Modular forms modulo 2
Mathematics Department Colloquium, Columbia University

Joël Bellaïche

Brandeis University, Yale University

November 30, 2012
Outline

I. Modular forms and Hecke algebra modulo 2 (published work of Nicolas and Serre)
Outline

I. Modular forms and Hecke algebra modulo 2 (published work of Nicolas and Serre)

II. Galois representation on the Hecke algebra modulo 2 (published work of me)

III. Special modular forms modulo 2 (work in progress of Nicolas, Serre, and me)

IV. Density of modular forms modulo 2 (work in progress of me)
Outline

I. Modular forms and Hecke algebra modulo 2 (published work of Nicolas and Serre)

II. Galois representation on the Hecke algebra modulo 2 (published work of me)

III. Special modular forms modulo 2 (work in progress of Nicolas, Serre, and me)
Outline

I. Modular forms and Hecke algebra modulo 2 (published work of Nicolas and Serre)

II. Galois representation on the Hecke algebra modulo 2 (published work of me)

III. Special modular forms modulo 2 (work in progress of Nicolas, Serre, and me)

IV. Density of modular forms modulo 2 (work in progress of me)
Part I.

Modular forms and Hecke algebra modulo 2

(after Jean-Louis Nicolas, Jean-Pierre Serre)
Modular forms

A *modular form* of weight $k$ (and level 1) is an analytic function on $\{q \in \mathbb{C}, |q - 1| < 1\}$,

$$ f(q) = \sum_{n=0}^{\infty} a_n q^n \in \mathbb{C}[[q]] $$

such that, setting $q = e^{2i\pi z}$, one has

$$ f(-1/z) = z^k f(z) $$

Examples:

$$ \Delta(q) = q \prod_{n \geq 1} (1 - q^n)^24 = \sum_{n=1}^{\infty} \tau(n) q^n. $$

$$ \Delta_k(q) = \sum_{n=k}^{\infty} \tau_k(n) q^n. $$
Modular forms

A modular form of weight $k$ (and level 1) is an analytic function on
$\{ q \in \mathbb{C}, |q - 1| < 1 \}$,

$$f(q) = \sum_{n=0}^{\infty} a_n q^n \in \mathbb{C}[[q]]$$

such that, setting $q = e^{2i\pi z}$, one has

$$f(-1/z) = z^k f(z)$$

Examples:

$$\Delta(q) = q \prod_{n \geq 1} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n.$$
Modular forms

A modular form of weight $k$ (and level 1) is an analytic function on \( \{ q \in \mathbb{C}, |q - 1| < 1 \} \),

\[
f(q) = \sum_{n=0}^{\infty} a_n q^n \in \mathbb{C}[[q]]
\]

such that, setting \( q = e^{2i\pi z} \), one has

\[
f(-1/z) = z^k f(z)
\]

Examples:

\[
\Delta(q) = q \prod_{n \geq 1} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n.
\]

\[
\Delta^k(q) = \sum_{n=k}^{\infty} \tau_k(n) q^n.
\]
The space $M$ of modular forms modulo 2

If $f(q) = \sum_{n=0}^{\infty} a_n q^n \in \mathbb{Z}[[q]]$ is a modular form, define

$$\tilde{f} = \sum \bar{a}_n q^n \in \mathbb{F}_2[[q]].$$

Example (Jacobi): $\tilde{\Delta} = 1 + q^9 + q^{25} + q^{49} + \cdots$

Fact (Swinnerton-Dyer): the subspace of $\mathbb{F}_2[[q]]$ generated by $\tilde{f}$ for all modular forms $f \in \mathbb{Z}[[q]]$ is $\mathbb{F}_2[\tilde{\Delta}]$.

Remark: if $f = \sum a_n q^n \in \mathbb{F}_2[[q]]$, then $f^2 = \sum a_n q^{2n}$ is not really new. Hence we only consider $\tilde{\Delta}_k$ with $k$ odd. We define, for every odd integer $k$,

$$M_k = \mathbb{F}_2[\tilde{\Delta}] \oplus \mathbb{F}_2[\tilde{\Delta}_{3}] \oplus \cdots \oplus \mathbb{F}_2[\tilde{\Delta}_{k}],$$

$$M = \bigcup_{k \geq 1} M_k$$

The space $M$ will be the main object of this talk.
The space $M$ of modular forms modulo 2

If $f(q) = \sum_{n=0}^{\infty} a_n q^n \in \mathbb{Z}[[q]]$ is a modular form, define

$$\tilde{f} = \sum \bar{a}_n q^n \in \mathbb{F}_2[[q]].$$

Example (Jacobi): $\tilde{\Delta} = \sum_{n \text{ odd}} q^{n^2} = 1 + q^9 + q^{25} + q^{49} + \ldots$
The space $M$ of modular forms modulo 2

If $f(q) = \sum_{n=0}^{\infty} a_n q^n \in \mathbb{Z}[[q]]$ is a modular form, define

$$\tilde{f} = \sum \tilde{a}_n q^n \in \mathbb{F}_2[[q]].$$

Example (Jacobi): $\tilde{\Delta} = \sum_{n \text{ odd}} q^{n^2} = 1 + q^9 + q^{25} + q^{49} + \ldots$

Fact (Swinnerton-Dyer): the subspace of $\mathbb{F}_2[[q]]$ generated by $\tilde{f}$ for all modular forms $f \in \mathbb{Z}[[q]]$ is $\mathbb{F}_2[\tilde{\Delta}].$
The space $M$ of modular forms modulo 2

If $f(q) = \sum_{n=0}^{\infty} a_n q^n \in \mathbb{Z}[[q]]$ is a modular form, define

$$\tilde{f} = \sum \bar{a}_n q^n \in \mathbb{F}_2[[q]].$$

Example (Jacobi): $\tilde{\Delta} = \sum_{n \text{ odd}} q^{n^2} = 1 + q^9 + q^{25} + q^{49} + \ldots$

Fact (Swinnerton-Dyer): the subspace of $\mathbb{F}_2[[q]]$ generated by $\tilde{f}$ for all modular forms $f \in \mathbb{Z}[[q]]$ is $\mathbb{F}_2[\tilde{\Delta}]$.

Remark: if $f = \sum a_n q^n \in \mathbb{F}_2[[q]]$, then $f^2 = \sum a_n q^{2n}$ is not really new. Hence we only consider $\tilde{\Delta}^k$ with $k$ odd. We define, for every odd integer $k$,
The space $M$ of modular forms modulo 2

If $f(q) = \sum_{n=0}^{\infty} a_n q^n \in \mathbb{Z}[[q]]$ is a modular form, define

$$\tilde{f} = \sum \tilde{a}_n q^n \in \mathbb{F}_2[[q]].$$

Example (Jacobi): $\tilde{\Delta} = \sum_{n \text{ odd}} q^{n^2} = 1 + q^9 + q^{25} + q^{49} + \ldots$

Fact (Swinnerton-Dyer): the subspace of $\mathbb{F}_2[[q]]$ generated by $\tilde{f}$ for all modular forms $f \in \mathbb{Z}[[q]]$ is $\mathbb{F}_2[\tilde{\Delta}]$.

Remark: if $f = \sum a_n q^n \in \mathbb{F}_2[[q]]$, then $f^2 = \sum a_n q^{2n}$ is not really new. Hence we only consider $\tilde{\Delta}^k$ with $k$ odd. We define, for every odd integer $k$,

$$M_k = \mathbb{F}_2 \tilde{\Delta} \oplus \mathbb{F}_2 \tilde{\Delta}^3 \oplus \cdots \oplus \tilde{\Delta}^k, \quad M = \bigcup_{k \geq 1, k \text{ odd}} M_k$$

The space $M$ will be the main object of this talk.
Motivation

The study of $M$ will give informations on the parity of many arithmetic functions, including:

▶ the generalized Ramanujan functions $\tau_k(n)$;

▶ the number $r_q(n)$ of representations of $n$ by a certain type of quadratic form $q$ (for example, $\tilde{\Delta}_{9} = \tilde{\Delta}_{8} \tilde{\Delta} = \sum a, b, \text{odd} q_8^a a^2 + b^2$, hence the coefficient $a_p$ of $\tilde{\Delta}_9$ is 1 if and only if $p \equiv 1 \pmod{8}$ and $n$ is not represented by $a^2 + 32b^2$).

▶ More indirectly, and speculatively, the partition function $p(n)$, which is conjectured to be odd or even half of the time in average.
Motivation

The study of $M$ will give informations on the parity of many arithmetic functions, including:

▶ the generalized Ramanujan functions $\tau_k(n)$;

▶ the number $r_q(n)$ of representations of $n$ by a certain type of quadratic form $q$ (for example, $\tilde{\Delta}_9 = \tilde{\Delta}_8 \tilde{\Delta} = \sum a, b$, odd $q^8 a^2 + b^2$ hence the coefficient $a_p$ of $\tilde{\Delta}_9$ is 1 if and only if $p \equiv 1 \pmod{8}$ and $n$ is not represented by $a^2 + 32 b^2$.)

▶ More indirectly, and speculatively, the partition function $p(n)$, which is conjectured to be odd or even half of the time in average.
Motivation

The study of $M$ will give informations on the parity of many arithmetic functions, including:

- the generalized Ramanujan functions $\tau_k(n)$;
- the number $r_q(n)$ of representations of $n$ by a certain type of quadratic form $q$;
The study of $M$ will give informations on the parity of many arithmetic functions, including:

- the generalized Ramanujan functions $\tau_k(n)$;
- the number $r_q(n)$ of representations of $n$ by a certain type of quadratic form $q$; (for example, 

\[ \tilde{\Delta}^9 = \tilde{\Delta}^8 \tilde{\Delta} = \sum_{a,b, \text{ odd}} q^{8a^2 + b^2} \]
Motivation

The study of $M$ will give informations on the parity of many arithmetic functions, including:

- the generalized Ramanujan functions $\tau_k(n)$;
- the number $r_q(n)$ of representations of $n$ by a a certain type of quadratic form $q$; (for example,

$$\tilde{\Delta}^9 = \tilde{\Delta}^8 \tilde{\Delta} = \sum_{a,b, \text{ odd}} q^{8a^2+b^2}$$

hence the coefficient $a_p$ of $\tilde{\Delta}^9$ is 1 if and only if $p \equiv 1 \pmod{8}$ and $n$ is not represented by $a^2 + 32b^2$.)
Motivation

The study of $M$ will give informations on the parity of many arithmetic functions, including:

- the generalized Ramanujan functions $\tau_k(n)$;
- the number $r_q(n)$ of representations of $n$ by a certain type of quadratic form $q$; (for example, 
  \[ \tilde{\Delta}^9 = \tilde{\Delta}^8 \tilde{\Delta} = \sum_{a,b, \text{ odd}} q^{8a^2+b^2} \]
  hence the coefficient $a_p$ of $\tilde{\Delta}^9$ is 1 if and only if $p \equiv 1 \pmod{8}$ and $n$ is not represented by $a^2 + 32b^2$.)
- More indirectly, and speculatively, the partition function $p(n)$, which is conjectured to be odd or even half of the time in average.
Hecke operators and the Hecke algebra $A$

For every prime $\ell$, the Hecke operator $T_\ell$ on $\mathbb{F}_2[[q]]$ is defined by

$$T_\ell \left( \sum a_n q^n \right) = \sum a_n q^{n\ell} + \ell \sum a_n \ell q^n,$$

The $T_\ell$'s stabilize $M_k$ and $M_{k+2}$. Let $A_k$ be the subalgebra of $\text{End}_{\mathbb{F}_2[[q]]}(M_k)$ generated by the Hecke operators $T_\ell$ for $\ell$ odd prime. The inclusion $M_k \subset M_{k+2}$ induces a surjective morphism $A_{k+2} \to A_k$. Set $A = \varprojlim A_k$. $A$ is called the Hecke algebra of modular forms modulo 2, and our main tool to study $M_k$, which is an $A$-module.
For every prime $\ell$, the Hecke operator $T_{\ell}$ on $\mathbb{F}_2[[q]]$ is defined by

$$T_{\ell}(\sum a_n q^n) = \sum a_n q^{n\ell} + \ell \sum a_{n\ell} q^n,$$

The $T_{\ell}$’s stabilize $M_k$ and $M$. 

