What is Reciprocity?

(an introduction to Langlands' vision)

Kapil Hari Paranjape

The Institute of Mathematical Sciences

Institute Seminar Week, 6th March 2008

The Truth about Mathematicians

Mathematicians are *lazy* people.

The Truth about Mathematicians

Mathematicians are *lazy* people.

They would rather use time thinking about how *to make a calculation simpler, . . .*

The Truth about Mathematicians

Mathematicians are *lazy* people.

They would rather use time thinking about how *to make a calculation simpler, than waste time actually doing the calculation.*

The Truth about Mathematicians

Mathematicians are *lazy* people.

They would rather use time thinking about how *to make a calculation simpler, than waste time actually doing the calculation.*

Good Mathematicians *still* manage to get the job done.

The Truth about Mathematicians

Mathematicians are *lazy* people.

They would rather use time thinking about how *to make a calculation simpler, than waste time actually doing the calculation.*

Good Mathematicians *still* manage to get the job done.

In other words, they actually *carry out the simpler procedure to complete the calculations.*

The Truth about Mathematicians

Mathematicians are *lazy* people.

They would rather use time thinking about how *to make a calculation simpler, than waste time actually doing the calculation.*

Good Mathematicians *still* manage to get the job done.

In other words, they actually *carry out the simpler procedure to complete the calculations.*

Mathematical philosophers get *others* to do the hard work.

The Truth about Mathematicians

Mathematicians are *lazy* people.

They would rather use time thinking about how *to make a calculation simpler, than waste time actually doing the calculation.*

Good Mathematicians *still* manage to get the job done.

In other words, they actually *carry out the simpler procedure to complete the calculations.*

Mathematical philosophers get *others* to do the hard work.

They chalk out a programme to carry out all kinds of calculations very quickly . . .

The Truth about Mathematicians

Mathematicians are *lazy* people.

They would rather use time thinking about how *to make a calculation simpler, than waste time actually doing the calculation.*

Good Mathematicians *still* manage to get the job done.

In other words, they actually *carry out the simpler procedure to complete the calculations.*

Mathematical philosophers get *others* to do the hard work.

They chalk out a programme to carry out all kinds of calculations very quickly and let others carry out this programme.

Arithmetic Modulo N

- The set $\mathbb{F}_N = \{0, \ldots, N-1\}$ carries the usual arithmetic operations; addition, multiplication and subtraction.

Arithmetic Modulo N

- The set $\mathbb{F}_N = \{0, \ldots, N-1\}$ carries the usual arithmetic operations; addition, multiplication and subtraction.
- Method: Apply the "usual" operation and then take the remainder after division by N.

Arithmetic Modulo N

- The set $\mathbb{F}_N = \{0, \dots, N-1\}$ carries the usual arithmetic operations; addition, multiplication and subtraction.
- Method: Apply the "usual" operation and then take the remainder after division by N.
  Negative numbers give positive remainders!

Arithmetic Modulo N

- The set $\mathbb{F}_N = \{0, \ldots, N-1\}$ carries the usual arithmetic operations; addition, multiplication and subtraction.
- Method: Apply the "usual" operation and then take the remainder after division by N.
  Negative numbers give positive remainders!
- When N is prime. This is a field.

Arithmetic Modulo N

- The set $\mathbb{F}_N = \{0, \ldots, N-1\}$ carries the usual arithmetic operations; addition, multiplication and subtraction.
- Method: Apply the "usual" operation and then take the remainder after division by N.
  Negative numbers give positive remainders!
- When N is prime. This is a field.
  Euclid's algorithm provides a way to divide by a non-zero element of this set.
  If $ab + kN = 1$ then $ab = 1$ modulo N.

How large is N?

For the rest of this talk N will be a *large* prime.

How large is N?

For the rest of this talk N will be a *large* prime.

```
? N=prime(random(1000000000))
```

How large is N?

For the rest of this talk N will be a *large* prime.

```
? N=prime(random(1000000000))
N=726377293
```

How large is N?

For the rest of this talk N will be a *large* prime.

```
? N=prime(random(1000000000))
N=726377293
```

For most humans this is probably large enough!

How large is N?

For the rest of this talk N will be a *large* prime.

```
? N=prime(random(1000000000))
N=726377293
```

For most humans this is probably large enough!
If you are as fast as a Xeon processor you can take about 300 more digits.

