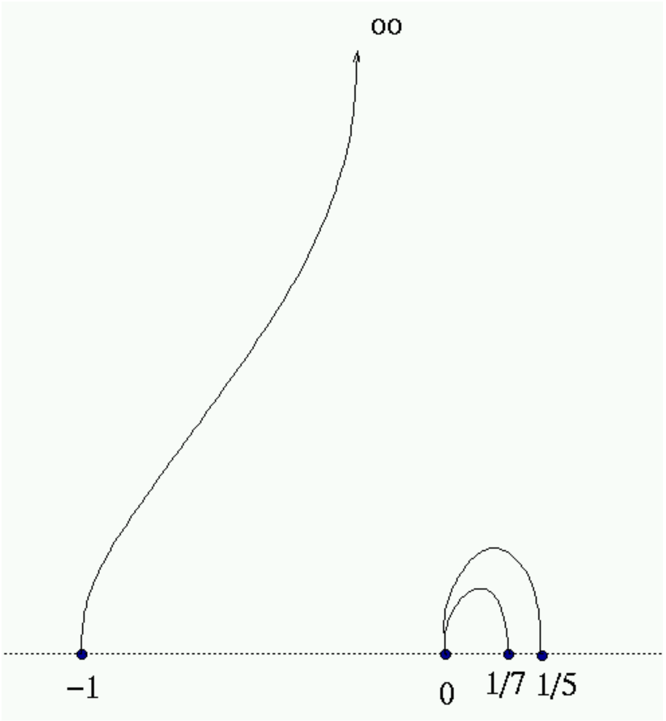
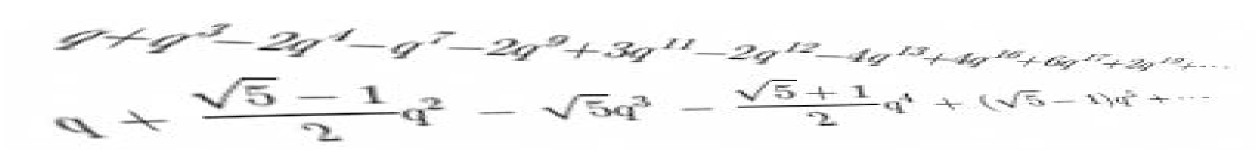
Introduction to Modular Symbols