Hecke operators and the Hecke algebra $A$
For every prime $\ell$, the Hecke operator $T_\ell$ on $\mathbb{F}_2[[q]]$ is defined by

$$T_\ell\left(\sum a_nq^n\right) = \sum a_nq^{n\ell} + \ell \sum a_n\ell q^n,$$

The $T_\ell$'s stabilize $M_k$ and $M$. Let $A_k$ be the subalgebra of $\text{End}_{\mathbb{F}_2}(M_k)$ generated by the Hecke operators $T_\ell$ for $\ell$ odd prime.
Hecke operators and the Hecke algebra $A$

For every prime $\ell$, the Hecke operator $T_\ell$ on $\mathbb{F}_2[[q]]$ is defined by

$$T_\ell(\sum a_n q^n) = \sum a_n q^{n\ell} + \ell \sum a_n \ell q^n,$$

The $T_\ell$’s stabilize $M_k$ and $M$. Let $A_k$ be the subalgebra of $\text{End}_{\mathbb{F}_2}(M_k)$ generated by the Hecke operators $T_\ell$ for $\ell$ odd prime. The inclusion $M_k \subset M_{k+2}$ induces a surjective morphism $A_{k+2} \rightarrow A_k$. 

For every prime $\ell$, the Hecke operator $T_\ell$ on $\mathbb{F}_2[[q]]$ is defined by

$$T_\ell(\sum a_nq^n) = \sum a_nq^{n\ell} + \ell \sum a_{n\ell}q^n,$$

The $T_\ell$’s stabilize $M_k$ and $M$. Let $A_k$ be the subalgebra of $\text{End}_{\mathbb{F}_2}(M_k)$ generated by the Hecke operators $T_\ell$ for $\ell$ odd prime. The inclusion $M_k \subset M_{k+2}$ induces a surjective morphism $A_{k+2} \rightarrow A_k$.

Set

$$A = \lim_{\leftarrow} A_k.$$

$A$ is called the Hecke algebra of modular forms modulo 2, and our main tool to study $M$, which is an $A$-module.
For every prime $\ell$, the Hecke operator $T_\ell$ on $\mathbb{F}_2[[q]]$ is defined by

$$T_\ell\left(\sum a_n q^n\right) = \sum a_n q^{n\ell} + \ell \sum a_n \ell q^n,$$

The $T_\ell$’s stabilize $M_k$ and $M$. Let $A_k$ be the subalgebra of $\text{End}_{\mathbb{F}_2}(M_k)$ generated by the Hecke operators $T_\ell$ for $\ell$ odd prime. The inclusion $M_k \subset M_{k+2}$ induces a surjective morphism $A_{k+2} \to A_k$.

Set

$$A = \lim_{\leftarrow} A_k.$$

$A$ is called the Hecke algebra of modular forms modulo 2, and our main tool to study $M$, which is an $A$-module.
What is the structure of the Hecke algebra $A$?

Three easy facts known in the late 1960’s
1. – There is only one semi-simple Galois representation $G_{\mathbb{Q}}$, $2 \to \text{GL}_2(\mathbb{F}_2)$, namely $1 \oplus 1$ (trace: 0).
2. – Consequence (Deligne): $T_\ell$ is nilpotent on $M_k$.
3. – Consequence: the algebra $A$ is a complete local ring, with the $T_\ell$ in its maximal ideal $m_A$.

Theorem (Nicolas-Serre, 2010-2012) $A = \mathbb{F}_2[[x, y]]$ where $x = T_3$, $y = T_5$. Hence $A$ is a noetherian complete regular local ring of dimension 2.

We can also take $x = T_\ell$, $\ell \equiv 3 \pmod{8}$, $y = T_\ell'$, $\ell' \equiv 5 \pmod{8}$.

Remark: same is true with 2 replaced by $p > 2$ (joint work with Khare).
What is the structure of the Hecke algebra $A$?

Three easy facts known in the late 1960’s

1.– There is only one semi-simple Galois representation $\text{Gal}_Q \to \text{GL}_2(F_2)$, namely $1 \oplus 1$ (trace: 0).
What is the structure of the Hecke algebra \( A \)?

Three easy facts known in the late 1960’s

1.– There is only one semi-simple Galois representation \( G_{\mathbb{Q},2} \to \text{GL}_2(\mathbb{F}_2) \), namely \( 1 \oplus 1 \) (trace: 0).

2.– Consequence (Deligne): \( T_\ell \) is nilpotent on \( M_k \).

3.– Consequence: the algebra \( A \) is a complete local ring, with the \( T_\ell \) in its maximal ideal \( m_A \).

Theorem (Nicolas-Serre, 2010-2012) \( A = \mathbb{F}_2[[x,y]] \) where \( x = T_3 \), \( y = T_5 \). Hence \( A \) is a noetherian complete regular local ring of dimension 2.

We can also take \( x = T_\ell \), \( \ell \equiv 3 \pmod{8} \), \( y = T_\ell' \), \( \ell' \equiv 5 \pmod{8} \).

Remark: same is true with 2 replaced by \( p > 2 \) (joint work with Khare).
What is the structure of the Hecke algebra $A$?

Three easy facts known in the late 1960’s

1.– There is only one semi-simple Galois representation $G_{\mathbb{Q},2} \to \text{GL}_2(\mathbb{F}_2)$, namely $1 \oplus 1$ (trace: 0).

2.– Consequence (Deligne): $T_\ell$ is nilpotent on $M_k$.

3.– Consequence: the algebra $A$ is a complete local ring, with the $T_\ell$ in its maximal ideal $m_A$.

**Theorem (Nicolas-Serre, 2010-2012)**

$A = \mathbb{F}_2[[x,y]]$ where $x = T_3$, $y = T_5$. Hence $A$ is a noetherian complete regular local ring of dimension 2.

We can also take $x = T_\ell$, $\ell \equiv 3 \pmod{8}$, $y = T_\ell'$, $\ell' \equiv 5 \pmod{8}$.

Remark: same is true with 2 replaced by $p > 2$ (joint work with Khare).
What is the structure of the Hecke algebra $A$?

Three easy facts known in the late 1960’s

1.– There is only one semi-simple Galois representation $G_{Q,2} \to \text{GL}_2(\mathbb{F}_2)$, namely $1 \oplus 1$ (trace: 0).

2.– Consequence (Deligne): $T_\ell$ is nilpotent on $M_k$.

3.– Consequence: the algebra $A$ is a complete local ring, with the $T_\ell$ in its maximal ideal $m_A$.

Theorem (Nicolas-Serre, 2010-2012)

$A = \mathbb{F}_2[[x, y]]$ where $x = T_3$, $y = T_5$. Hence $A$ is a noetherian complete regular local ring of dimension 2.
What is the structure of the Hecke algebra $A$?

Three easy facts known in the late 1960’s

1.– There is only one semi-simple Galois representation $G_{Q,2} \to \text{GL}_2(F_2)$, namely $1 \oplus 1$ (trace: 0).

2.– Consequence (Deligne): $T_\ell$ is nilpotent on $M_k$.

3.– Consequence: the algebra $A$ is a complete local ring, with the $T_\ell$ in its maximal ideal $m_A$.

Theorem (Nicolas-Serre, 2010-2012)

$A = F_2[[x,y]]$ where $x = T_3$, $y = T_5$. Hence $A$ is a noetherien complete regular local ring of dimension 2.

We can also take $x = T_\ell$, $\ell \equiv 3 \, (\text{mod } 8)$, $y = T_{\ell'}$, $\ell' \equiv 5 \, (\text{mod } 8)$. 

What is the structure of the Hecke algebra $A$?

Three easy facts known in the late 1960’s

1.– There is only one semi-simple Galois representation $G_{\mathbb{Q}, 2} \to \text{GL}_2(\mathbb{F}_2)$, namely $1 \oplus 1$ (trace: 0).

2.– Consequence (Deligne): $T_\ell$ is nilpotent on $M_k$.

3.– Consequence: the algebra $A$ is a complete local ring, with the $T_\ell$ in its maximal ideal $m_A$.

Theorem (Nicolas-Serre, 2010-2012)

$A = \mathbb{F}_2[[x, y]]$ where $x = T_3$, $y = T_5$. Hence $A$ is a noetherian complete regular local ring of dimension 2.

We can also take $x = T_\ell$, $\ell \equiv 3 \pmod{8}$, $y = T_{\ell'}$, $\ell' \equiv 5 \pmod{8}$. Their proof is hard, very long, completely elementary.
What is the structure of the Hecke algebra $A$?

Three easy facts known in the late 1960's

1.– There is only one semi-simple Galois representation $G_{\mathbb{Q},2} \to \text{GL}_2(\mathbb{F}_2)$, namely $1 \oplus 1$ (trace: 0).

2.– Consequence (Deligne): $T_\ell$ is nilpotent on $M_k$.

3.– Consequence: the algebra $A$ is a complete local ring, with the $T_\ell$ in its maximal ideal $m_A$.

Theorem (Nicolas-Serre, 2010-2012)

$A = \mathbb{F}_2[[x,y]]$ where $x = T_3$, $y = T_5$. Hence $A$ is a noetherian complete regular local ring of dimension 2.

We can also take $x = T_\ell$, $\ell \equiv 3 \pmod{8}$, $y = T_{\ell'}$, $\ell' \equiv 5 \pmod{8}$. Their proof is hard, very long, completely elementary.

Remark: same is true with 2 replaced by $p > 2$ (joint work with Khare).
What is the structure of the Hecke algebra $A$?

Three easy facts known in the late 1960’s

1.– There is only one semi-simple Galois representation $G_{\mathbb{Q},2} \to \text{GL}_2(\mathbb{F}_2)$, namely $1 \oplus 1$ (trace: 0).

2.– Consequence (Deligne): $T_\ell$ is nilpotent on $M_k$.

3.– Consequence: the algebra $A$ is a complete local ring, with the $T_\ell$ in its maximal ideal $m_A$.

Theorem (Nicolas-Serre, 2010-2012)

$A = \mathbb{F}_2[[x, y]]$ where $x = T_3$, $y = T_5$. Hence $A$ is a noetherian complete regular local ring of dimension 2.

We can also take $x = T_\ell$, $\ell \equiv 3 \pmod{8}$, $y = T_{\ell'}$, $\ell' \equiv 5 \pmod{8}$. Their proof is hard, very long, completely elementary.

Remark: same is true with 2 replaced by $p > 2$ (joint work with Khare).
What are the consequences for the structure of $M$?

The $A$-module $M$ is the dualizing module of $A$. 
What are the consequences for the structure of $M$?

The $A$-module $M$ is the dualizing module of $A$. Hence,

**Corollary**

*There exists a unique basis $m(a, b)_{a \geq 0, b \geq 0}$ of $M$ such that:*

\[ m(0, 0) = \tilde{\Delta}, \quad T_3 m(a, b) = m(a - 1, b) \text{ if } a > 0, \quad T_5 m(a, b) = m(a, b - 1) \text{ if } b > 0, \quad \text{and } T_5 m(a, 0) = 0. \]

The first coefficient $a_1$ of $m(a, b)$ is 0 except if $a = b = 0$. Such a basis is called an adapted basis (for $X = T_3$ and $Y = T_5$).
What are the consequences for the structure of $M$?