How large is N?

For the rest of this talk N will be a *large* prime.

```
? N=prime(random(1000000000))
N=726377293
```

For most humans this is probably large enough!
If you are as fast as a Xeon processor you can take about 300 more digits.
So take N as

```
1495145408827625078292664907290148913964441697228976
4445366358595008337533666363448445244767319428213864
1842496975368703352911650953541829107677855943186814
2223164587340540087754181159128253617165405682750216
1712347287973437514175773829454091516732839564970608
0984751898535619484306219840829692491753915601587
```

How large is N?

For the rest of this talk N will be a *large* prime.

```
? N=prime(random(1000000000))
N=726377293
```

For most humans this is probably large enough!
If you are as fast as a Xeon processor you can take about 300 more digits.
So take N as

```
1495145408827625078292664907290148913964441697228976
4445366358595008337533666363448445244767319428213864
1842496975368703352911650953541829107677855943186814
2223164587340540087754181159128253617165405682750216
1712347287973437514175773829454091516732839564970608
0984751898535619484306219840829692491753915601587
```

It *is* a prime!

Squares modulo N

Elements of $\mathbb{F}_N$ like 1, 4, 9 and 16 are squares modulo N.

Squares modulo N

Elements of $\mathbb{F}_N$ like 1, 4, 9 and 16 are squares modulo N.
However, there *could be* other squares modulo N. For example,

Squares modulo N

Elements of $\mathbb{F}_N$ like 1, 4, 9 and 16 are squares modulo N. However, there *could be* other squares modulo N. For example,

$$5 = 6^2 - 31$$

so 5 is a square modulo 31.

Squares modulo N

Elements of $\mathbb{F}_N$ like 1, 4, 9 and 16 are squares modulo N.
However, there *could be* other squares modulo N. For example,

$$5 = 6^2 - 31$$

so 5 is a square modulo 31.
Even when N is large there are some uniformities. For example,

If $N = 4M + 1$ then -1 is a square modulo N.

Squares modulo N

Elements of $\mathbb{F}_N$ like 1, 4, 9 and 16 are squares modulo N.
However, there *could be* other squares modulo N. For example,

$$5 = 6^2 - 31$$

so 5 is a square modulo 31.
Even when N is large there are some uniformities. For example,

If $N = 4M + 1$ then -1 is a square modulo N.

How do we decide whether 5 is a square modulo 726377293?

A “bad” solution

We get a “quick and dirty” solution based on some observations.

A "bad" solution

We get a "quick and dirty" solution based on some observations.

- The collection $\mathbb{F}_N^* = \{1, \ldots, N-1\}$ forms a *cyclic* group under multiplication modulo N.

A “bad” solution

We get a “quick and dirty” solution based on some observations.

- The collection $\mathbb{F}_N^* = \{1, \ldots, N-1\}$ forms a *cyclic* group under multiplication modulo N.
- If 5 is a square, then its order can be at most $(N-1)/2$.

A "bad" solution

We get a "quick and dirty" solution based on some observations.

- The collection $\mathbb{F}_N^* = \{1, \ldots, N-1\}$ forms a *cyclic* group under multiplication modulo N.
- If 5 is a square, then its order can be at most $(N-1)/2$.
- We can calculate $5^{(N-1)/2}$ modulo N and check whether it is 1 or not.

A "bad" solution

We get a "quick and dirty" solution based on some observations.

- The collection $\mathbb{F}_N^* = \{1, \ldots, N-1\}$ forms a *cyclic* group under multiplication modulo N.
- If 5 is a square, then its order can be at most $(N-1)/2$.
- We can calculate $5^{(N-1)/2}$ modulo N and check whether it is 1 or not.

However, we also observe that this method is too painful.

A "bad" solution

We get a "quick and dirty" solution based on some observations.

- The collection $\mathbb{F}_N^* = \{1, \ldots, N-1\}$ forms a *cyclic* group under multiplication modulo N.
- If 5 is a square, then its order can be at most $(N-1)/2$.
- We can calculate $5^{(N-1)/2}$ modulo N and check whether it is 1 or not.

However, we also observe that this method is too painful.

In particular, it involves calculations with big numbers like 726377293!

