# Calculation and arithmetic significance of modular forms

Gabor Wiese

07/11/2014

# An elliptic curve

Let us consider the elliptic curve given by the (affine) equation

$$y^2 + y = x^3 - x^2 - 10x - 20$$

We show its real shape.
We count its points modulo primes. We rather count the points of the projective curve

$$y^2z + yz^2 = x^3 - x^2z - 10xz^2 - 20z^3$$

and find

| prime | 2 | 3 | 5 | 7 | 13 | 17 | 19 | 23 | 29 | 31 | 37 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| nb points | 5 | 5 | 5 | 10 | 10 | 20 | 20 | 25 | 30 | 25 | 35 |

# Modular (Manin) symbols

Let us consider $\mathbb{P}^1(\mathbb{F}_{11})$, the projective line over the finite field $\mathbb{F}_{11} = GF(11)$, i.e.

$$(0:1), (1:1), (2:1), (3:1), (4:1), (5:1), (6:1), (7:1), (8:1), (9:1), (10:1), (1:0)$$

Consider $A := \mathbb{Q}[\mathbb{P}^1(\mathbb{F}_{11})]$, that is, the set of formal $\mathbb{Q}$-linear combinations of the elements of $\mathbb{P}^1(\mathbb{F}_{11})$, i.e.

$$a_0(0:1) + a_1(1:1) + a_2(2:1) + \ldots + a_{10}(10:1) + a_\infty(1:0)$$

For an integer matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, we consider $(u:v)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.
This maps $\mathbb{P}^1(\mathbb{F}_{11})$ to itself (a 'right action'; by transposition we also get a left action).
Let $\sigma = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\tau = \left(\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Put

$$M := A/\big(A(1+\sigma) + A(1+\tau+\tau^2)\big).$$

This turns out to be a $\mathbb{Q}$-vector space of dimension 3:
modular (Manin) symbols of level 11 and weight 2.

# Modular (Manin) symbols (ctd.)

Inside $M = A/\big(A(1+\sigma) + A(1+\tau+\tau^2)\big)$ we take $C$, the cuspidal part of the plus-subspace (easy to define). It is a $\mathbb{Q}$-vector space of dimension 1. For a positive integer $n$ define the set

$$\mathcal{X}_n = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbb{Z}^{2\times 2} \mid \det = n, a > b \geq 0, d > c \geq 0\}.$$

For instance

$$\mathcal{X}_3 = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 1 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 2 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 2 \\ 0 & 1 \end{smallmatrix}\right)\}.$$

Define the Hecke operator $T_n$ (via the left action of matrices on $\mathbb{P}^1(\mathbb{F}_{11})$)

$$T_n : C \to C, \quad c \mapsto \sum_{m \in \mathcal{X}_n} m.c$$

| n | 2 | 3 | 5 | 7 | 13 | 17 | 19 | 23 | 29 | 31 | 37 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $T_n$ | -2 | -1 | 1 | -2 | 4 | -2 | 0 | -1 | 0 | 7 | 3 |

# Comparison

Recall the two tables:

| prime | 2 | 3 | 5 | 7 | 13 | 17 | 19 | 23 | 29 | 31 | 37 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| nb points | 5 | 5 | 5 | 10 | 10 | 20 | 20 | 25 | 30 | 25 | 35 |
| $T_p$ | -2 | -1 | 1 | -2 | 4 | -2 | 0 | -1 | 0 | 7 | 3 |

We observe the fundamental rule:

$$T_p = p + 1 - \text{nb points}.$$

# A modular form

Define the Fourier series (with $q = e^{2\pi i z}$)

$$f(z) = \sum_{n=1}^{\infty} T_n \cdot q^n = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 + \dots$$

Let $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ be the upper half plane.
Then, $f$ is a holomorphic function $\mathbb{H} \to \mathbb{C}$ such that

$$f\left(\frac{az+b}{11cz+d}\right) = (11cz+d)^2 \cdot f(z) \text{ for all } \left(\begin{smallmatrix} a & b \\ 11c & d \end{smallmatrix}\right) \in \mathbb{Z}^{2\times 2} \text{ with } \det = 1,$$

a modular form of level 11 and weight 2.
We plot it in the unit disk $\mathbb{D}$ via

$$\mathbb{D} \to \mathbb{H}, \quad \tau \mapsto i\frac{1+\tau}{1-\tau}.$$

# What is going on?

## Theorem 1 (Manin, 1970s).

*Modular (Manin) symbols always compute modular forms.*

$\rightarrow$ The 'standard way' to compute modular forms.
$\rightarrow$ No surprise that $f = \sum_{n=1}^{\infty} T_n q^n$ is a modular form.