The $A$-module $M$ is the dualizing module of $A$. Hence, 

**Corollary**

*There exists a unique basis $m(a, b)_{a \geq 0, b \geq 0}$ of $M$ such that:*

- $m(0, 0) = \tilde{\Delta}$
What are the consequences for the structure of $M$?

The $A$-module $M$ is the dualizing module of $A$. Hence,

**Corollary**

*There exists a unique basis $m(a, b)_{a \geq 0, b \geq 0}$ of $M$ such that:*

- $m(0, 0) = \tilde{\Delta}$
- $T_3 m(a, b) = m(a - 1, b)$ if $a > 0$, and $T_3 m(0, b) = 0$. 
What are the consequences for the structure of $M$?

The $A$-module $M$ is the dualizing module of $A$. Hence,

**Corollary**

*There exists a unique basis $m(a, b)_{a \geq 0, b \geq 0}$ of $M$ such that:*

- $m(0, 0) = \tilde{\Delta}$
- $T_3 m(a, b) = m(a - 1, b)$ if $a > 0$, and $T_3 m(0, b) = 0$.
- $T_5 m(a, b) = m(a, b - 1)$ if $b > 0$, and $T_5 m(a, 0) = 0$. 
What are the consequences for the structure of $M$?

The $A$-module $M$ is the dualizing module of $A$. Hence,

Corollary

There exists a unique basis $m(a, b)_{a \geq 0, b \geq 0}$ of $M$ such that:

- $m(0, 0) = \tilde{\Delta}$
- $T_3 m(a, b) = m(a - 1, b)$ if $a > 0$, and $T_3 m(0, b) = 0$.
- $T_5 m(a, b) = m(a, b - 1)$ if $b > 0$, and $T_5 m(a, 0) = 0$.
- The first coefficient $a_1$ of $m(a, b)$ is 0 except if $a = b = 0$. 
What are the consequences for the structure of $M$?

The $A$-module $M$ is the dualizing module of $A$. Hence,

Corollary

There exists a unique basis $m(a, b)_{a \geq 0, b \geq 0}$ of $M$ such that:

- $m(0, 0) = \tilde{\Delta}$
- $T_3 m(a, b) = m(a - 1, b)$ if $a > 0$, and $T_3 m(0, b) = 0$.
- $T_5 m(a, b) = m(a, b - 1)$ if $b > 0$, and $T_5 m(a, 0) = 0$.
- the first coefficient $a_1$ of $m(a, b)$ is 0 except if $a = b = 0$.

Such a basis is called an adapted basis (for $X = T_3$ and $Y = T_5$)
More structure: a simple grading by \((\mathbb{Z}/8\mathbb{Z})^*\)

Grading of \(M\): for \(i \in (\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}\), let \(M^i \subset M\) generated by the \(\tilde{\Delta}^k, k \equiv i \pmod{8}\).
More structure: a simple grading by \((\mathbb{Z}/8\mathbb{Z})^*\)

Grading of \(M\): for \(i \in (\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}\), let \(M^i \subset M\) generated by the \(\tilde{\Delta}^k\), \(k \equiv i \pmod{8}\).

\[
M^i = \{ f = \sum a_n q^n \in M, \quad a_n = 1 \Rightarrow n \equiv i \pmod{8} \}.
\]

\[
M = M^1 \oplus M^3 \oplus M^5 \oplus M^7.
\]
More structure: a simple grading by \((\mathbb{Z}/8\mathbb{Z})^*\)

Grading of \(M\): for \(i \in (\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}\), let \(M^i \subset M\) generated by the \(\tilde{\Delta}^k\), \(k \equiv i\) (mod 8).

\[ M^i = \{ f = \sum a_n q^n \in M, \quad a_n = 1 \Rightarrow n \equiv i \pmod{8} \}. \]

\[ M = M^1 \oplus M^3 \oplus M^5 \oplus M^7. \]

Also, let \(A^1 = \mathbb{F}_2[[x^2, y^2]]\), \(A^3 = xA^1\), \(A^5 = yA^1\), \(A^7 = xyA^1\). Then

\[ A = A^1 \oplus A^3 \oplus A^5 \oplus A^7, \]

\(A\) is a graded algebra and \(M\) a graded \(A\)-module.
More structure: a simple grading by \((\mathbb{Z}/8\mathbb{Z})^*\)

Grading of \(M\): for \(i \in (\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}\), let \(M^i \subset M\) generated by the \(\tilde{\Delta}^k\), \(k \equiv i \pmod{8}\).

\[
M^i = \{ f = \sum a_n q^n \in M, \quad a_n = 1 \Rightarrow n \equiv i \pmod{8} \}.
\]

\[
M = M^1 \oplus M^3 \oplus M^5 \oplus M^7.
\]

Also, let \(A^1 = \mathbb{F}_2[[x^2, y^2]], A^3 = xA^1, A^5 = yA^1, A^7 = xyA^1\). Then

\[
A = A^1 \oplus A^3 \oplus A^5 \oplus A^7,
\]

\(A\) is a graded algebra and \(M\) a graded \(A\)-module. That is

\[
A^i A^j \subset A^{ij}, \quad A^i M^j \subset M^{ij}.
\]
More structure: a simple grading by \((\mathbb{Z}/8\mathbb{Z})^*\)

Grading of \(M\): for \(i \in (\mathbb{Z}/8\mathbb{Z})^* = \{1, 3, 5, 7\}\), let \(M^i \subset M\) generated by the \(\tilde{\Delta}^k, k \equiv i \pmod{8}\).

\[
M^i = \{ f = \sum a_n q^n \in M, \quad a_n = 1 \Rightarrow n \equiv i \pmod{8}\}.
\]

\[
M = M^1 \oplus M^3 \oplus M^5 \oplus M^7.
\]

Also, let \(A^1 = \mathbb{F}_2[[x^2, y^2]], A^3 = xA^1, A^5 = yA^1, A^7 = xyA^1\). Then

\[
A = A^1 \oplus A^3 \oplus A^5 \oplus A^7,
\]

\(A\) is a graded algebra and \(M\) a graded \(A\)-module. That is

\[
A^i A^j \subset A^{ij}, \quad A^i M^j \subset M^{ij}.
\]

One has \(T_p \in A^{p\pmod{8}}\). The form \(m(a, b)\) is in \(M^{3a5b\pmod{8}}\).
Part II.

Galois representation on the Hecke algebra modulo 2
The universal Galois representation on $A$

Let $G$ be the maximal pro-2-quotient on $G_{\mathbb{Q},2}$.

**Theorem**

- There exists a unique continuous $r : G \rightarrow \text{GL}_2(A)$ such that $\text{tr } r(\text{Frob}_\ell) = T_\ell$ for $\ell \neq 2$. It is absolutely irreducible, and $\det r = 1$.  

- $r(\mod m_A) \cong \begin{pmatrix} 1 & \eta_0 & 1 \\ \eta \end{pmatrix}$, where $\eta$ is the character attached to $\mathbb{Q}(\sqrt{2})$.

- If $P$ is a prime of height 1, let $k(P) = \text{Frac}(A/P)$, $r_P : G \rightarrow \text{GL}_2(k(P))$. Then $r_P$ is irreducible for all $P$; absolutely irreducible for all $P$ but one: $P_0 = (x+y+x^3+x^5+x^9+x^{11}+x^{129}+...)$; strongly absolutely irreducible for all $P$ excepted $P_0$, $(x)$, $(y)$.

I'm going to explain the proof of the first point.
The universal Galois representation on $A$

Let $G$ be the maximal pro-$2$-quotient on $G_{\mathbb{Q},2}$.

**Theorem**

- There exists a unique continuous $r : G \rightarrow \text{GL}_2(A)$ such that $\text{tr} \ r(\text{Frob}_\ell) = T_\ell$ for $\ell \neq 2$. It is absolutely irreducible, and $\det r = 1$.

- $r \ (\text{mod } m_A) \cong \begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix}$,
The universal Galois representation on $A$

Let $G$ be the maximal pro-2-quotient on $G_{\mathbb{Q},2}$.

Theorem

- There exists a unique continuous $r: G \rightarrow \text{GL}_2(\mathbb{A})$ such that $\text{tr } r(\text{Frob}_\ell) = T_\ell$ for $\ell \neq 2$. It is absolutely irreducible, and $\det r = 1$.

- $r \pmod{m_A} \cong \begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix}$, where $\eta$ is the character attached to $\mathbb{Q}(\sqrt{2})$. 

I'm going to explain the proof of the first point.
The universal Galois representation on $A$

Let $G$ be the maximal pro-2-quotient on $G_{\mathbb{Q},2}$.

**Theorem**

- There exists a unique continuous $r : G \to \text{GL}_2(A)$ such that $\text{tr} \ r(\text{Frob}_\ell) = T_\ell$ for $\ell \neq 2$. It is absolutely irreducible, and $\det r = 1$.

- $r \ (\text{mod} \ m_A) \simeq \begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix}$, where $\eta$ is the character attached to $\mathbb{Q}(\sqrt{2})$.

- If $\mathcal{P}$ is a prime of height 1, let $k(\mathcal{P}) = \text{Frac}(A/\mathcal{P})$, $r_\mathcal{P} : G \to \text{GL}_2(k(\mathcal{P}))$. Then $r_\mathcal{P}$ is irreducible for all $\mathcal{P}$; absolutely irreducible for all $\mathcal{P}$ but one: $\mathcal{P}_0 = (x + y + x^3 + x^5 + x^9 + x^{11} + x^{12} + ...)$; strongly absolutely irreducible for all $\mathcal{P}$ excepted $\mathcal{P}_0$, $(x)$, $(y)$.
The universal Galois representation on $A$

Let $G$ be the maximal pro-$2$-quotient on $G_{Q,2}$.

**Theorem**

- There exists a unique continuous $r : G \to \text{GL}_2(A)$ such that $\text{tr} r(\text{Frob}_\ell) = T_\ell$ for $\ell \neq 2$. It is absolutely irreducible, and $\det r = 1$.
- $r \ (\text{mod} \ m_A) \simeq \begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix}$, where $\eta$ is the character attached to $Q(\sqrt{2})$.
- If $\mathcal{P}$ is a prime of height $1$, let $k(\mathcal{P}) = \text{Frac}(A/\mathcal{P})$, $r_\mathcal{P} : G \to \text{GL}_2(k(\mathcal{P}))$. Then $r_\mathcal{P}$ is
  - irreducible for all $\mathcal{P}$;
The universal Galois representation on $A$

Let $G$ be the maximal pro-2-quotient on $G_{\mathbb{Q},2}$.

**Theorem**

- There exists a unique continuous $r : G \to \text{GL}_2(A)$ such that $\text{tr} \ r(\text{Frob}_\ell) = T_\ell$ for $\ell \neq 2$. It is absolutely irreducible, and $\det r = 1$.
- $r \pmod{m_A} \simeq \begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix}$, where $\eta$ is the character attached to $\mathbb{Q}(\sqrt{2})$.
- If $\mathcal{P}$ is a prime of height 1, let $k(\mathcal{P}) = \text{Frac}(A/\mathcal{P})$, $r_\mathcal{P} : G \to \text{GL}_2(k(\mathcal{P}))$. Then $r_\mathcal{P}$ is
  - irreducible for all $\mathcal{P}$;
  - absolutely irreducible for all $\mathcal{P}$ but one: $\mathcal{P}_0 = (x + y + x^3 + x^5 + x^9 + x^{11} + x^{129} + \ldots)$;
The universal Galois representation on $A$

Let $G$ be the maximal pro-2-quotient on $G_{\mathbb{Q},2}$.