Enter Carl Friedrich Gauss

We already know that Gauss found a lazy way to add numbers from 1 to 100.

Enter Carl Friedrich Gauss

We already know that Gauss found a lazy way to add numbers from 1 to 100. So he was a good mathematician! Q.E.D.

Enter Carl Friedrich Gauss

We already know that Gauss found a lazy way to add numbers from 1 to 100. So he was a good mathematician! Q.E.D.

Gauss asked himself whether there is a way to decide whether 5 is a square modulo large primes N,

Enter Carl Friedrich Gauss

We already know that Gauss found a lazy way to add numbers from 1 to 100. So he was a good mathematician! Q.E.D.

Gauss asked himself whether there is a way to decide whether 5 is a square modulo large primes N, while calculating with "small" numbers of the order of 5

Enter Carl Friedrich Gauss

We already know that Gauss found a lazy way to add numbers from 1 to 100. So he was a good mathematician! Q.E.D.

Gauss asked himself whether there is a way to decide whether 5 is a square modulo large primes N, while calculating with "small" numbers of the order of 5 rather than large numbers of the order of N.

Enter Carl Friedrich Gauss

We already know that Gauss found a lazy way to add numbers from 1 to 100. So he was a good mathematician! Q.E.D.

Gauss asked himself whether there is a way to decide whether 5 is a square modulo large primes N, while calculating with "small" numbers of the order of 5 rather than large numbers of the order of N.

Gauss' law of Quadratic Reciprocity is his answer.

Enter Carl Friedrich Gauss

We already know that Gauss found a lazy way to add numbers from 1 to 100. So he was a good mathematician! Q.E.D.

Gauss asked himself whether there is a way to decide whether 5 is a square modulo large primes N, while calculating with "small" numbers of the order of 5 rather than large numbers of the order of N.

Gauss' law of Quadratic Reciprocity is his answer.

The royal road to quadratic reciprocity goes via *cyclotomic numbers*. (Which is poetic name for the roots of unity.)

An observation about fifth roots of unity

Let ξ denote a fifth root of 1.

An observation about fifth roots of unity

Let ξ denote a fifth root of 1. Then ξ satisfies the equation.

$$\xi^4 + \xi^3 + \xi^2 + \xi + 1 = 0$$

An observation about fifth roots of unity

Let ξ denote a fifth root of 1. Then ξ satisfies the equation.

$$\xi^4 + \xi^3 + \xi^2 + \xi + 1 = 0$$

Putting $\eta = \xi + \xi^4$, we get

$$\eta^2 = (\xi + \xi^4)^2 = \xi^2 + \xi^3 + 2 = 1 - (\xi + \xi^4) = 1 - \eta$$

An observation about fifth roots of unity

Let ξ denote a fifth root of 1. Then ξ satisfies the equation.

$$\xi^4 + \xi^3 + \xi^2 + \xi + 1 = 0$$

Putting $\eta = \xi + \xi^4$, we get

$$\eta^2 = (\xi + \xi^4)^2 = \xi^2 + \xi^3 + 2 = 1 - (\xi + \xi^4) = 1 - \eta$$

In other words

$$(1 + 2\eta)^2 = 1 + 4\eta + 4\eta^2 = 1 + 4 = 5$$

An observation about fifth roots of unity

Let ξ denote a fifth root of 1. Then ξ satisfies the equation.

$$\xi^4 + \xi^3 + \xi^2 + \xi + 1 = 0$$

Putting $\eta = \xi + \xi^4$, we get

$$\eta^2 = (\xi + \xi^4)^2 = \xi^2 + \xi^3 + 2 = 1 - (\xi + \xi^4) = 1 - \eta$$

In other words

$$(1 + 2\eta)^2 = 1 + 4\eta + 4\eta^2 = 1 + 4 = 5$$

So $(1 + 2\eta)$ is *a* square root of 5.

The Frobenius automorphism

When N is a prime, the binomial theorem says that

$$(x+y)^N = x^N + y^N \text{ modulo } N$$

The Frobenius automorphism

When N is a prime, the binomial theorem says that

$$(x+y)^N = x^N + y^N \text{ modulo } N$$

We can also apply this to *matrices* x and y as long as $xy = yx$.