## Theorem 2 (Wiles et al, 1995, 2000).

*Every elliptic curve over $\mathbb{Q}$ is modular.*

## Corollary (Fermat's Last Theorem).

*For $n \geq 3$, there are no integers $a, b, c \geq 1$ s.t. $a^n + b^n = c^n$.*

Sketch of proof. Enough with $n = p \geq 3$ prime.
Suppose $a^p + b^p = c^p$ with integers $a, b, c \geq 1$.
Consider elliptic curve ('Frey curve') $E : y^2 = x(x - a^p)(x + b^p)$.
By modularity theorem (precise version): $E$ comes from a modular form of level 2 and weight 2.
But, there is no such form. Contradiction!

# Factorisation types

Consider the polynomial $f(X) = X^6 - 6X^4 + 9X^2 + 23$.
We factor it over $\mathbb{F}_p$ into irreducibles.

| $p$ | factorisation |
|---|---|
| 5 | $(X^2+3)(X^2+X+1)(X^2+4X+1)$ |
| 13 | $(X^3+10X+4)(X^3+10X+9)$ |
| 17 | $(X^2+3)(X^2+2X+6)(X^2+15X+6)$ |
| 19 | $(X^2+9)(X^2+X+12)(X^2+18X+12)$ |
| 31 | $(X^3+28X+15)(X^3+28X+16)$ |
| 47 | $(X^3+44X+20)(X^3+44X+27)$ |
| 53 | $(X^2+22)(X^2+5X+25)(X^2+48X+25)$ |
| 59 | $(X+9)(X+21)(X+29)(X+30)(X+38)(X+50)$ |
| 73 | $(X^3+70X+14)(X^3+70X+59)$ |
| 97 | $(X^2+39)(X^2+41X+42)(X^2+56X+42)$ |
| 101 | $(X+4)(X+28)(X+32)(X+69)(X+73)(X+97)$ |

# Factorisation types

Consider the polynomial $f(X) = X^6 - 6X^4 + 9X^2 + 23$.
We factor it over $\mathbb{F}_p$ into irreducibles.

| $p$ | factorisation |
|---|---|
| 5 | ()()() |
| 13 | ()() |
| 17 | ()()() |
| 19 | ()()() |
| 31 | ()() |
| 47 | ()() |
| 53 | ()()() |
| 59 | ()()()()()() |
| 73 | ()() |
| 97 | ()()() |
| 101 | ()()()()()() |

Define for primes $p \neq 23$

$a_p = 0 \quad \Leftrightarrow \quad$ 3 factors

$a_p = -1 \quad \Leftrightarrow \quad$ 2 factors

$a_p = 2 \quad \Leftrightarrow \quad$ 6 factors

# One more modular form

| | |
|---|---|
| | set $a_1 = 1$ |
| | set $a_{23} = 1$ |
| $p \neq 23$: if 3 factors, | set $a_p = 0$ |
| $p \neq 23$: if 2 factors, | set $a_p = -1$ |
| $p \neq 23$: if 6 factors, | set $a_p = 2$ |
| for all $p$, $n \geq 2$, | set $a_{p^n} = a_p \cdot a_{p^{n-1}} - \left(\frac{-23}{p}\right) a_{p^{n-2}}$. |
| if $\gcd(n, m) = 1$, | set $a_{nm} = a_n \cdot a_m$. |

Define

$$f = \sum_{n=1}^{\infty} a_n \cdot q^n = q - q^2 - q^3 + q^6 + q^8 - q^{13} - q^{16} + q^{23} - q^{24} + \ldots,$$

a modular form of level 23 and weight 1.

