- Notice that, in the special case we just discussed, all of the maximal subgroups of G are normalizers of a p-group for some prime p.
- Definition: A **local subgroup** of a group G is a subgroup which is equal to the normalizer of a p-group.

Lessons to be learnt

- Notice that, in the special case we just discussed, all of the maximal subgroups of G are normalizers of a p-group for some prime p.
- Definition: A **local subgroup** of a group G is a subgroup which is equal to the normalizer of a p-group.
- It turns out that the local subgroups are the most important when it comes to understanding 'internal structure'.

Lessons to be learnt

- Notice that, in the special case we just discussed, all of the maximal subgroups of G are normalizers of a p-group for some prime p.
- Definition: A **local subgroup** of a group G is a subgroup which is equal to the normalizer of a p-group.
- It turns out that the local subgroups are the most important when it comes to understanding 'internal structure'.
- And so **local analysis** is born.

Involution centralizers

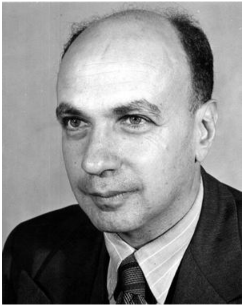
The most important local subgroups are involution centralizers.

Involution centralizers

The most important local subgroups are involution centralizers. Note that the Odd Order Theorem implies that a nonabelian simple group always contains such a thing.

Involution centralizers

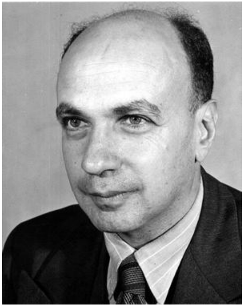
The most important local subgroups are involution centralizers. Note that the Odd Order Theorem implies that a nonabelian simple group always contains such a thing.



Richard Brauer

Involution centralizers

The most important local subgroups are involution centralizers. Note that the Odd Order Theorem implies that a nonabelian simple group always contains such a thing.



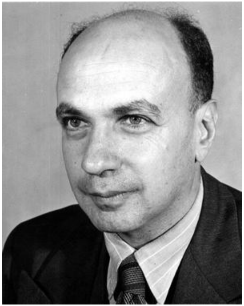
Richard Brauer

Theorem

(Brauer 1955) *There are a finite number of simple groups with a specified involution centralizer.*

Involution centralizers

The most important local subgroups are involution centralizers. Note that the Odd Order Theorem implies that a nonabelian simple group always contains such a thing.



Richard Brauer

Theorem

(Brauer 1955) *There are a finite number of simple groups with a specified involution centralizer.*

11 of the 21 modern sporadic groups were discovered by examining involution centralizers...

J_1

J_1

In 1966 Janko discovered J_1, the first new sporadic group since Mathieu. His theorem is typical of the area.

J_1

In 1966 Janko discovered J_1, the first new sporadic group since Mathieu. His theorem is typical of the area.

J_1

In 1966 Janko discovered J_1, the first new sporadic group since Mathieu. His theorem is typical of the area.

Theorem

If G is a simple group with abelian Sylow 2-subgroups of order 8 and the centralizer of some involution of G is isomorphic to $C_2 \times \mathrm{Alt}(5)$, then G is a uniquely determined simple group of order 175, 560.

J_1

In 1966 Janko discovered J_1, the first new sporadic group since Mathieu. His theorem is typical of the area.

Theorem

If G is a simple group with abelian Sylow 2-subgroups of order 8 and the centralizer of some involution of G is isomorphic to $C_2 \times \mathrm{Alt}(5)$, then G is a uniquely determined simple group of order 175, 560.

Moreover Janko gave two matrices in $GL_7(11)$ which generated this new group.

A game of two halves

The discovery of a new sporadic group often proceeded in two stages. Take the other Janko groups J_2 and J_3, for instance.

A game of two halves

The discovery of a new sporadic group often proceeded in two stages. Take the other Janko groups J_2 and J_3, for instance.

Theorem

(Janko 1969) *If G is a simple group in which the centralizer of an involution is isomorphic to $(Q_8 * Q_8).\mathrm{Alt}(5)$, then one of the following holds:*

1. *G has two classes of involutions and $|G| = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7$;*
2. *G has one class of involutions and $|G| = 2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$.*

A game of two halves

The discovery of a new sporadic group often proceeded in two stages. Take the other Janko groups J_2 and J_3, for instance.

Theorem

(Janko 1969) *If G is a simple group in which the centralizer of an involution is isomorphic to $(Q_8 * Q_8).\mathrm{Alt}(5)$, then one of the following holds:*

1. *G has two classes of involutions and $|G| = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7$;*
2. *G has one class of involutions and $|G| = 2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$.*

Janko proved this theorem with local analysis. In both cases he determined the complete local structure of such a group G as well as its character table.