**Theorem**

- There exists a unique continuous $r : G \to \text{GL}_2(A)$ such that $\text{tr} \ r(\text{Frob}_\ell) = T_\ell$ for $\ell \neq 2$. It is absolutely irreducible, and $\det r = 1$.

- $r \pmod{m_A} \simeq \begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix}$, where $\eta$ is the character attached to $\mathbb{Q}(\sqrt{2})$.

- If $\mathcal{P}$ is a prime of height 1, let $k(\mathcal{P}) = \text{Frac}(A/\mathcal{P})$, $r_\mathcal{P} : G \to \text{GL}_2(k(\mathcal{P}))$. Then $r_\mathcal{P}$ is
  - irreducible for all $\mathcal{P}$;
  - absolutely irreducible for all $\mathcal{P}$ but one: $\mathcal{P}_0 = (x + y + x^3 + x^5 + x^9 + x^{11} + x^{129} + \ldots)$;
  - strongly absolutely irreducible for all $\mathcal{P}$ excepted $\mathcal{P}_0$, $(x)$, $(y)$. 

I'm going to explain the proof of the first point.
The universal Galois representation on $A$

Let $G$ be the maximal pro-2-quotient on $G_{\mathbb{Q},2}$.

**Theorem**

- There exists a unique continuous $r : G \to \text{GL}_2(A)$ such that $	ext{tr} \ r(\text{Frob}_\ell) = T_\ell$ for $\ell \neq 2$. It is absolutely irreducible, and $\det r = 1$.

- $r \pmod{m_A} \simeq \begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix}$, where $\eta$ is the character attached to $\mathbb{Q}(\sqrt{2})$.

- If $P$ is a prime of height 1, let $k(P) = \text{Frac}(A/P)$, $r_P : G \to \text{GL}_2(k(P))$. Then $r_P$ is
  - irreducible for all $P$;
  - absolutely irreducible for all $P$ but one:
    $P_0 = (x + y + x^3 + x^5 + x^9 + x^{11} + x^{129} + \ldots)$;
  - strongly absolutely irreducible for all $P$ excepted $P_0$, $(x)$, $(y)$.

I’m going to explain the proof of the first point.
Chenevier’s pseudorepresentations

Traditional pseudorepresentations (Taylor, Rouquier) work only in characteristic greater than the dimension.

Let $A$ be a commutative ring, $G$ a group. A pseudorepresentation of $G$ on $A$ is a pair $(t, d)$ of applications from $G$ to $A$ such that:

(i) $d: G \rightarrow A^\ast$ is a group morphism.

(ii) $t(1) = 2$.

(iii) $t(gh) = t(hg)$.

(iv) $t(gh) + d(h) \cdot t(gh^{-1}) = t(g) \cdot t(h)$. 

Chenevier’s pseudorepresentations

Traditional pseudorepresentations (Taylor, Rouquier) work only in characteristic greater than the dimension. Chenevier’s pseudorepresentation always work.
Chenevier’s pseudorepresentations

Traditional pseudorepresentations (Taylor, Rouquier) work only in characteristic greater than the dimension. Chenevier’s pseudorepresentation always work but are much more complicated to define.
Chenevier’s pseudorepresentations

Traditional pseudorepresentations (Taylor, Rouquier) work only in characteristic greater than the dimension. Chenevier’s pseudorepresentation always work but are much more complicated to define. I will only define them in dimension 2.
Chenevier’s pseudorepresentations

Traditional pseudorepresentations (Taylor, Rouquier) work only in characteristic greater than the dimension. Chenevier’s pseudorepresentation always work but are much more complicated to define. I will only define them in dimension 2.

Let $A$ be a commutative ring, $G$ a group.
Chenevier’s pseudorepresentations

Traditional pseudorepresentations (Taylor, Rouquier) work only in characteristic greater than the dimension. Chenevier’s pseudorepresentation always work but are much more complicated to define. I will only define them in dimension 2.

Let $A$ be a commutative ring, $G$ a group. A pseudorepresentation of $G$ on $A$ is a pair $(t, d)$ of applications from $G$ to $A$ such that:

(i) $d : G \rightarrow A^*$ is a group morphism.

(ii) $t(1) = 2$.

(iii) $t(gh) = t(hg)$.

(iv) $t(gh) + d(h)t(gh^{-1}) = t(g)t(h)$. 
Facts about Chenevier’s pseudorepresentations

- If $r : G \to \text{GL}_2(A)$ is a representation, $(\text{tr } r, \det r)$ is a pseudo-representation.
Facts about Chenevier’s pseudorepresentations

- If $r : G \to \text{GL}_2(A)$ is a representation, $(\text{tr } r, \text{det } r)$ is a pseudo-representation.
- If $K$ is an algebraically closed field, any pseudorepresentation $(t, d)$ of $G$ to $K$ is $(\text{tr } r, \text{det } r)$ for a unique semi-simple representation $r : G \to \text{GL}_2(K)$. 
Facts about Chenevier’s pseudorepresentations

- If $r : G \to \text{GL}_2(A)$ is a representation, $(\text{tr } r, \text{det } r)$ is a pseudo-representation.
- If $K$ is an algebraically closed field, any pseudorepresentation $(t, d)$ of $G$ to $K$ is $(\text{tr } r, \text{det } r)$ for a unique semi-simple representation $r : G \to \text{GL}_2(K)$.
- If $B$ is a subring of $A$, $(t, d)$ pseudorepresentation of $G$ to $A$ such that $t(G) \subset B$, $d(G) \subset B^*$, then $(t, g)$ is a pseudorepresentation on $G$ to $B$. (”pseudorepresentations descend and glue well”).
Facts about Chenevier’s pseudorepresentations

- If $r : G \to \text{GL}_2(A)$ is a representation, $(\text{tr } r, \det r)$ is a pseudo-representation.

- If $K$ is an algebraically closed field, any pseudorepresentation $(t, d)$ of $G$ to $K$ is $(\text{tr } r, \det r)$ for a unique semi-simple representation $r : G \to \text{GL}_2(K)$.

- If $B$ is a subring of $A$, $(t, d)$ pseudorepresentation of $G$ to $A$ such that $t(G) \subset B$, $d(G) \subset B^*$, then $(t, g)$ is a pseudorepresentation on $G$ to $B$. (”pseudorepresentations descend and glue well”)

Proof of the existence of the representation $r$

**Step 1** Construct a continuous pseudorepresentation $(t, d): G \to A$ such that $t(\text{Frob}_p) = T_p$, $d = 1$. One glues Deligne’s representations attached to eigenforms of level 1 in characteristic 0 and reduces modulo 2.
Proof of the existence of the representation $r$

**Step 1** Construct a continuous pseudorepresentation $(t, d) : G \to A$ such that $t(Frob_p) = T_p$, $d = 1$. One glues Deligne’s representations attached to eigenforms of level 1 in characteristic 0 and reduces modulo 2.

**Step 2** Let $K = \text{Frac}(A)$, $\bar{K} = \text{alg. closure of } K$. By Chenevier’s theorem, there exists $r : G \to \text{SL}_2(\bar{K})$, such that $\text{tr } r(Frob_p) = T_p$. (Remark: I don’t claim that $r$ is continuous)
Proof of the existence of the representation $r$

**Step 1** Construct a continuous pseudorepresentation $(t, d) : G \to A$ such that $t(Frob_p) = T_p$, $d = 1$. One glues Deligne’s representations attached to eigenforms of level 1 in characteristic 0 and reduces modulo 2.

**Step 2** Let $K = \text{Frac}(A)$, $\bar{K} = \text{alg. closure of } K$. By Chenevier’s theorem, there exists $r : G \to \text{SL}_2(\bar{K})$, such that $\text{tr } r(Frob_p) = T_p$. (Remark: I don’t claim that $r$ is continuous)

**Step 3** Claim: $r$ is (absolutely) irreducible.
Proof of the existence of the representation $r$

**Step 1** Construct a continuous pseudorepresentation $(t, d) : G \to A$ such that $t(Frob_p) = T_p$, $d = 1$. One glues Deligne’s representations attached to eigenforms of level 1 in characteristic 0 and reduces modulo 2.

**Step 2** Let $K = \text{Frac}(A)$, $\bar{K}$ = alg. closure of $K$. By Chenevier’s theorem, there exists $r : G \to \text{SL}_2(\bar{K})$, such that $\text{tr} \ r(Frob_p) = T_p$. (Remark: I don’t claim that $r$ is continuous)

**Step 3** Claim: $r$ is (absolutely) irreducible. If not, $r$, hence $t = \text{tr} \ r$ factors through $G^{ab}$. 

Proof of the existence of the representation \( r \)

**Step 1** Construct a continuous pseudorepresentation \((t, d) : G \to A\) such that \(t(\text{Frob}_p) = T_p, \ d = 1\). One glues Deligne’s representations attached to eigenforms of level 1 in characteristic 0 and reduces modulo 2.

**Step 2** Let \( K = \text{Frac}(A), \ \tilde{K} = \text{alg. closure of} \ K\). By Chenevier’s theorem, there exists \( r : G \to \text{SL}_2(\tilde{K})\), such that \(\text{tr} \ r(\text{Frob}_p) = T_p\). (Remark: I don’t claim that \( r \) is continuous)

**Step 3** Claim: \( r \) is (absolutely) irreducible. If not, \( r \), hence \( t = \text{tr} \ r \) factors through \( G^{ab} \). Therefore for any integer \( k \), \( t(\text{Frob}_p) = T_p \) in \( A_k \subset \text{End}(M_k) \) depends only on \( \text{Frob}_p \) in a finite abelian extension of \( \mathbb{Q} \) unramified outside 2.
Proof of the existence of the representation $r$

**Step 1** Construct a continuous pseudorepresentation $(t, d): G \to A$ such that $t(Frob_p) = T_p$, $d = 1$. One glues Deligne’s representations attached to eigenforms of level 1 in characteristic 0 and reduces modulo 2.

**Step 2** Let $K = \text{Frac}(A)$, $\bar{K} = \text{alg. closure of } K$. By Chenevier’s theorem, there exists $r: G \to \text{SL}_2(\bar{K})$, such that $\text{tr } r(Frob_p) = T_p$. (Remark: I don’t claim that $r$ is continuous)

**Step 3** Claim: $r$ is (absolutely) irreducible. If not, $r$, hence $t = \text{tr } r$ factors through $G^{ab}$. Therefore for any integer $k$, $t(Frob_p) = T_p$ in $A_k \subset \text{End}(M_k)$ depends only on $Frob_p$ in a finite abelian extension of $\mathbb{Q}$ unramified outside 2. But for $k = 9$,
Proof of the existence of the representation $r$

**Step 1** Construct a continuous pseudorepresentation $(t, d) : G \to A$ such that $t(Frob_p) = T_p$, $d = 1$. One glues Deligne’s representations attached to eigenforms of level 1 in characteristic 0 and reduces modulo 2.

**Step 2** Let $K = \text{Frac}(A)$, $\bar{K} = \text{alg. closure of } K$. By Chenevier’s theorem, there exists $r : G \to \text{SL}_2(\bar{K})$, such that $\text{tr} r(Frob_p) = T_p$. (Remark: I don’t claim that $r$ is continuous)

**Step 3** Claim: $r$ is (absolutely) irreducible. If not, $r$, hence $t = \text{tr} r$ factors through $G^{ab}$. Therefore for any integer $k$, $t(Frob_p) = T_p$ in $A_k \subset \text{End}(M_k)$ depends only on $Frob_p$ in a finite abelian extension of $\mathbb{Q}$ unramified outside 2. But for $k = 9$, $T_p\tilde{\Delta}^9 = \tilde{\Delta}$ if and only if $p \equiv 1 \pmod{8}$ and $p$ is not represented by $a^2 + 32b^2$, and this condition does not depend on $Frob_p$ in an abelian extension of $\mathbb{Q}$ (because 32 is not idoneal – Euler).
Proof of the existence of the representation $r$

**Step 1** Construct a continuous pseudorepresentation $(t, d) : G \to A$ such that $t(Frob_p) = T_p$, $d = 1$. One glues Deligne’s representations attached to eigenforms of level 1 in characteristic 0 and reduces modulo 2.