# Galois groups

A symmetry (called field automorphism) of $\mathbb{C}$ is a function $\sigma : \mathbb{C} \to \mathbb{C}$ such that for all $z_1, z_2 \in \mathbb{C}$

$$\sigma(z_1 + z_2) = \sigma(z_1) + \sigma(z_2) \text{ and } \sigma(z_1 \cdot z_2) = \sigma(z_1) \cdot \sigma(z_2).$$

We factor our polynomial over $\mathbb{C}$:

$$f(X) = X^6 - 6X^4 + 9X^2 + 23 = (X - a_1)(X - a_2)\dots(X - a_6).$$

The symmetry group $\mathrm{Gal}(f)$ of $f$ (called Galois group) is the group of those permutations of the set of roots $\{a_1, a_2, \dots, a_6\}$ of $f$ that come from symmetries of $\mathbb{C}$.

# A Galois representation

The factorisation of a polynomial $f$ over $\mathbb{F}_p$ into irreducibles

$$(\text{degree } d_1) \cdot (\text{degree } d_2) \cdot \ldots \cdot (\text{degree } d_r)$$

gives rise to an element $\text{Frob}_p \in \text{Gal}(f)$, called Frobenius at $p$, having cycle type (as permutation)

$$(\text{cycle of length } d_1)(\text{cycle of length } d_2)\ldots(\text{cycle of length } d_r).$$

Our case: There is a group homomorphism

$$\rho : \text{Gal}(f) \to \mathrm{GL}_2(\mathbb{C}),$$

called a Galois representation, such that:

| $f$ mod $p$ | $\text{Frob}_p$ | $\rho(\text{Frob}_p)$ | trace | $a_p$ |
|---|---|---|---|---|
| ()()()()()() | identity | $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ | 2 | 2 |
| ()() | 2 3-cycles | $\left(\begin{smallmatrix}\zeta&0\\0&\zeta^2\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}\zeta^2&0\\0&\zeta\end{smallmatrix}\right)$, $\zeta = e^{2\pi i/3}$ | $-1$ | $-1$ |
| ()()() | 3 2-cycles | $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&\zeta\\\zeta^2&0\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&\zeta^2\\\zeta&0\end{smallmatrix}\right)$ | 0 | 0 |

# Galois representations

Let's become big (uncountable).
Take $\mathrm{Gal}(\overline{\mathbb{Q}})$, the (projective) limit of the Galois groups $\mathrm{Gal}(f)$ for all irreducible integer polynomials $f$, i.e.
$\mathrm{Gal}(\overline{\mathbb{Q}})$ is the smallest group that admits all $\mathrm{Gal}(f)$ as quotients.

It is called the absolute Galois group.
It is a/the central object of algebraic number theory. Mysterious!!

Like any group, it is studied through representations.

| | | sources |
|---|---|---|
| $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}) \to \mathrm{GL}_2(\mathbb{C})$ | Artin repres. | our example<br>modular forms weight 1 |
| $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ | $p$-adic repres. | elliptic curves (Tate module)<br>modular forms weight $\geq 2$ |
| $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ | mod $p$ repres. | elliptic curves ($p$-torsion)<br>modular forms weight $\geq 2$ |

# Summary and theorems

Modular forms are easy to compute.
We saw an example (using modular (Manin) symbols).

## Theorem (Deligne, Serre,...).

*Modular forms* $f = \sum_{n=1}^{\infty} a_n q^n$ *('Hecke eigenforms') give rise to Galois representations* $\rho$ *such that*

$$\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = a_p$$

*for (almost) all primes* $p$*.*

We saw an example in weight 1.

# Summary and theorems

**Theorem** (Khare, Wintenberger, 'Serre's modularity conjecture', 2009).

*Every 2-dimensional 'odd' mod p Galois representation comes from a modular form.*

**(Almost) Theorem** (Kisin, Emerton, 'Fontaine-Mazur conj.', 2010+).

*Every 2-dimensional 'geometric' p-adic Galois representation comes from a modular form.*

Meaning:

- Elliptic curve $\mapsto$ $p$-adic Galois repres. (via Tate module)
  $\Rightarrow$ elliptic curves are modular ($\Rightarrow$ Wiles, Fermat's Last Thm)
  We saw the modularity of one elliptic curve in the beginning.
- Galois representations are parametrised via modular forms.
- Galois representations are hard/impossible to compute. Modular forms are easy to compute.
  $\Rightarrow$ Use modular forms computations to learn about Galois representations!!! (That's what we do a lot...)