The Frobenius automorphism

When N is a prime, the binomial theorem says that

$$(x+y)^N = x^N + y^N \text{ modulo } N$$

We can also apply this to *matrices* x and y as long as $xy = yx$. Moreover, if x is a matrix with entries in $\mathbb{F}_N$, then

$$x^N = x \text{ modulo } N \text{ if and only if } x = k\,\mathrm{Id}$$

i. e. x is a diagonal matrix with $k \in \mathbb{F}_N$.

Matrices solve equations

Any equation can be solved using matrices and vice versa.

Matrices solve equations

Any equation can be solved using matrices and vice versa. Solutions of the equation

$$T^n + a_1 T^{N-1} + \dots a_n = 0$$

Matrices solve equations

Any equation can be solved using matrices and vice versa. Solutions of the equation

$$T^n + a_1 T^{N-1} + \dots a_n = 0$$

are represented as the matrix

$$M_f = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ -a_n & -a_{n-1} & -a_{n-2} & \dots & -a_1 \end{pmatrix}$$

Matrices solve equations

Any equation can be solved using matrices and vice versa. Solutions of the equation

$$T^n + a_1 T^{N-1} + \ldots a_n = 0$$

are represented as the matrix

$$M_f = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ -a_n & -a_{n-1} & -a_{n-2} & \ldots & -a_1 \end{pmatrix}$$

So henceforth when we write a solution of an equation we mean the corresponding matrix!

The fifth root of unity as a matrix

For example, the fifth root of unity can be represented by the matrix

$$\xi = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & -1 & -1 & -1 \end{pmatrix}$$

In particular, we can check whether $\eta = \xi + \xi^4$ is a scalar matrix modulo N by checking whether $\eta^N = \eta$.

Easy calculation

Since 726377293 is 3 modulo 5 we have

Easy calculation

Since 726377293 is 3 modulo 5 we have

$$\xi^{726377293} = \xi^3$$

Easy calculation

Since 726377293 is 3 modulo 5 we have

$$\xi^{726377293} = \xi^3$$

Moreover,

$$(\xi^4)^{726377293} = (\xi^3)^4 = \xi^2$$

Easy calculation

Since 726377293 is 3 modulo 5 we have

$$\xi^{726377293} = \xi^3$$

Moreover,

$$(\xi^4)^{726377293} = (\xi^3)^4 = \xi^2$$

Hence we see that

$$\eta^{726377293} = \xi^3 + \xi^2 = 1 - \eta \text{ modulo } 726377293$$

Easy calculation

Since 726377293 is 3 modulo 5 we have

$$\xi^{726377293} = \xi^3$$

Moreover,

$$(\xi^4)^{726377293} = (\xi^3)^4 = \xi^2$$

Hence we see that

$$\eta^{726377293} = \xi^3 + \xi^2 = 1 - \eta \text{ modulo } 726377293$$

In other words, η is not an integer modulo 726377293. It follows that 5 is not a square modulo 726377293.

All N at once

If N reduces to 1 or 4 modulo 5

All N at once

If N reduces to 1 or 4 modulo 5

then 5 *is a square modulo* N.

All N at once

If N reduces to 1 or 4 modulo 5

then 5 *is a square modulo* N.

if N reduces to 2 or 3 modulo 5

All N at once

If N reduces to 1 or 4 modulo 5

then 5 *is a square modulo* N.

if N reduces to 2 or 3 modulo 5

then 5 *is not a square modulo* N.

All N at once

If N reduces to 1 or 4 modulo 5

then 5 *is a square modulo* N.

if N reduces to 2 or 3 modulo 5

then 5 *is not a square modulo* N.

It's that simple!

Painful Calculation

```
? N=726377293
N = 726377293
? t=(N-1)/2;a=Mod(5,N);b=Mod(1,N);sp="  ";
? while(t,printp(t,sp,a,sp,b);if(t\%2,b=a*b);\
  a=a^2;t=divrem(t,2)[1]);printp(t,sp,a,sp,b)
```

Painful Calculation

```
? N=726377293
N = 726377293
? t=(N-1)/2;a=Mod(5,N);b=Mod(1,N);sp="  ";
? while(t,printp(t,sp,a,sp,b);if(t\%2,b=a*b);\
  a=a^2;t=divrem(t,2)[1]);printp(t,sp,a,sp,b)
```

```
 363188646            (5 mod N)            (1 mod N)
 181594323           (25 mod N)            (1 mod N)
  90797161          (625 mod N)           (25 mod N)
```