**Step 2** Let $K = \text{Frac}(A)$, $\bar{K} = \text{alg. closure of } K$. By Chenevier’s theorem, there exists $r : G \to \text{SL}_2(\bar{K})$, such that $\text{tr} r(Frob_p) = T_p$. (Remark: I don’t claim that $r$ is continuous)

**Step 3** Claim: $r$ is (absolutely) irreducible. If not, $r$, hence $t = \text{tr} r$ factors through $G^{\text{ab}}$. Therefore for any integer $k$, $t(Frob_p) = T_p$ in $A_k \subset \text{End}(M_k)$ depends only on $Frob_p$ in a finite abelian extension of $\mathbb{Q}$ unramified outside 2. But for $k = 9$, $T_p\tilde{\Delta}^9 = \tilde{\Delta}$ if and only if $p \equiv 1 \pmod{8}$ and $p$ is not represented by $a^2 + 32b^2$, and this condition does not depend on $Frob_p$ in an abelian extension of $\mathbb{Q}$ (because 32 is not idoneal – Euler). Contradiction.
Proof of the existence of the representation \( r \)

**Step 4** The representation \( r \) is defined over \( K \).
Proof of the existence of the representation $r$

**Step 4** The representation $r$ is defined over $K$. If not, since $\text{tr} r(G) \subset K$ and $r$ is absolutely irreducible, there is a field of quaternions $H$ over $K$ such that $r$ factors through $G \to H^*$. Then for $c \in G$ the complex conjugation, $r(c)^2 = r(c^2) = 1$, so $(r(c) - 1)^2 = 0$ and $r(c) = 1$ since $H$ is a field, and $r$ is even.
Proof of the existence of the representation $r$

**Step 4** The representation $r$ is defined over $K$. If not, since $\text{tr} \ r(G) \subset K$ and $r$ is absolutely irreducible, there is a field of quaternions $H$ over $K$ such that $r$ factors through $G \rightarrow H^*$. Then for $c \in G$ the complex conjugation, $r(c)^2 = r(c^2) = 1$, so $(r(c) - 1)^2 = 0$ and $r(c) = 1$ since $H$ is a field, and $r$ is even. So $r$ factors through the maximal totally real quotient of $G$, which is abelian.
Proof of the existence of the representation $r$

**Step 4** The representation $r$ is defined over $K$. If not, since $\text{tr} \, r(G) \subset K$ and $r$ is absolutely irreducible, there is a field of quaternions $H$ over $K$ such that $r$ factors through $G \to H^*$. Then for $c \in G$ the complex conjugation, $r(c)^2 = r(c^2) = 1$, so $(r(c) - 1)^2 = 0$ and $r(c) = 1$ since $H$ is a field, and $r$ is even. So $r$ factors through the maximal totally real quotient of $G$, which is abelian. Contradiction.
Proof of the existence of the representation $r$

Step 4 The representation $r$ is defined over $K$. If not, since $\text{tr} \ r(G) \subset K$ and $r$ is absolutely irreducible, there is a field of quaternions $H$ over $K$ such that $r$ factors through $G \to H^*$. Then for $c \in G$ the complex conjugation, $r(c)^2 = r(c^2) = 1$, so $(r(c) - 1)^2 = 0$ and $r(c) = 1$ since $H$ is a field, and $r$ is even. So $r$ factors through the maximal totally real quotient of $G$, which is abelian. Contradiction.

Step 5 Since $\text{tr} \ r \subset A$ and $r : \to \text{SL}_2(K)$ is absolutely irreducible, $r$ stabilizes an $A$-lattice $M \subset K^2$. 
Proof of the existence of the representation \( r \)

**Step 4** The representation \( r \) is defined over \( K \). If not, since \( \text{tr} \, r(G) \subset K \) and \( r \) is absolutely irreducible, there is a field of quaternions \( H \) over \( K \) such that \( r \) factors through \( G \to H^* \). Then for \( c \in G \) the complex conjugation, \( r(c)^2 = r(c^2) = 1 \), so \( (r(c) - 1)^2 = 0 \) and \( r(c) = 1 \) since \( H \) is a field, and \( r \) is even. So \( r \) factors through the maximal totally real quotient of \( G \), which is abelian. Contradiction.

**Step 5** Since \( \text{tr} \, r \subset A \) and \( r : \to \text{SL}_2(K) \) is absolutely irreducible, \( r \) stabilizes an \( A \)-lattice \( M \subset K^2 \). The bidual \( M'' \) of \( M \) is a reflexive module over \( A \) which is a regular local ring of dimension 2, hence is free. Hence a representation \( r : G \to \text{SL}_2(A) \) of trace \( t \).
Proof of the existence of the representation $r$

**Step 4** The representation $r$ is defined over $K$. If not, since $\text{tr} \ r(G) \subseteq K$ and $r$ is absolutely irreducible, there is a field of quaternions $H$ over $K$ such that $r$ factors through $G \to H^*$. Then for $c \in G$ the complex conjugation, $r(c)^2 = r(c^2) = 1$, so $(r(c) - 1)^2 = 0$ and $r(c) = 1$ since $H$ is a field, and $r$ is even. So $r$ factors through the maximal totally real quotient of $G$, which is abelian. Contradiction.

**Step 5** Since $\text{tr} \ r(1) \subseteq A$ and $r : \to \text{SL}_2(K)$ is absolutely irreducible, $r$ stabilizes an $A$-lattice $M \subseteq K^2$. The bidual $M''$ of $M$ is a reflexive module over $A$ which is a regular local ring of dimension 2, hence is free. Hence a representation $r : G \to \text{SL}_2(A)$ of trace $t$.

**Step 6** Since $r$ is absolutely irreducible, and $\text{tr} \ r = t$ is continuous, $r$ is continuous.
Universality of $A$

**Theorem**

The algebra $A$, with the pseudorepresentation $(t, 1)$ constructed in step 1 above, is the universal deformation ring $R$ of the pseudorepresentation $(0, 1) : G \to \mathbb{F}_2$, with the condition $d = 1$ and $t(c) = 0$. 
Universality of $A$

Theorem

The algebra $A$, with the pseudorepresentation $(t, 1)$ constructed in step 1 above, is the universal deformation ring $R$ of the pseudorepresentation $(0, 1) : G \to \mathbb{F}_2$, with the condition $d = 1$ and $t(c) = 0$.

This is an "$R = T$" theorem, excepted that $T$ is called $A$. This is also the main tool to prove the other points of the theorem.
Part III.

Special modular forms modulo 2

(joint with Jean-Louis Nicolas, Jean-Pierre Serre)
Definitions of special modular forms.

For every $f$, $T_p f$ depends only on $f$ in some finite extension $L$ of $\mathbb{Q}$, unramified outside 2, of degree a power of 2. Let $L(f)$ the smallest such extension.
Definitions of special modular forms.

For every $f$, $T_p f$ depends only on $f$ in some finite extension $L$ of $\mathbb{Q}$, unramified outside 2, of degree a power of 2. Let $L(f)$ the smallest such extension.

One says that $f \in M$ is abelian if $L(f)$ is abelian. Examples: $\tilde{\Delta}^9$ is not abelian, but $\tilde{\Delta}^3$, $\tilde{\Delta}^5$, $\tilde{\Delta}^7$ are.
Definitions of special modular forms.

For every \( f \), \( T_p f \) depends only on \( f \) in some finite extension \( L \) of \( \mathbb{Q} \), unramified outside 2, of degree a power of 2. Let \( L(f) \) the smallest such extension.

One says that \( f \in M \) is **abelian** if \( L(f) \) is abelian. Examples: \( \tilde{\Delta}^9 \) is not abelian, but \( \tilde{\Delta}^3, \tilde{\Delta}^5, \tilde{\Delta}^7 \) are.

One says that \( f \in M \) is **\( \mathbb{Q}(i) \)-dihedral**, resp. **\( \mathbb{Q}(\sqrt{-2}) \)-dihedral** if \( L(f) \) is a dihedral extension of \( \mathbb{Q} \) containing \( \mathbb{Q}(i) \) (resp. \( \mathbb{Q}(\sqrt{-2}) \)).
Definitions of special modular forms.

For every $f$, $T_p f$ depends only on $f$ in some finite extension $L$ of $\mathbb{Q}$, unramified outside 2, of degree a power of 2. Let $L(f)$ the smallest such extension.

One says that $f \in M$ is abelian if $L(f)$ is abelian. Examples: $\tilde{\Delta}^9$ is not abelian, but $\tilde{\Delta}^3$, $\tilde{\Delta}^5$, $\tilde{\Delta}^7$ are.

One says that $f \in M$ is $\mathbb{Q}(i)$-dihedral, resp. $\mathbb{Q}(\sqrt{-2})$-dihedral if $L(f)$ is a dihedral extension of $\mathbb{Q}$ containing $\mathbb{Q}(i)$ (resp. $\mathbb{Q}(\sqrt{-2})$).

One says that $f$ is special if it is a linear combination of abelian and dihedral forms.
Definitions of special modular forms.

For every \( f \), \( T_p f \) depends only on \( f \) in some finite extension \( L \) of \( \mathbb{Q} \), unramified outside 2, of degree a power of 2. Let \( L(f) \) the smallest such extension.

One says that \( f \in M \) is abelian if \( L(f) \) is abelian. Examples: \( \tilde{\Delta}^9 \) is not abelian, but \( \tilde{\Delta}^3, \tilde{\Delta}^5, \tilde{\Delta}^7 \) are.

One says that \( f \in M \) is \( \mathbb{Q}(i) \)-dihedral, resp. \( \mathbb{Q}(\sqrt{-2}) \)-dihedral if \( L(f) \) is a dihedral extension of \( \mathbb{Q} \) containing \( \mathbb{Q}(i) \) (resp. \( \mathbb{Q}(\sqrt{-2}) \)).

One says that \( f \) is special if it is a linear combination of abelian and dihedral forms.
Characterization of special modular forms

Theorem
A form $f \in M$ is $\mathbb{Q}(i)$-dihedral iff $xf = 0$ or $\tilde{\Delta}$. A form $f \in M$ is dihedral of type $\mathbb{Q}(\sqrt{-2})$ iff $yf = 0$ or $\tilde{\Delta}$. A form $f \in M$ is abelian iff $f$ is killed by $\mathcal{P}_0^2$. 

Corollary
The space of $\mathbb{Q}(i)$-dihedral forms is generated by the $m(0,b), b \in \mathbb{N}$ and $m(1,0) = \tilde{\Delta}$. The space of $\mathbb{Q}(\sqrt{-2})$-dihedral forms is generated by the $m(a,0), a \in \mathbb{N}$ and $m(0,1) = \tilde{\Delta}$. 

Corollary
Special forms are sparse: in the subspace of $M$ generated by the $m(a,b)$ with $a + b < n$, of dimension $n(n+1)/2$, the dimension of the subspace of abelian forms is $2^n - 1$, and dimension of the subspace of dihedral forms of each type is $n+1$. 