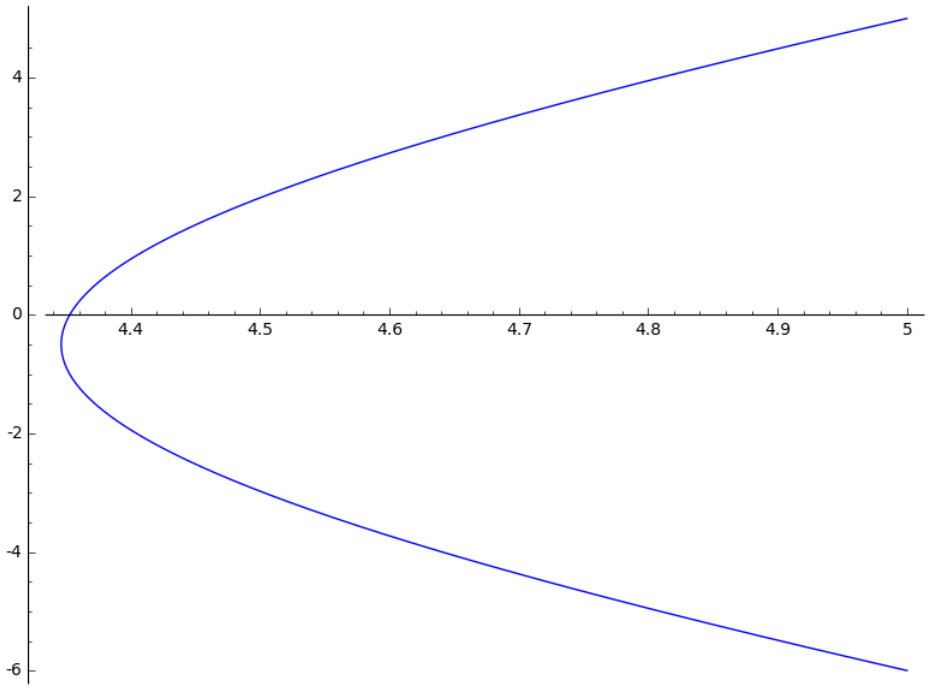
Thanks for your attention!

# Elliptic-curve-talk

```
E=EllipticCurve("11A1")
E
```

```
Elliptic Curve defined by y^2 + y = x^3 - x^2 - 10*x - 20 over
Rational Field
```

```
E.plot(xmin = 2, xmax=5)
```




```
E.reduction(2).points()
```

```
[(0 : 0 : 1), (0 : 1 : 0), (0 : 1 : 1), (1 : 0 : 1), (1 : 1 : 1)]
```

```
E.reduction(3).points()
```

```
[(0 : 1 : 0), (1 : 0 : 1), (1 : 2 : 1), (2 : 0 : 1), (2 : 2 : 1)]
```

```
E.reduction(5).points()
```

```
[(0 : 0 : 1), (0 : 1 : 0), (0 : 4 : 1), (1 : 0 : 1), (1 : 4 : 1)]
```

```
E.reduction(7).points()
```

```
[(0 : 1 : 0), (1 : 3 : 1), (2 : 2 : 1), (2 : 4 : 1), (4 : 1 : 1), (4
: 5 : 1), (5 : 1 : 1), (5 : 5 : 1), (6 : 1 : 1), (6 : 5 : 1)]
```

```
E.reduction(7).cardinality()
```

```
10
```

```
E.reduction(13).cardinality()
```

```
10
```

```
E.reduction(17).cardinality()
```

```
20
```

```
list(primes(19,38))
```

```
[19, 23, 29, 31, 37]
```

```
[E.reduction(p).cardinality() for p in list(primes(19,38))]
```

```
[20, 25, 30, 25, 35]
```