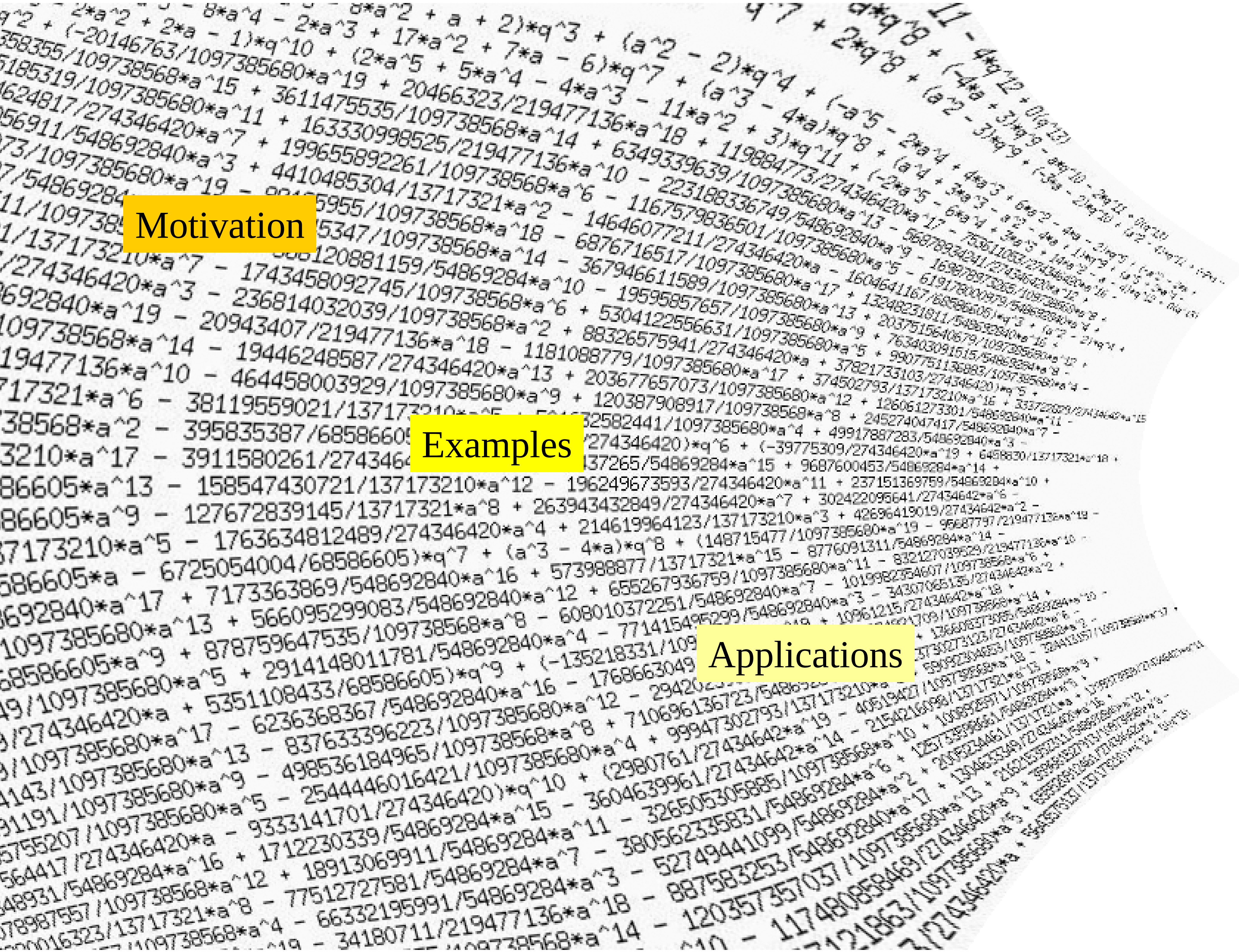
Math 252

September 26, 2003

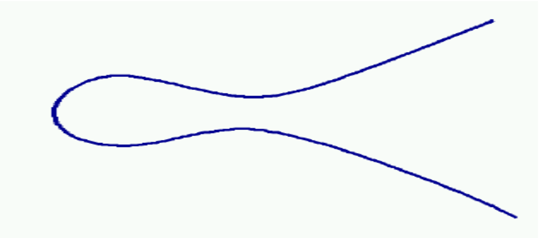


William A. Stein



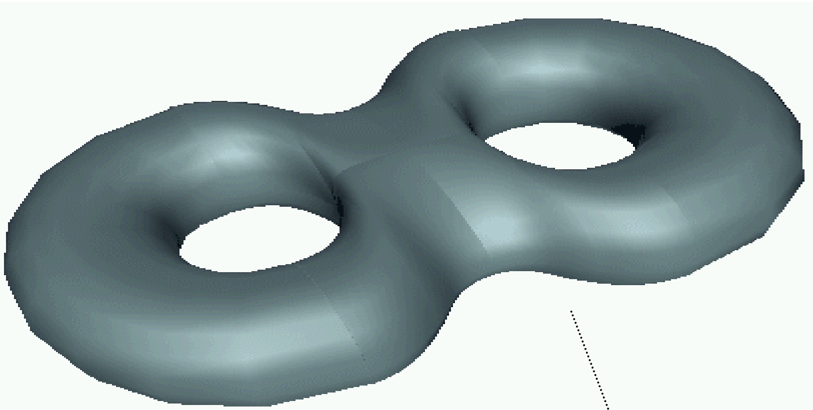

Motivation
Examples
Applications

Motivation



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

Modular forms give order to the mysterious world of elliptic curves and abelian varieties.



$y^2 = x^6 + 14x^5 + 35x^4 + 48x^3 + 35x^2 + 14x + 1$

Because of the modularity theorem, modular forms of level N "explain" all of the elliptic curves of conductor N.

$q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + 6q^6 - q^7 + 6q^9 + \cdots$

$q + q^3 - 2q^4 - q^7 - 2q^9 + 3q^{11} - 2q^{12} - 4q^{13} + \cdots$

$y^2 + y = x^3 + x^2 - 23x - 50$

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

Birch and Swinnerton-Dyer

- In the 1960s, B. Birch and H.P.F. Swinnerton- Dyer computed amazing data about elliptic curves, which lead to a fundamental conjecture.
- The conjecture is still very much open!   For more details, see Wiles's paper at the Clay Math Institute Millenial Problems web page.