A game of two halves

The discovery of a new sporadic group often proceeded in two stages. Take the other Janko groups J_2 and J_3, for instance.

Theorem

(Janko 1969) *If G is a simple group in which the centralizer of an involution is isomorphic to $(Q_8 * Q_8).\mathrm{Alt}(5)$, then one of the following holds:*

1. *G has two classes of involutions and $|G| = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7$;*
2. *G has one class of involutions and $|G| = 2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$.*

Janko proved this theorem with local analysis. In both cases he determined the complete local structure of such a group G as well as its character table.
But does such a group **exist?**

A game of two halves

The discovery of a new sporadic group often proceeded in two stages. Take the other Janko groups J_2 and J_3, for instance.

Theorem

(Janko 1969) *If G is a simple group in which the centralizer of an involution is isomorphic to $(Q_8 * Q_8).\mathrm{Alt}(5)$, then one of the following holds:*

1. *G has two classes of involutions and $|G| = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7$;*
2. *G has one class of involutions and $|G| = 2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$.*

Janko proved this theorem with local analysis. In both cases he determined the complete local structure of such a group G as well as its character table.

But does such a group **exist?** And, if it does, is it **unique?**

The second half

The second half

For both cases, the answer to both questions is “yes”.

The second half

For both cases, the answer to both questions is “yes”.

1. For the first case, $|G| = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7 = 604,800$. Hall and Wales constructed a group of the required form inside $\mathrm{Sym}(100)$. They were also able to prove uniqueness.

The second half

For both cases, the answer to both questions is "yes".

1. For the first case, $|G| = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7 = 604,800$. Hall and Wales constructed a group of the required form inside $\mathrm{Sym}(100)$. They were also able to prove uniqueness.
2. For the second case, $|G| = 50,232,960$. Higman and McKay constructed a simple group of this order, and Wong was able to show that if such a group existed then it was unique.

The second half

For both cases, the answer to both questions is “yes”.

1. For the first case, $|G| = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7 = 604,800$. Hall and Wales constructed a group of the required form inside $\mathrm{Sym}(100)$. They were also able to prove uniqueness.
2. For the second case, $|G| = 50,232,960$. Higman and McKay constructed a simple group of this order, and Wong was able to show that if such a group existed then it was unique.

Methods varied and, at least initially, involved the use of computers.

Proof Structure

Proof Structure

Proof Structure

Danny Gorenstein

Proof Structure

Danny Gorenstein

In 1972 Danny Gorenstein proposed a 16-point program for proving CFSG. He broke down the different possible centralizer types into different categories, and encouraged people to go at it!

Proof Structure

Danny Gorenstein

In 1972 Danny Gorenstein proposed a 16-point program for proving CFSG. He broke down the different possible centralizer types into different categories, and encouraged people to go at it!

Hypothesis: Suppose G is a minimal counter-example to CFSG. i.e. the composition factors of all proper subgroups of G are in one of the four families. Then...

What were the chances?

What were the chances?

Ron Solomon writes of the period,

> *Not a single leading group theorist besides Gorenstein believed in 1972 that the Classification would be completed this century. By 1976, almost everyone believed that the Classification problem was "busted". The principal reason was Michael Aschbacher's lightning assaults on the B-Conjecture, the Thin Group Problem, and the Strongly p-embedded 2-local problem.*

What were the chances?

Ron Solomon writes of the period,

> *Not a single leading group theorist besides Gorenstein believed in 1972 that the Classification would be completed this century. By 1976, almost everyone believed that the Classification problem was "busted". The principal reason was Michael Aschbacher's lightning assaults on the B-Conjecture, the Thin Group Problem, and the Strongly p-embedded 2-local problem.*

Michael Aschbacher

How did it end?

How did it end?

- The existence of a new sporadic group M was predicted in 1973 independently by B. Fischer and R. Griess.

How did it end?

- The existence of a new sporadic group M was predicted in 1973 independently by B. Fischer and R. Griess.
- Griess was interested in classifying those simple groups containing $2.B$ as the centralizer of an involution.

How did it end?

- The existence of a new sporadic group M was predicted in 1973 independently by B. Fischer and R. Griess.
- Griess was interested in classifying those simple groups containing $2.B$ as the centralizer of an involution.
- Griess calculated that, if M existed, it had order

  $$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

How did it end?

- The existence of a new sporadic group M was predicted in 1973 independently by B. Fischer and R. Griess.
- Griess was interested in classifying those simple groups containing $2.B$ as the centralizer of an involution.
- Griess calculated that, if M existed, it had order

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

- Griess later constructed a group M with the given properties as the automorphism of an algebra over a real vector space of dimension 196 884.

How did it end?