. . . (24 lines elided!)

```
         2   (116419545 mod N)   (62288545 mod N)
         1   (229055375 mod N)   (62288545 mod N)
         0    (15956006 mod N)          (N-1 mod N)
```

Painful Calculation

```
? N=726377293
N = 726377293
? t=(N-1)/2;a=Mod(5,N);b=Mod(1,N);sp="  ";
? while(t,printp(t,sp,a,sp,b);if(t\%2,b=a*b);\
  a=a^2;t=divrem(t,2)[1]);printp(t,sp,a,sp,b)

 363188646          (5 mod N)          (1 mod N)
 181594323         (25 mod N)          (1 mod N)
  90797161        (625 mod N)         (25 mod N)
```

...(24 lines elided!)

```
         2   (116419545 mod N)   (62288545 mod N)
         1   (229055375 mod N)   (62288545 mod N)
         0    (15956006 mod N)        (N-1 mod N)
```

This method is too painful.

When is 7 a square modulo N?

We note that

$$\left((\tau+\tau^{-1})+(\tau^3+\tau^{-3})+(\tau^9+\tau^{-9})\right)^2 = 7$$

where τ is a 28-th root of unity.

When is 7 a square modulo N?

We note that

$$\left((\tau+\tau^{-1})+(\tau^3+\tau^{-3})+(\tau^9+\tau^{-9})\right)^2=7$$

where τ is a 28-th root of unity.
Thus $\tau \mapsto \tau^k$ takes $\sqrt{7}$ to itself if and only if k is

> *1 or* $27 = 28 - 1$, *or*
> *3 or* $25 = 28 - 3$, *or*
> *9 or* $19 = 28 - 9$ *modulo 28.*

When is 7 a square modulo N?

We note that

$$\left((\tau + \tau^{-1}) + (\tau^3 + \tau^{-3}) + (\tau^9 + \tau^{-9})\right)^2 = 7$$

where τ is a 28-th root of unity.
Thus $\tau \mapsto \tau^k$ takes $\sqrt{7}$ to itself if and only if k is

> 1 *or* $27 = 28 - 1$, *or*
> *3 or* $25 = 28 - 3$, *or*
> *9 or* $19 = 28 - 9$ *modulo 28.*

Thus, 7 is a square modulo N if and only if N is congruent to 1, 3, 9, 19, 25 or 27 modulo 28.

Conceptual statment of Quadratic reciprocity

The problem of studying the solutions of $T^2 - a = 0$ *modulo a large prime* N

Conceptual statment of Quadratic reciprocity

The problem of studying the solutions of $T^2 - a = 0$ *modulo a large prime* N

is equivalent *to*

Conceptual statment of Quadratic reciprocity

The problem of studying the solutions of $T^2 - a = 0$ *modulo a large prime* N

is equivalent *to*

the problem of studying the N*-th power map acting on the* b*-th roots of unity*

Conceptual statment of Quadratic reciprocity

The problem of studying the solutions of $T^2 - a = 0$ modulo a large prime N

is equivalent *to*

the problem of studying the N-th power map acting on the b-th roots of unity, where b is somehow derived from a.

Conceptual statment of Quadratic reciprocity

The problem of studying the solutions of $T^2 - a = 0$ modulo a large prime N

is equivalent *to*

the problem of studying the N-th power map acting on the b-th roots of unity, where b is somehow derived from a.

Actually b is either a or $4a$ depending on whether a is 1 or 3 modulo 4.

The Theorem of Kronecker and Weber

Indeed, there is a class A of algebraic equations $f(T) = 0$ such that

> *The problem of studying the equation $f(T) = 0$ modulo a large prime N*
>
> *is equivalent to*
>
> *the problem of studying the behaviour of the N-th power map acting on the b-th roots of unity*

The Theorem of Kronecker and Weber

Indeed, there is a class A of algebraic equations $f(T) = 0$ such that

> *The problem of studying the equation $f(T) = 0$ modulo a large prime N*
>
> *is equivalent to*
>
> *the problem of studying the behaviour of the N-th power map acting on the b-th roots of unity, where b is (somehow) derived from the coefficients of $f(T)$.*

The Theorem of Kronecker and Weber

Indeed, there is a class A of algebraic equations $f(T) = 0$ such that

> *The problem of studying the equation $f(T) = 0$ modulo a large prime N*
>
> *is equivalent to*
>
> *the problem of studying the behaviour of the N-th power map acting on the b-th roots of unity, where b is (somehow) derived from the coefficients of $f(T)$.*

The class A is called the class of *abelian equations and b is called the* conductor of the equation $f(T)$.