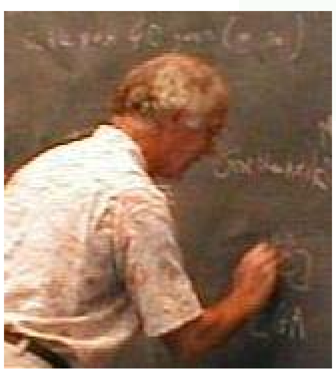
The BSD Conjecture

Let E be an elliptic curve over $\mathbf{Q}$, and let $L(E,s)$ be the associated L-function. Then

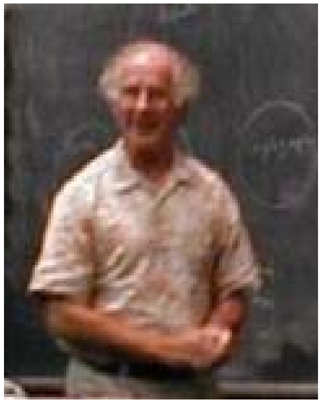
$$\operatorname{ord}_{s=1} L(E,s) = \operatorname{rank} E(\mathbf{Q})$$

and

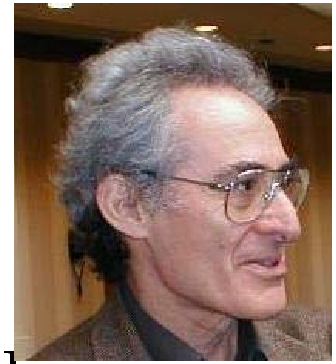
$$\frac{L^{(r)}(E,1)}{r!} = \frac{\prod c_p \cdot \Omega_E \cdot \mathrm{Reg}_E \cdot \#\text{Ш}_E}{\#E(\mathbf{Q})_{\mathrm{tor}}^2}.$$



Birch first introduced modular symbols



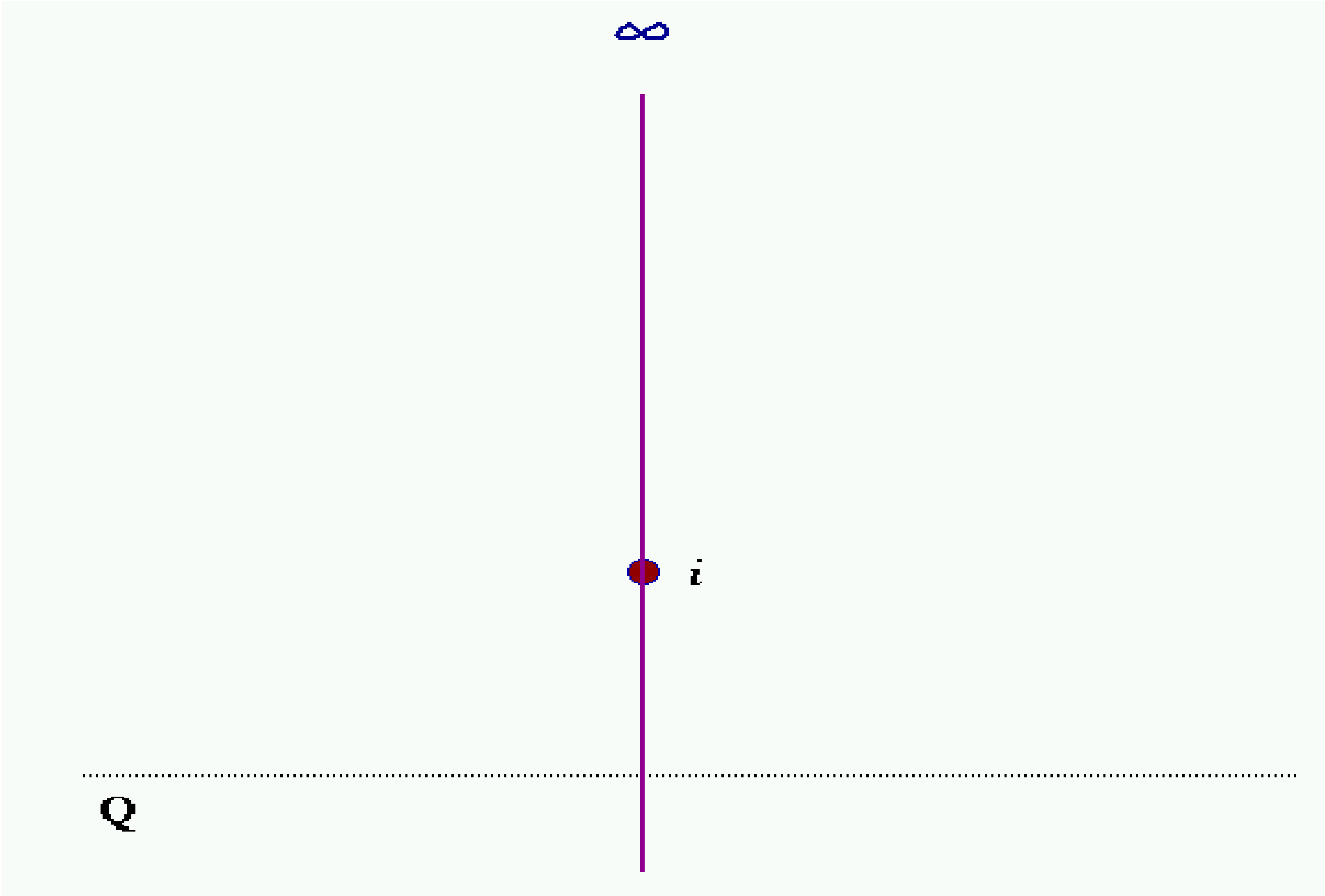
- While gather data towards the conjecture, Birch introduced modular symbols.
- Yuri Manin and Barry Mazur independently developed a systematic theory.