Theorem
A form $f \in M$ is $\mathbb{Q}(i)$-dihedral iff $xf = 0$ or $\tilde{\Delta}$. A form $f \in M$ is dihedral of type $\mathbb{Q}(\sqrt{-2})$ iff $yf = 0$ or $\tilde{\Delta}$. A form $f \in M$ is abelian iff $f$ is killed by $P_0^2$. 
Characterization of special modular forms

Theorem
A form $f \in M$ is $\mathbb{Q}(i)$-dihedral iff $xf = 0$ or $\tilde{\Delta}$. A form $f \in M$ is dihedral of type $\mathbb{Q}(\sqrt{-2})$ iff $yf = 0$ or $\tilde{\Delta}$. A form $f \in M$ is abelian iff $f$ is killed by $P_0^2$.

Corollary
The space of $\mathbb{Q}(i)$-dihedral forms is generated by the $m(0, b)$, $b \in \mathbb{N}$ and $m(1, 0) = \tilde{\Delta}^3$. The space of $\mathbb{Q}(\sqrt{-2})$-dihedral forms is generated by the $m(a, 0)$, $a \in \mathbb{N}$ and $m(0, 1) = \tilde{\Delta}^5$. 
Characterization of special modular forms

**Theorem**
A form $f \in M$ is $\mathbb{Q}(i)$-dihedral iff $xf = 0$ or $\tilde{\Delta}$. A form $f \in M$ is dihedral of type $\mathbb{Q}(\sqrt{-2})$ iff $yf = 0$ or $\tilde{\Delta}$. A form $f \in M$ is abelian iff $f$ is killed by $P_0^2$.

**Corollary**
The space of $\mathbb{Q}(i)$-dihedral forms is generated by the $m(0, b)$, $b \in \mathbb{N}$ and $m(1, 0) = \tilde{\Delta}^3$. The space of $\mathbb{Q}(\sqrt{-2})$-dihedral forms is generated by the $m(a, 0)$, $a \in \mathbb{N}$ and $m(0, 1) = \tilde{\Delta}^5$.

**Corollary**
Special forms are sparse: in the subspace of $M$ generated by the $m(a, b)$ with $a + b < n$, of dimension $n(n + 1)/2$, the dimension of the subspace of abelian forms is $2n - 1$, and dimension of the subspace of dihedral forms of each type is $n + 1$. 
Powers of $\tilde{\Delta}$ that are special

Proposition

For any $r$, $\tilde{\Delta}^{2^r+1}$ and for any odd $r$, $\tilde{\Delta}^{(2^r+1)/3}$ are dihedral. For $k = 1, 3, 5, 7, 19, 21$, $\tilde{\Delta}^k$ is abelian.
Powers of $\tilde{\Delta}$ that are special

**Proposition**

For any $r$, $\tilde{\Delta}^{2^r+1}$ and for any odd $r$, $\tilde{\Delta}^{(2^r+1)/3}$ are dihedral. For $k = 1, 3, 5, 7, 19, 21$, $\tilde{\Delta}^k$ is abelian.

**Conjecture**

The only forms $\tilde{\Delta}^k$ that are special are the ones given in the proposition.

In particular, there are only 6 values of $k$ (explicitly $1, 3, 5, 7, 19, 21$), conjecturally, such that $\tilde{\Delta}^k$ is abelian.
Powers of $\tilde{\Delta}$ that are special

**Proposition**

For any $r$, $\tilde{\Delta}^{2r+1}$ and for any odd $r$, $\tilde{\Delta}^{(2r+1)/3}$ are dihedral. For $k = 1, 3, 5, 7, 19, 21$, $\tilde{\Delta}^k$ is abelian.

**Conjecture**

The only forms $\tilde{\Delta}^k$ that are special are the ones given in the proposition.

In particular, there are only 6 values of $k$ (explicitly $1, 3, 5, 7, 19, 21$), conjecturally, such that $\tilde{\Delta}^k$ is abelian. This is vaguely reminiscent of the finiteness of idoneal numbers (conjectured by Euler, proved by Hecke and Landau under GRH, then unconditionally).
Powers of $\tilde{\Delta}$ that are special

Proposition

For any $r$, $\tilde{\Delta}^{2r+1}$ and for any odd $r$, $\tilde{\Delta}^{(2r+1)/3}$ are dihedral. For $k = 1, 3, 5, 7, 19, 21$, $\tilde{\Delta}^k$ is abelian.

Conjecture

The only forms $\tilde{\Delta}^k$ that are special are the ones given in the proposition.

In particular, there are only 6 values of $k$ (explicitly $1, 3, 5, 7, 19, 21$), conjecturally, such that $\tilde{\Delta}^k$ is abelian. This is vaguely reminiscent of the finiteness of idoneal numbers (conjectured by Euler, proved by Hecke and Landau under GRH, then unconditionally).

Our conjecture is proved for most $k$’s.
Part IV.

Density of modular forms modulo 2
Density: definitions and reductions

For $f = \sum a_n q^n \in M$, the set $\{p, a_p = 1\}$ has a density, denoted $\delta(f)$ (by Chebotarev, since $a_p$ depends only on $\text{Frob}_p$ in $\text{Gal}(L(f)/\mathbb{Q})$).
Density: definitions and reductions

For \( f = \sum a_n q^n \in M \), the set \( \{ p, a_p = 1 \} \) has a density, denoted \( \delta(f) \) (by Chebotarev, since \( a_p \) depends only on \( \text{Frob}_p \) in \( \text{Gal}(L(f)/\mathbb{Q}) \)). One has \( 0 \leq \delta(f) \leq 1 \), \( \delta(f) \in \mathbb{Z}[1/2] \).
Density: definitions and reductions

For $f = \sum a_n q^n \in M$, the set $\{p, a_p = 1\}$ has a density, denoted $\delta(f)$ (by Chebotarev, since $a_p$ depends only on $\text{Frob}_p$ in $\text{Gal}(L(f)/\mathbb{Q})$). One has $0 \leq \delta(f) \leq 1$, $\delta(f) \in \mathbb{Z}[1/2]$.

Aim: compute $\delta(f)$ for $f \in M$. 
Density: definitions and reductions

For $f = \sum a_n q^n \in M$, the set $\{p, a_p = 1\}$ has a density, denoted $\delta(f)$ (by Chebotarev, since $a_p$ depends only on $\text{Frob}_p$ in $\text{Gal}(L(f)/\mathbb{Q})$). One has $0 \leq \delta(f) \leq 1$, $\delta(f) \in \mathbb{Z}[1/2]$.

Aim: compute $\delta(f)$ for $f \in M$.

Remark: If $f = f_1 + f_3 + f_5 + f_7$ with $f_i \in M^i$, $\delta(f) = \delta(f_1) + \delta(f_3) + \delta(f_5) + \delta(f_7)$. This reduces the study of density to the case of homegenous $f$, i.e. $f \in M^i$ for some $i \in (\mathbb{Z}/8\mathbb{Z})^*$. For $f$ homogeneous, $\delta(f) \leq 1/4$. 
Density: qualitative results

Theorem
If $f \in M, f \neq 0, \tilde{\Delta}$, then $\delta(f) > 0$. 

Corollary
Let $f = \sum a_n q^n$, and $g = \sum b_n q^n$. If $a_p = b_p$ for every prime $p$ (except possibly a set of density $0$), then $f = g$ or $f = g + \tilde{\Delta}$ (hence $a_n = b_n$ for all $n$ except odd squares).

Corollary
For every odd $k \geq 3$, there exists infinitely many $p$ such that $\tau_k(p)$ is odd.

Theorem
If $f$ is homogenous and $f \neq 0, \tilde{\Delta}, \tilde{\Delta}_5$, then $\delta(f) < 1/4$. For any $f \in M$, $\delta(f) < 1$.

Corollary
For every odd $k$, there exists infinitely many $p$ such that $\tau_k(p)$ is even.
Density: qualitative results

**Theorem**
If $f \in M$, $f \neq 0, \tilde{\Delta}$, then $\delta(f) > 0$.

**Corollary**
Let $f = \sum a_nq^n$, and $g = \sum b_nq^n$. If $a_p = b_p$ for every prime $p$ (except possibly a set of density $0$), then $f = g$ or $f = g + \tilde{\Delta}$ (hence $a_n = b_n$ for all $n$ except odd squares).
Density: qualitative results

**Theorem**

If \( f \in M, f \neq 0, \tilde{\Delta}, \) then \( \delta(f) > 0. \)

**Corollary**

Let \( f = \sum a_n q^n, \) and \( g = \sum b_n q^n. \) If \( a_p = b_p \) for every prime \( p \) (except possibly a set of density 0), then \( f = g \) or \( f = g + \tilde{\Delta} \) (hence \( a_n = b_n \) for all \( n \) except odd squares).

**Corollary**

For every odd \( k \geq 3, \) there exists infinitely many \( p \) such that \( \tau_k(p) \) is odd.
Density: qualitative results

Theorem
If \( f \in M, f \neq 0, \tilde{\Delta}, \) then \( \delta(f) > 0. \)

Corollary
Let \( f = \sum a_nq^n \) and \( g = \sum b_nq^n. \) If \( a_p = b_p \) for every prime \( p \) (except possibly a set of density 0), then \( f = g \) or \( f = g + \tilde{\Delta} \) (hence \( a_n = b_n \) for all \( n \) except odd squares).

Corollary
For every odd \( k \geq 3, \) there exists infinitely many \( p \) such that \( \tau_k(p) \) is odd.

Theorem
If \( f \) is homogenous and \( f \neq \tilde{\Delta}^3, \tilde{\Delta}^5, \) \( \delta(f) < 1/4. \) For any \( f \in M, \) \( \delta(f) < 1 \)
Density: qualitative results

Theorem
If \( f \in M, f \neq 0, \tilde{\Delta}, \) then \( \delta(f) > 0. \)

Corollary
Let \( f = \sum a_nq^n, \) and \( g = \sum b_nq^n. \) If \( a_p = b_p \) for every prime \( p \) (except possibly a set of density 0), then \( f = g \) or \( f = g + \tilde{\Delta} \) (hence \( a_n = b_n \) for all \( n \) except odd squares).

Corollary
For every odd \( k \geq 3, \) there exists infinitely many \( p \) such that \( \tau_k(p) \) is odd.

Theorem
If \( f \) is homogenous and \( f \neq \tilde{\Delta}^3, \tilde{\Delta}^5, \) \( \delta(f) < 1/4. \) For any \( f \in M, \) \( \delta(f) < 1 \)

Corollary
For every odd \( k, \) there exists infinitely many \( p \) such that \( \tau_k(p) \) is even.
Density: qualitative results

**Theorem**

If $f \in M$, $f \neq 0, \tilde{\Delta}$, then $\delta(f) > 0$.

**Corollary**

Let $f = \sum a_n q^n$, and $g = \sum b_n q^n$. If $a_p = b_p$ for every prime $p$ (except possibly a set of density 0), then $f = g$ or $f = g + \tilde{\Delta}$ (hence $a_n = b_n$ for all $n$ except odd squares).

**Corollary**

For every odd $k \geq 3$, there exists infinitely many $p$ such that $\tau_k(p)$ is odd.

**Theorem**

If $f$ is homogenous and $f \neq \tilde{\Delta}^3, \tilde{\Delta}^5$, $\delta(f) < 1/4$. For any $f \in M$, $\delta(f) < 1$.

**Corollary**

For every odd $k$, there exists infinitely many $p$ such that $\tau_k(p)$ is even.
Density: quantitative results and a conjecture

For \( f \) in \( M \), its nilpotence index is the smallest \( a \) such that \( x^n y^m f = 0 \) for every \( n, m \) such that \( n + m > a \).
Density: quantitative results and a conjecture

For $f$ in $M$, its nilpotence index is the smallest $a$ such that $x^n y^m f = 0$ for every $n, m$ such that $n + m > a$.