# Modular-symbols-talk

```
C=ModularSymbols(11,2,1).cuspidal_subspace()
C
```

```
Modular Symbols subspace of dimension 1 of Modular Symbols space of
dimension 2 for Gamma_0(11) of weight 2 with sign 1 over Rational
Field
```

```
C.hecke_operator(2).matrix()
```

```
[-2]
```

```
C.hecke_operator(3).matrix()
```

```
[-1]
```

```
C.hecke_operator(5).matrix()
```

```
[1]
```

```
[C.hecke_operator(p).matrix()[0,0] for p in list(primes(1,38))]
```

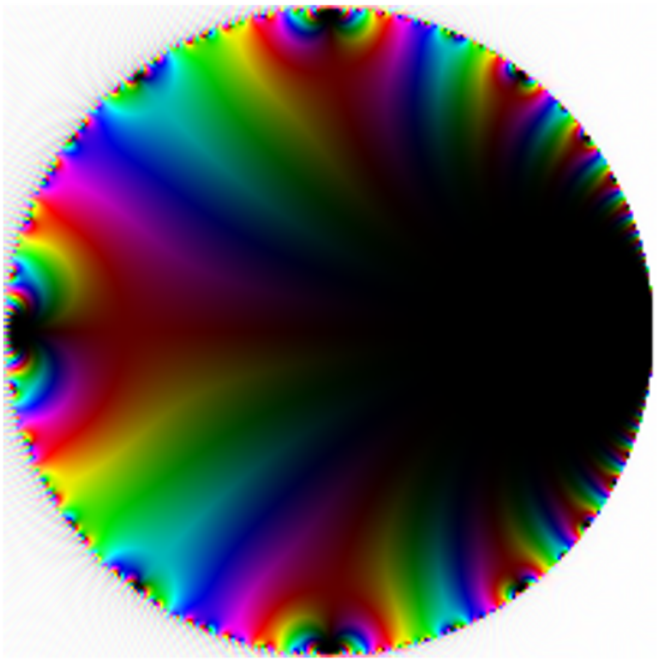
```
[-2, -1, 1, -2, 1, 4, -2, 0, -1, 0, 7, 3]
```

```
T_list=[C.hecke_operator(p).matrix()[0,0] for p in range(1,100)]
T_list
```

```
[1, -2, -1, 2, 1, 2, -2, 0, -2, -2, 1, -2, 4, 4, -1, -4, -2, 4, 0,
2, 2, -2, -1, 0, -4, -8, 5, -4, 0, 2, 7, 8, -1, 4, -2, -4, 3, 0, -4,
0, -8, -4, -6, 2, -2, 2, 8, 4, -3, 8, 2, 8, -6, -10, 1, 0, 0, 0, 5,
-2, 12, -14, 4, -8, 4, 2, -7, -4, 1, 4, -3, 0, 4, -6, 4, 0, -2, 8,
-10, -4, 1, 16, -6, 4, -2, 12, 0, 0, 15, 4, -8, -2, -7, -16, 0, -8,
-7, 6, -2]
```

```
z = var('z')
q = exp(2*pi*(z+1)/(z-1))
f=0;
for a in range (1,100):
  f = f+T_list[a-1]*q^a;
```

```
p = complex_plot (f, (-1,1) , (-1 ,1) , plot_points=200)
p.axes(false)
p
```



```
# coefficients calculated in Magma and copied here
S_list = [ 1, -1, -1, 0, 0, 1, 0, 1, 0, 0, 0, 0, -1, 0, 0, -1, 0, 0, 0, 0, 0, 0, 1, -1, 1, 1, 1, 0, -1, 0,
-1, 0, 0, 0, 0, 0, 0, 0, 1, 0, -1, 0, 0, 0, 0, -1, -1, 1, 1, -1, 0, 0, 0, -1, 0, 0, 0, 1, 2, 0, 0, 1, 0, 1,
0, 0, 0, 0, -1, 0, -1, 0, -1, 0, -1, 0, 0, -1, 0, 0, -1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, -1,
0 ]
```

```
z = var('z')
q = exp(2*pi*(z+1)/(z-1))
g=0;
for a in range (1,100):
  g = g+S_list[a-1]*q^a;
```

```
p1 = complex_plot (g, (-1,1) , (-1 ,1) , plot_points=200)
p1.axes(false)
p1
```