The Importance of Linear Algebra

The reason why studying the N-th power map on the roots of unity is easy can be explained as follows.

The Importance of Linear Algebra

The reason why studying the N-th power map on the roots of unity is easy can be explained as follows.

The N-th power map permutes the roots of unity

The Importance of Linear Algebra

The reason why studying the N-th power map on the roots of unity is easy can be explained as follows.

The N-th power map permutes the roots of unity

By suitable representation of the b-th roots of unity as as matrix X_b, we see that the N-th power map is given by

$$X_b \mapsto T_N X_b T_N^{-1}$$

where T_N is just a cyclic permutation matrix.

The Importance of Linear Algebra

The reason why studying the N-th power map on the roots of unity is easy can be explained as follows.

The N-th power map permutes the roots of unity

By suitable representation of the b-th roots of unity as as matrix X_b, we see that the N-th power map is given by

$$X_b \mapsto T_N X_b T_N^{-1}$$

where T_N is just a cyclic permutation matrix.

Question: Can we find a similar T_N for other problems?

The Trace formula of Weil and Grothendieck

Given a system S of algebraic equations in any number of variables:

The Trace formula of Weil and Grothendieck

Given a system S of algebraic equations in any number of variables:

1. there is a finite collection of vector spaces $H^i(S)$; one for each i between 0 and $2\dim(S)$.

The Trace formula of Weil and Grothendieck

Given a system S of algebraic equations in any number of variables:

1. there is a finite collection of vector spaces $H^i(S)$; one for each i between 0 and $2\dim(S)$.
2. for each large prime N, there is an automorphism $T_{i,N}$ of $H^i(S)$.

The Trace formula of Weil and Grothendieck

Given a system S of algebraic equations in any number of variables:

1. there is a finite collection of vector spaces $H^i(S)$; one for each i between 0 and $2\dim(S)$.
2. for each large prime N, there is an automorphism $T_{i,N}$ of $H^i(S)$.

The number of solutions of S modulo N is given by the simple formula

The Trace formula of Weil and Grothendieck

Given a system S of algebraic equations in any number of variables:

1. there is a finite collection of vector spaces $H^i(S)$; one for each i between 0 and $2\dim(S)$.
2. for each large prime N, there is an automorphism $T_{i,N}$ of $H^i(S)$.

The number of solutions of S modulo N is given by the simple formula

$$\#S(\mathbb{F}_N) = \sum_{k=0}^{2\dim(S)} (-1)^k \operatorname{Trace}(T_{k,N})$$

The Trace formula of Weil and Grothendieck

Given a system S of algebraic equations in any number of variables:

1. there is a finite collection of vector spaces $H^i(S)$; one for each i between 0 and $2\dim(S)$.
2. for each large prime N, there is an automorphism $T_{i,N}$ of $H^i(S)$.

The number of solutions of S modulo N is given by the simple formula

$$\#S(\mathbb{F}_N) = \sum_{k=0}^{2\dim(S)} (-1)^k \operatorname{Trace}(T_{k,N})$$

Since we will study each k separately in what follows. I will drop the subscript k hereon.

It's too easy!

"Determine the trace of a matrix T_N."

It's too easy!

"Determine the trace of a matrix T_N."

Sounds easy enough! What's the catch?

It's too easy!

"Determine the trace of a matrix T_N."

Sounds easy enough! What's the catch?

The Catch: The phrase "there exists a matrix T_N" says nothing about how to *construct* it!

Langlands' Philosophy

Langlands' Philosophy

1. We expect the T_N's to have a nice distribution so that the L-function

$$L(\{T_N\}, s) = \prod_N \det\left(1 - T_N N^{-s}\right)^{-1}$$

should have nice analytic properties.