**Theorem**

If $f$ is special and homogeneous, of nilpotence index $a$, then

$$
\delta(f) = 2^{-v(a)} - u(a) - 1,
$$

where $v(a)$ is the 2-valuation of $a$, $u(a)$ is the number of digits 1 in the expansion of $a$ in basis 2.

Computed with Sage the density of $\tilde{\Delta}_k$, $k < 4000$ and linear combinations of $\tilde{\Delta}_k$, $k < 80$, for primes up to $1$ million. Very close to 0.125.

Theorem

The conjecture is true for all forms of nilpotence index at most 12, for all the forms $m(a, 1)$ (or $m(1, a)$) and linear combinations thereof, for all forms $m(2^r - 1, 2)$, etc.
Density: quantitative results and a conjecture

For $f$ in $M$, its nilpotence index is the smallest $a$ such that $x^n y^m f = 0$ for every $n, m$ such that $n + m > a$.

Theorem

If $f$ is special and homogeneous, of nilpotence index $a$, then
\[ \delta(f) = 2^{-v(a) - u(a) - 1}, \]
where $v(a)$ is the 2-valuation of $a$, $u(a)$ is the numbers of digits 1 in the expansion of $a$ in basis 2.

Conjecture

If $f$ is non-special and homogenous, then $\delta(f) = 1/8$. 
Density: quantitative results and a conjecture

For $f$ in $M$, its nilpotence index is the smallest $a$ such that $x^ny^mf = 0$ for every $n, m$ such that $n + m > a$.

**Theorem**

If $f$ is special and homogeneous, of nilpotence index $a$, then

$$\delta(f) = 2^{-v(a)} - u(a) - 1,$$

where $v(a)$ is the 2-valuation of $a$, $u(a)$ is the numbers of digits 1 in the expansion of $a$ in basis 2.

**Conjecture**

If $f$ is non-special and homogenous, then $\delta(f) = 1/8$.

Computed with sage the density of $\tilde{\Delta}_k$, $k < 4000$ and linear combinations of $\tilde{\Delta}_k$, $k < 80$, for primes up to a 1 million. Very close to 0.125.

**Theorem**

The conjecture is true for all forms of nilpotence index at most 12, for all the forms $m(a, 1)$ (or $m(1, a)$) and linear combinations thereof, for all forms $m(2^r - 1, 2)$, etc.
Density: quantitative results and a conjecture

For \( f \) in \( M \), its nilpotence index is the smallest \( a \) such that \( x^ny^mf = 0 \) for every \( n, m \) such that \( n + m > a \).

**Theorem**

If \( f \) is special and homogeneous, of nilpotence index \( a \), then \( \delta(f) = 2^{-v(a)-u(a)-1} \), where \( v(a) \) is the 2-valuation of \( a \), \( u(a) \) is the numbers of digits 1 in the expansion of \( a \) in basis 2.

**Conjecture**

If \( f \) is non-special and homogenous, then \( \delta(f) = 1/8 \).

Computed with sage the density of \( \tilde{\Delta}^k \), \( k < 4000 \) and linear combinations of \( \tilde{\Delta}^k \), \( k < 80 \), for primes up to a 1 million. Very close to 0.125.

**Theorem**

The conjecture is true for all forms of nilpotence index at most 12, for all the forms \( m(a, 1) \) (or \( m(1, a) \)) and linear combinations thereof, for all forms \( m(2^r - 1, 2) \), etc.
Tools for the proofs: the structure of the pro-2-group $G$

Let $F$ be the Frattini subgroup of $G$. Then

$$G/F = \text{Gal}(\mathbb{Q}(\mu_8)/\mathbb{Q}) = (\mathbb{Z}/8\mathbb{Z})^*$$

We write $G^i$ for the preimage of $i = 1, 3, 5, 7$ in $G/F$. We have $\text{Frob}_p \in G^{p(\text{mod } 8)}$ and $t(G^i) \in A^i$. Let $c \in G$ be a complex conjugation. Hence $c \in G^7$.

**Lemma (Serre)**

*Any element of order 2 of $G$ is conjugate to $c$.***
Tools for the proofs: the structure of the pro-2-group $G$

Let $F$ be the Frattini subgroup of $G$. Then

$$G/F = \text{Gal}(\mathbb{Q}(\mu_8)/\mathbb{Q}) = (\mathbb{Z}/8\mathbb{Z})^*$$

We write $G^i$ for the preimage of $i = 1, 3, 5, 7$ in $G/F$. We have $\text{Frob}_p \in G^{p(\text{mod } 8)}$ and $t(G^i) \in A_i$.

Let $c \in G$ be a complex conjugation. Hence $c \in G^7$.

**Lemma (Serre)**

Any element of order 2 of $G$ is conjugate to $c$.

**Lemma**

Let $u$ be any element in $G^3$ or $G^5$. Then $G$ has the presentation $\langle u, c | c^2 = 1 \rangle$ in the category of pro-2-groups.
Tools for the proofs: the structure of the pro-2-group $G$

Let $F$ be the Frattini subgroup of $G$. Then

$$G/F = \text{Gal}(\mathbb{Q}(\mu_8)/\mathbb{Q}) = (\mathbb{Z}/8\mathbb{Z})^*$$

We write $G^i$ for the preimage of $i = 1, 3, 5, 7$ in $G/F$. We have $\text{Frob}_p \in G^{p^{(\text{mod } 8)}}$ and $t(G^i) \in A^i$.

Let $c \in G$ be a complex conjugation. Hence $c \in G^7$.

**Lemma (Serre)**

*Any element of order 2 of $G$ is conjugate to $c$.***

**Lemma**

*Let $u$ be any element in $G^3$ or $G^5$. Then $G$ has the presentation $\langle u, c | c^2 = 1 \rangle$ in the category of pro-2-groups.*

The proof uses a result of Shafarevich.
Tools for the proofs: the structure of the pro-2-group $G$

Let $F$ be the Frattini subgroup of $G$. Then

$$G/F = \text{Gal}(\mathbb{Q}(\mu_8)/\mathbb{Q}) = (\mathbb{Z}/8\mathbb{Z})^*$$

We write $G^i$ for the preimage of $i = 1, 3, 5, 7$ in $G/F$. We have $\text{Frob}_p \in G^{p(\mod 8)}$ and $t(G^i) \in A^i$.

Let $c \in G$ be a complex conjugation. Hence $c \in G^7$.

**Lemma (Serre)**

*Any element of order 2 of $G$ is conjugate to $c$.***

**Lemma**

*Let $u$ be any element in $G^3$ or $G^5$. Then $G$ has the presentation $\langle u, c | c^2 = 1 \rangle$ in the category of pro-2-groups.*

The proof uses a result of Shafarevich.

Let us **choose** $u$ and $c$ as in the lemma, with $u \in G^3$ to fix ideas.
Tools for the proofs: the structure of the pro-2-group $G$

Let $F$ be the Frattini subgroup of $G$. Then

$$G/F = \text{Gal}(\mathbb{Q}(\mu_8)/\mathbb{Q}) = (\mathbb{Z}/8\mathbb{Z})^*$$

We write $G^i$ for the preimage of $i = 1, 3, 5, 7$ in $G/F$. We have $\text{Frob}_p \in G^{p \mod 8}$ and $t(G^i) \in A^i$.

Let $c \in G$ be a complex conjugation. Hence $c \in G^7$.

**Lemma (Serre)**

Any element of order 2 of $G$ is conjugate to $c$.

**Lemma**

Let $u$ be any element in $G^3$ or $G^5$. Then $G$ has the presentation

$$\langle u, c | c^2 = 1 \rangle$$

in the category of pro-2-groups.

The proof uses a result of Shafarevich.

Let us choose $u$ and $c$ as in the lemma, with $u \in G^3$ to fix ideas.

Let us write $t(u) = X \in A$, $t(cu) = Y \in A$. Then $X, Y$ are analogs of $x, y$. 
Tools for the proofs: the Fricke polynomials

Let $\Gamma$ be the discrete subgroup of $G$ generated by $u$ and $c$. 

Proposition

For $\gamma \in \Gamma$, $t(\gamma) \in F_2[\![X,Y]\!]$.

Classical Fricke polynomials are polynomials in $\mathbb{Z}[\![X,Y,Z]\!]$ arising in representation theory and quantum physics. The $t(\gamma)$ are the reduction mod $(\mathbb{Z},2)$ of those polynomials. Example: $t(u^n)$ is the Chebychev polynomial of degree $n$ in $X$ modulo 2.

Corollary

One has $A = F_2[\![X,Y]\!]$. One has $(x) = (X)$, $(y) = (Y)$, $P_0 = (X+Y)$.

Proof: $t(G) \subset F_2[\![X,Y]\!]$ and $t(G)$ generates $A$ as an algebra by universality.

Proposition

The closed subspace of $A$ generated by $t(G)$ is the maximal ideal $mA$.

Proof: computations.
Tools for the proofs: the Fricke polynomials

Let $\Gamma$ be the discrete subgroup of $G$ generated by $u$ and $c$.

**Proposition**

For $\gamma \in \Gamma$, $t(\gamma) \in \mathbb{F}_2[X, Y]$.

Classical Fricke polynomials are polynomials in $\mathbb{Z}[X, Y, Z]$ arising in representation theory and quantum physics. The $t(\gamma)$ are the reduction mod $(\mathbb{Z}, 2)$ of those polynomials. Example: $t(u^n)$ is the Chebychev polynomial of degree $n$ in $X$ modulo 2.

**Corollary**

One has $A = F_2[[X, Y]]$. One has $(x) = (X)$, $(y) = (Y)$, $P_0 = (X + Y)$.

**Proof:**

$t(G) \subset F_2[[X, Y]]$ and $t(G)$ generates $A$ as an algebra by universality.

**Proposition**

The closed subspace of $A$ generated by $t(G)$ is the maximal ideal $m_A$.

**Proof:** computations.
Tools for the proofs: the Fricke polynomials

Let $\Gamma$ be the discrete subgroup of $G$ generated by $u$ and $c$.

Proposition

For $\gamma \in \Gamma$, $t(\gamma) \in \mathbb{F}_2[X, Y]$.

Classical Fricke polynomials are polynomials in $\mathbb{Z}[X, Y, Z]$ arising in representation theory and quantum physics. The $t(\gamma)$ are the reduction mod $(Z, 2)$ of those polynomials. Example: $t(u^n)$ is the Chebychev polynomial of degree $n$ in $X$ modulo 2.
Tools for the proofs: the Fricke polynomials

Let \( \Gamma \) be the discrete subgroup of \( G \) generated by \( u \) and \( c \).

**Proposition**

For \( \gamma \in \Gamma \), \( t(\gamma) \in \mathbb{F}_2[X, Y] \).

Classical *Fricke polynomials* are polynomials in \( \mathbb{Z}[X, Y, Z] \) arising in representation theory and quantum physics. The \( t(\gamma) \) are the reduction mod \( \mathbb{Z}, 2 \) of those polynomials. Example: \( t(u^n) \) is the Chebychev polynomial of degree \( n \) in \( X \) modulo 2.

**Corollary**

One has \( A = \mathbb{F}_2[[X, Y]] \). One has \( (x) = (X), (y) = (Y), P_0 = (X + Y) \).
Tools for the proofs: the Fricke polynomials

Let $\Gamma$ be the discrete subgroup of $G$ generated by $u$ and $c$.

Proposition

For $\gamma \in \Gamma$, $t(\gamma) \in \mathbb{F}_2[X, Y]$.

Classical Fricke polynomials are polynomials in $\mathbb{Z}[X, Y, Z]$ arising in representation theory and quantum physics. The $t(\gamma)$ are the reduction mod $(Z, 2)$ of those polynomials. Example: $t(u^n)$ is the Chebychev polynomial of degree $n$ in $X$ modulo 2.