- The existence of a new sporadic group M was predicted in 1973 independently by B. Fischer and R. Griess.
- Griess was interested in classifying those simple groups containing $2.B$ as the centralizer of an involution.
- Griess calculated that, if M existed, it had order

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

- Griess later constructed a group M with the given properties as the automorphism of an algebra over a real vector space of dimension 196 884.
- Thompson showed that M was the only group with the given properties admitting an irreducible representation of degree 196 883.

How did it end?

- The existence of a new sporadic group M was predicted in 1973 independently by B. Fischer and R. Griess.
- Griess was interested in classifying those simple groups containing $2.B$ as the centralizer of an involution.
- Griess calculated that, if M existed, it had order

$$2^{46}\cdot 3^{20}\cdot 5^{9}\cdot 7^{6}\cdot 11^{2}\cdot 13^{3}\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71.$$

- Griess later constructed a group M with the given properties as the automorphism of an algebra over a real vector space of dimension 196 884.
- Thompson showed that M was the only group with the given properties admitting an irreducible representation of degree 196 883.
- So, when Norton showed that all groups of this kind have such an irreducible representation, the uniqueness of M was proved.... and so was CFSG.

Some moonshine to finish

The proof of the CFSG spawned a great deal of new mathematics, of which the most celebrated involves the Monster group, and is known as **Monstrous Moonshine**.

Some moonshine to finish

The proof of the CFSG spawned a great deal of new mathematics, of which the most celebrated involves the Monster group, and is known as **Monstrous Moonshine**.

- Suppose that f is a meromorphic function on $\mathbb{H}$.

Some moonshine to finish

The proof of the CFSG spawned a great deal of new mathematics, of which the most celebrated involves the Monster group, and is known as **Monstrous Moonshine**.

- Suppose that f is a meromorphic function on $\mathbb{H}$.
- f is called a **modular function** if it satisfies

$$f\left(\frac{az+b}{cz+d}\right) = f(z)$$

for all transformations in $\Gamma = PSL_2(\mathbb{Z})$. We can think of f as a function on the Riemann surface $\mathbb{H}/\Gamma$.

More moonshine

- A particularly important modular function is the **elliptic modular function** j. It has Fourier series

$$j(q) = q^{-1} + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

More moonshine

- A particularly important modular function is the **elliptic modular function** j. It has Fourier series

$$j(q) = q^{-1} + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

- Observe that:

$$\begin{aligned} 196884 &= 196883 + 1 \\ 21493760 &= 21296786 + 196883 + 1 \\ 864299970 &= 842609326 + 21296786 + 2 \times 196883 + 2 \times 1. \end{aligned}$$

More moonshine

- A particularly important modular function is the **elliptic modular function** j. It has Fourier series

$$j(q) = q^{-1} + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

- Observe that:

$$\begin{aligned} 196884 &= 196883 + 1 \\ 21493760 &= 21296786 + 196883 + 1 \\ 864299970 &= 842609326 + 21296786 + 2 \times 196883 + 2 \times 1. \end{aligned}$$

Numbers on the RHS are dimensions of irreducible representations of the monster!

More moonshine

- A particularly important modular function is the **elliptic modular function** j. It has Fourier series

$$j(q) = q^{-1} + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

- Observe that:

$$196884 = 196883 + 1$$
$$21493760 = 21296786 + 196883 + 1$$
$$864299970 = 842609326 + 21296786 + 2 \times 196883 + 2 \times 1.$$

  Numbers on the RHS are dimensions of irreducible representations of the monster!

- These connections led Conway and Thompson to conjecture the existence of a particular graded module on which M acts naturally. What is more this action yields a 'natural construction' of the Fourier expansion of different modular functions.

The Bootleggers

The Bootleggers

John Conway

John Thompson

Richard Borcherds

The Bootleggers

John Conway

John Thompson

Richard Borcherds

Describing the experience of proving the Moonshine conjectures, Borcherds remarked:

> *I sometimes wonder if this is the feeling you get when you take certain drugs. I don't actually know, as I have not tested this theory of mine.*

All sorted then?

We've missed out a **lot** of material...

All sorted then?

We've missed out a **lot** of material...

... Signalizer functors, p-fusion, abstract fusion systems, N-groups, minimal simple groups, the Bender method, strong embedding, the generalized Fitting group, Thompson factorization, the Z^*-theorem, Aschbacher Blocks, 3-transposition groups, the Leech lattice, the amalgam method, Aschbacher and Smith's quasithin theorem,...

All sorted then?

We've missed out a **lot** of material...

... Signalizer functors, p-fusion, abstract fusion systems, N-groups, minimal simple groups, the Bender method, strong embedding, the generalized Fitting group, Thompson factorization, the Z^*-theorem, Aschbacher Blocks, 3-transposition groups, the Leech lattice, the amalgam method, Aschbacher and Smith's quasithin theorem,...

Thanks for coming!