Langlands' Philosophy

1. We expect the T_N's to have a nice distribution so that the L-function
$$L(\{T_N\}, s) = \prod_N \det\left(1 - T_N N^{-s}\right)^{-1}$$
should have nice analytic properties.
2. The theory of "Automorphic representations" gives a large list of such collections $\{T_N\}$ with nice analytic properties.

Langlands' Philosophy

1. We expect the T_N's to have a nice distribution so that the L-function

$$L(\{T_N\}, s) = \prod_N \det\left(1 - T_N N^{-s}\right)^{-1}$$

   should have nice analytic properties.
2. The theory of "Automorphic representations" gives a large list of such collections $\{T_N\}$ with nice analytic properties.

Question: Wouldn't it be nice if the second list contained the first?

Langlands' Philosophy

1. We expect the T_N's to have a nice distribution so that the L-function
$$L(\{T_N\}, s) = \prod_N \det\left(1 - T_N N^{-s}\right)^{-1}$$
should have nice analytic properties.
2. The theory of "Automorphic representations" gives a large list of such collections $\{T_N\}$ with nice analytic properties.

Question: Wouldn't it be nice if the second list contained the first?
Since it would be *nice* — so we conjecture it to be so!

Langlands' Philosophy

1. We expect the T_N's to have a nice distribution so that the L-function

$$L(\{T_N\}, s) = \prod_N \det\left(1 - T_N N^{-s}\right)^{-1}$$

   should have nice analytic properties.
2. The theory of "Automorphic representations" gives a large list of such collections $\{T_N\}$ with nice analytic properties.

Question: Wouldn't it be nice if the second list contained the first?
Since it would be *nice* — so we conjecture it to be so!
Actually, there is a bit more evidence than that!

Are we there yet?

The construction of automorphic representations is analytic...

Are we there yet?

The construction of automorphic representations is analytic, and analysis does not generally yield exact formulae.

Are we there yet?

The construction of automorphic representations is analytic, and analysis does not generally yield exact formulae.
But we want integers!

Are we there yet?

The construction of automorphic representations is analytic, and analysis does not generally yield exact formulae.
But we want integers!

Solution (Proposed in collaboration with Dinakar Ramakrishnan.)

Are we there yet?

The construction of automorphic representations is analytic, and analysis does not generally yield exact formulae.
But we want integers!

Solution (Proposed in collaboration with Dinakar Ramakrishnan.)
Construct canonical algebraic problems S_π for each (or enough) automorphic representations.

Are we there yet?

The construction of automorphic representations is analytic, and analysis does not generally yield exact formulae.
But we want integers!

Solution (Proposed in collaboration with Dinakar Ramakrishnan.)
Construct canonical algebraic problems S_π for each (or enough) automorphic representations.

Idea S_π generalise the role played "roots of unity" in Kronecker-Weber.

Are we there yet?

The construction of automorphic representations is analytic, and analysis does not generally yield exact formulae.
But we want integers!

Solution (Proposed in collaboration with Dinakar Ramakrishnan.)
Construct canonical algebraic problems S_π for each (or enough) automorphic representations.

Idea S_π generalise the role played "roots of unity" in Kronecker-Weber.

We have constructed examples of S_π for a number of cases and proposed some candidate classes.

A small step for Langlands . . .

Elliptic curves E are given by an equation of the form

$$y^2 = x^3 + ax + b$$

A small step for Langlands . . .

Elliptic curves E are given by an equation of the form

$$y^2 = x^3 + ax + b$$

In this case, $T_{0,N} = 1$ and $T_{2,N}$ is also easy

A small step for Langlands . . .

Elliptic curves E are given by an equation of the form

$$y^2 = x^3 + ax + b$$

In this case, $T_{0,N} = 1$ and $T_{2,N}$ is also easy

So we study $T_N = T_{1,N}$ which is a 2×2 matrix.

A small step for Langlands . . .

Elliptic curves E are given by an equation of the form

$$y^2 = x^3 + ax + b$$

In this case, $T_{0,N} = 1$ and $T_{2,N}$ is also easy

So we study $T_N = T_{1,N}$ which is a 2×2 matrix. Let $a_N = \mathrm{Trace}(T_N)$.

A small step for Langlands ...

Elliptic curves E are given by an equation of the form

$$y^2 = x^3 + ax + b$$

In this case, $T_{0,N} = 1$ and $T_{2,N}$ is also easy

So we study $T_N = T_{1,N}$ which is a 2×2 matrix. Let $a_N = \mathrm{Trace}(T_N)$.