Corollary

One has $A = \mathbb{F}_2[[X, Y]]$. One has $(x) = (X)$, $(y) = (Y)$, $P_0 = (X + Y)$.

Proof: $t(G) \subset \mathbb{F}_2[[X, Y]]$ and $t(G)$ generates $A$ as an algebra by universality.
Tools for the proofs: the Fricke polynomials

Let $\Gamma$ be the discrete subgroup of $G$ generated by $u$ and $c$.

**Proposition**

For $\gamma \in \Gamma$, $t(\gamma) \in \mathbb{F}_2[X, Y]$.

Classical *Fricke polynomials* are polynomials in $\mathbb{Z}[X, Y, Z]$ arising in representation theory and quantum physics. The $t(\gamma)$ are the reduction mod $(Z, 2)$ of those polynomials. Example: $t(u^n)$ is the Chebychev polynomial of degree $n$ in $X$ modulo 2.

**Corollary**

One has $A = \mathbb{F}_2[[X, Y]]$. One has $(x) = (X)$, $(y) = (Y)$, $P_0 = (X + Y)$.

Proof: $t(G) \subset \mathbb{F}_2[[X, Y]]$ and $t(G)$ generates $A$ as an algebra by universality.

**Proposition**

The closed subspace of $A$ generated by $t(G)$ is the maximal ideal $m_A$.

Proof: computations.
Proof of the theorem of positive density

**Theorem**

*If* \( f \in M, f \neq 0, \Delta, \delta(f) > 0 \)

**Proof:** Define

\[
H = H_f = \{ T \in A, \ a_1(Tf) = 0 \}.
\]
Proof of the theorem of positive density

**Theorem**

If \( f \in M, f \neq 0, \Delta, \delta(f) > 0 \)

**Proof:** Define

\[
H = H_f = \{ T \in A, \ a_1(Tf) = 0 \}.
\]

Then \( H \) is an open hyperplan of \( A \), and \( H \neq m_A \) because \( f \neq \tilde{\Delta} \).
Proof of the theorem of positive density

**Theorem**

*If* $f \in M$, $f \neq 0$, $\Delta$, $\delta(f) > 0$

**Proof:** Define

$$H = H_f = \{ T \in A, \ a_1(Tf) = 0 \}.$$  

Then $H$ is an open hyperplan of $A$, and $H \neq m_A$ because $f \neq \tilde{\Delta}$. Since $a_p = a_1(T_pf)$ is 1 if and only if $T_p \in H$, and $T_p = t(Frob_p)$, one has by Chebotarev

$$\delta(f) = \mu_G(t^{-1}(H)),$$

where $\mu_G$ is the Haar probability measure on $G$.  

Proof of the theorem of positive density

Theorem

If $f \in M, f \neq 0, \Delta, \delta(f) > 0$

Proof: Define

$$H = H_f = \{ T \in A, \ a_1(Tf) = 0 \}.$$  

Then $H$ is an open hyperplan of $A$, and $H \neq m_A$ because $f \neq \tilde{\Delta}$. Since $a_p = a_1(T_p f)$ is 1 if and only if $T_p \in H$, and $T_p = t(Frob_p)$, one has by Chebotarev

$$\delta(f) = \mu_G(t^{-1}(H)),$$

where $\mu_G$ is the Haar probablity measure on $G$. But $t^{-1}(H)$ is open and non-empty since $t(G)$ is dense in $m_A$. QED.
Idea of the proof of $\delta(f) = 1/8$ for some $f \in M^i$

Proposition

There exists unique continuous action of $\text{Out}(G)$ on $A$ such that if $\psi \in \text{Out}(G)$, $g \in G$, $\psi \cdot t(g) = t(\psi(g))$.

Idea of proof: $A$ is the universal deformation of the pseudo-deformation $(0,1)$ with the conditions $d = 1$, $t(c) = 0$. Since $t(\psi(c)) = 0$ for $\psi \in \text{Aut}(G)$ because of Serre’s lemma, $\psi$ defines an automorphism on $A$. 
Idea of the proof of $\delta(f) = 1/8$ for some $f \in M^i$

Proposition

*There exists unique continuous action of Out($G$) on $A$ such that if $\psi \in \text{Out}(G)$, $g \in G$, $\psi \cdot t(g) = t(\psi(g))$.***

Idea of proof: $A$ is the universal deformation of the pseudo-deformation $(0,1)$ with the conditions $d = 1$, $t(c) = 0$. Since $t(\psi(c)) = 0$ for $\psi \in \text{Aut}(G)$ because of Serre’s lemma, $\psi$ defines an automorphism on $A$.

Lemma

*For any $v \in G^3$, there exists a unique automorphism of $G$ such that $\psi(u) = v$, $\psi(c) = c$. This automorphisms stabilizes $G^i$ for $i \in (\mathbb{Z}/8\mathbb{Z})^*$.***
Idea of the proof of $\delta(f) = 1/8$ for some $f \in M^i$

Proposition

*There exists unique continuous action of Out$(G)$ on $A$ such that if $\psi \in$ Out$(G)$, $g \in G$, $\psi \cdot t(g) = t(\psi(g))$.***

Idea of proof: $A$ is the universal deformation of the pseudo-deformation $(0,1)$ with the conditions $d = 1$, $t(c) = 0$. Since $t(\psi(c)) = 0$ for $\psi \in$ Aut$(G)$ because of Serre’s lemma, $\psi$ defines an automorphism on $A$.

Lemma

*For any $v \in G^3$, there exists a unique automorphism of $G$ such that $\psi(u) = v$, $\psi(c) = c$. This automorphisms stabilizes $G^i$ for $i \in (\mathbb{Z}/8\mathbb{Z})^*$.***

Since $f \in M^i$, $H^i = H \cap A^i$ is an hyperplan of $A^i$. Using the lemma, one constructs for suitable $f$’s a $\psi \in$ Out$(G)$ such that $\psi \cdot H^i = A^i - H^i$, $\psi \cdot (A^i - H^i) = H^i$. 
Idea of the proof of $\delta(f) = 1/8$ for some $f \in M^i$

Proposition

There exists unique continuous action of $\text{Out}(G)$ on $A$ such that if $\psi \in \text{Out}(G)$, $g \in G$, $\psi \cdot t(g) = t(\psi(g))$.

Idea of proof: $A$ is the universal deformation of the pseudo-deformation $(0,1)$ with the conditions $d = 1$, $t(c) = 0$. Since $t(\psi(c)) = 0$ for $\psi \in \text{Aut}(G)$ because of Serre’s lemma, $\psi$ defines an automorphism on $A$.

Lemma

For any $v \in G^3$, there exists a unique automorphism of $G$ such that $\psi(u) = v$, $\psi(c) = c$. This automorphisms stabilizes $G^i$ for $i \in (\mathbb{Z}/8\mathbb{Z})^*$.

Since $f \in M^i$, $H^i = H \cap A^i$ is an hyperplan of $A^i$. Using the lemma, one constructs for suitable $f$’s a $\psi \in \text{Out}(G)$ such that $\psi \cdot H^i = A^i - H^i$, $\psi \cdot (A^i - H^i) = H^i$. Hence

$$\mu_G(t^{-1}(H)) = \mu_G(t^{-1}(H_i)) = 1/2\mu_G(G^i) = 1/2 \cdot 1/4 = 1/8.$$
Personal reminder

1. Cover part V
2. Has part V been covered?
   - Yes: Take questions
   - No: Cover part V
3. Observe remaining time $T$ (in minutes)
   - $T > 5$?
     - Yes: Go to restaurant
     - No: Apologize
   - $T < -5$?
     - Yes: Go to restaurant
     - No: Take questions
Part V.

Speculation on the partition function modulo 2
Partitions and $\tilde{\Delta}^{-1/3}$

Let

$$P(q) = \sum_{n=0}^{\infty} p(n)q^n = \prod_{n \geq 1} (1 - q^n)^{-1}$$

Thus,

$$qP(q)^{-24} = \Delta(q)$$

Or

$$q^{-1/3}P(q)^8 = \Delta(q)^{-1/3} \in \mathbb{Z}((q^{1/3})).$$

Reducing mod 2,

$$q^{-1/3} \tilde{P}(q^8) = \tilde{\Delta}(q)^{-1/3}.$$

Hence to understand $\tilde{P}$, one needs to understand $\tilde{\Delta}^{-1/3}$.
Analyzing $\tilde{\Delta}^{-1/3}$

In some sense,

$$\tilde{\Delta}^{-1/3} = \lim_{r \to \infty} \tilde{\Delta}^{(2^r - 1)/3}$$

For odd $r$, $\tilde{\Delta}^{(2^r - 1)/3}$ is in $M$, non-special according to our first conjecture, hence of density $1/8$ according to our second conjecture.
Analyzing $\tilde{\Delta}^{-1/3}$

In some sense,

$$\tilde{\Delta}^{-1/3} = \lim_{r \to \infty} \tilde{\Delta}^{(2^r-1)/3}$$

For odd $r$, $\tilde{\Delta}^{(2^r-1)/3}$ is in $M$, non-special according to our first conjecture, hence of density $1/8$ according to our second conjecture.

Hence, $\tilde{\Delta}^{-1/3}$ should also have density $1/8$, and this would imply that for $j = 0, 1$

$$A_j(x) := \# \{ n \leq x, p(n) \equiv 1 \pmod{2} \} > \frac{1}{2} \left( \frac{x}{\log(x)} \right) + o \left( \frac{x}{\log(x)} \right)$$

much closer to the conjectures $A_j(x) \sim \frac{1}{2} x$ than anything known today (best lower bounds are in $x^{1/2} \log(x)$.)
Analyzing $\tilde{\Delta}^{-1/3}$

In some sense,

$$\tilde{\Delta}^{-1/3} = \lim_{r \to \infty} \tilde{\Delta}^{(2^r - 1)/3}$$

For odd $r$, $\tilde{\Delta}^{(2^r - 1)/3}$ is in $M$, non-special according to our first conjecture, hence of density $1/8$ according to our second conjecture.

Hence, $\tilde{\Delta}^{-1/3}$ should also have density $1/8$, and this would imply that for $j = 0, 1$

$$A_j(x) := \# \{ n \leq x, p(n) \equiv 1 \pmod{2} \} > \frac{1}{2} \left(\frac{x}{\log(x)}\right) + o\left(\frac{x}{\log(x)}\right)$$

much closer to the conjectures $A_j(x) \sim \frac{1}{2}x$ that anything known today (best lower bounds are in $x^{1/2} \log(x)$.)

To make this argument work, one needs, besides our two conjectures, a strong form of effective Chebotarev, that one can perhaps obtain by Large Sieve methods.
Analyzing $\tilde{\Delta}^{-1/3}$

In some sense,

$$\tilde{\Delta}^{-1/3} = \lim_{r \to \infty} \tilde{\Delta}(2^r-1)/3$$

For odd $r$, $\tilde{\Delta}(2^r-1)/3$ is in $M$, non-special according to our first conjecture, hence of density $1/8$ according to our second conjecture.

Hence, $\tilde{\Delta}^{-1/3}$ should also have density $1/8$, and this would imply that for $j = 0, 1$

$$A_j(x) := \#\{n \leq x, p(n) \equiv 1 \pmod{2}\} > \frac{1}{2}(x/\log(x)) + o(x/\log(x))$$

much closer to the conjectures $A_j(x) \sim \frac{1}{2}x$ that anything known today (best lower bounds are in $x^{1/2} \log(x)$.)

To make this argument work, one needs, besides our two conjectures, a strong form of effective Chebotarev, that one can perhaps obtain by Large Sieve methods. At least, the method is sound numerically.