Wiles and Taylor showed that

$$L(E, s) = L(\{T_N\}, s) = \prod_N \left(1 - a_N N^{-s} + N^{1-2s}\right)^{-1}$$

is the zeta function of a modular form f of level $\Delta(a, b)$.

A small step for Langlands ...

Elliptic curves E are given by an equation of the form

$$y^2 = x^3 + ax + b$$

In this case, $T_{0,N} = 1$ and $T_{2,N}$ is also easy

So we study $T_N = T_{1,N}$ which is a 2×2 matrix. Let $a_N = \mathrm{Trace}(T_N)$.

Wiles and Taylor showed that

$$L(E,s) = L(\{T_N\}, s) = \prod_N \left(1 - a_N N^{-s} + N^{1-2s}\right)^{-1}$$

is the zeta function of a modular form f of level $\Delta(a,b)$. (*Fermat's Last Theorem was an insignificant consequence!*)

A small step for Langlands ...

Elliptic curves E are given by an equation of the form

$$y^2 = x^3 + ax + b$$

In this case, $T_{0,N} = 1$ and $T_{2,N}$ is also easy

So we study $T_N = T_{1,N}$ which is a 2×2 matrix. Let $a_N = \mathrm{Trace}(T_N)$.

Wiles and Taylor showed that

$$L(E,s) = L(\{T_N\},s) = \prod_N \left(1 - a_N N^{-s} + N^{1-2s}\right)^{-1}$$

is the zeta function of a modular form f of level $\Delta(a,b)$. (*Fermat's Last Theorem was an insignificant consequence!*)

There are only finitely many modular forms of a given level.

A small step for Langlands . . .

Elliptic curves E are given by an equation of the form

$$y^2 = x^3 + ax + b$$

In this case, $T_{0,N} = 1$ and $T_{2,N}$ is also easy

So we study $T_N = T_{1,N}$ which is a 2×2 matrix. Let $a_N = \mathrm{Trace}(T_N)$.

Wiles and Taylor showed that

$$L(E, s) = L(\{T_N\}, s) = \prod_N \left(1 - a_N N^{-s} + N^{1-2s}\right)^{-1}$$

is the zeta function of a modular form f of level $\Delta(a, b)$. (*Fermat's Last Theorem was an insignificant consequence!*)

There are only finitely many modular forms of a given level.

So given the level and a few coefficients one can determine a *unique* modular form f_E.

A small step for Langlands . . .

Elliptic curves E are given by an equation of the form

$$y^2 = x^3 + ax + b$$

In this case, $T_{0,N} = 1$ and $T_{2,N}$ is also easy

So we study $T_N = T_{1,N}$ which is a 2×2 matrix. Let $a_N = \mathrm{Trace}(T_N)$.

Wiles and Taylor showed that

$$L(E,s) = L(\{T_N\}, s) = \prod_N \left(1 - a_N N^{-s} + N^{1-2s}\right)^{-1}$$

is the zeta function of a modular form f of level $\Delta(a,b)$. (*Fermat's Last Theorem was an insignificant consequence!*)
There are only finitely many modular forms of a given level.
So given the level and a few coefficients one can determine a *unique* modular form f_E.

Question: Can one improve on Schoof's algorithm by using this to compute a_N for large N?

A small step for Langlands ...

Elliptic curves E are given by an equation of the form

$$y^2 = x^3 + ax + b$$

In this case, $T_{0,N} = 1$ and $T_{2,N}$ is also easy

So we study $T_N = T_{1,N}$ which is a 2×2 matrix. Let $a_N = \mathrm{Trace}(T_N)$.

Wiles and Taylor showed that

$$L(E,s) = L(\{T_N\}, s) = \prod_N \left(1 - a_N N^{-s} + N^{1-2s}\right)^{-1}$$

is the zeta function of a modular form f of level $\Delta(a,b)$. (*Fermat's Last Theorem was an insignificant consequence!*)
There are only finitely many modular forms of a given level.
So given the level and a few coefficients one can determine a *unique* modular form f_E.

Question: Can one improve on Schoof's algorithm by using this to compute a_N for large N? ... Can one make the giant leap?