- John Cremona later used modular symbols to enumerate the > 30000 elliptic curves of conductor up to 6000.

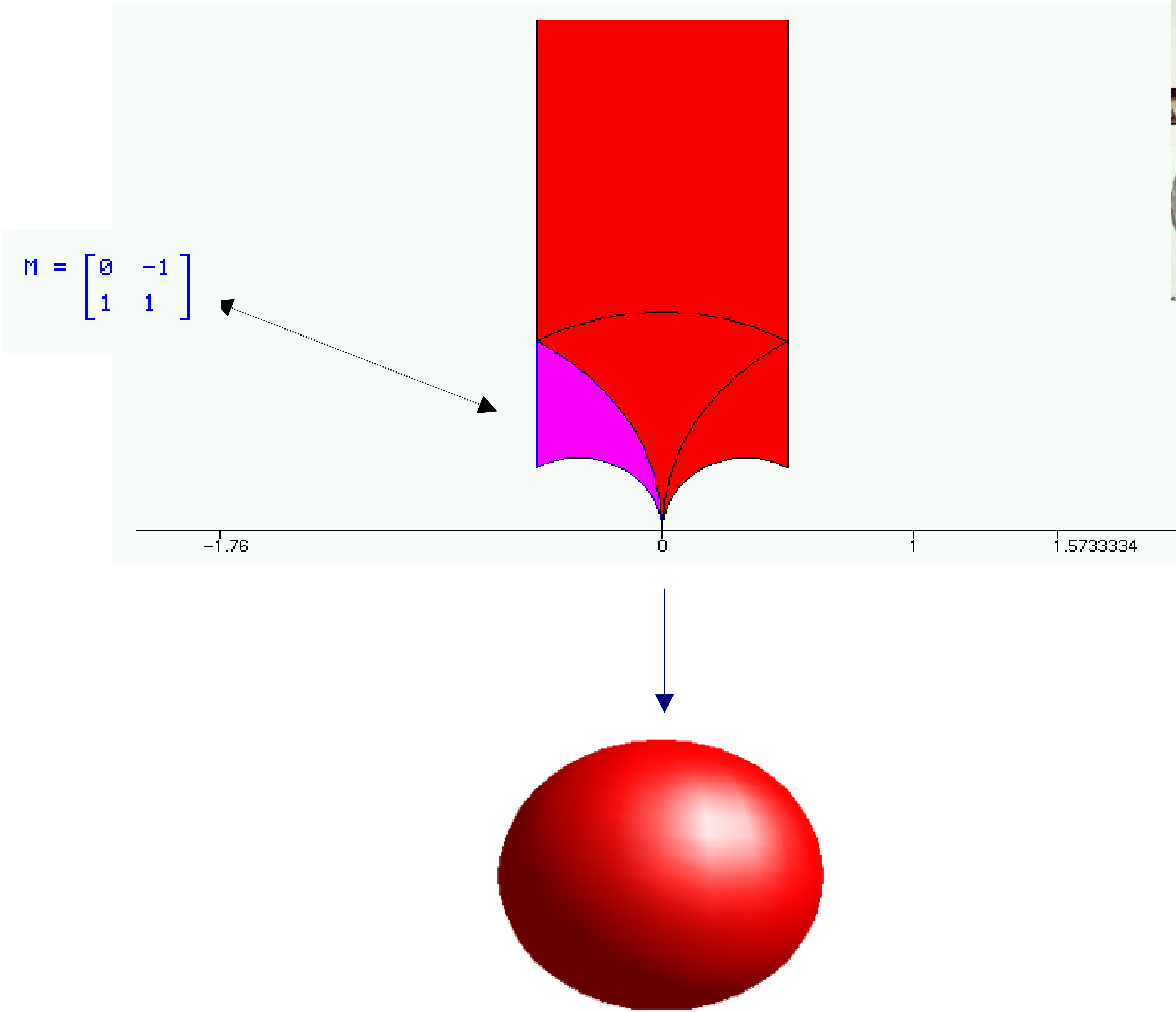
How can we compute with objects attached to subgroups of the modular group?

Modular Curves



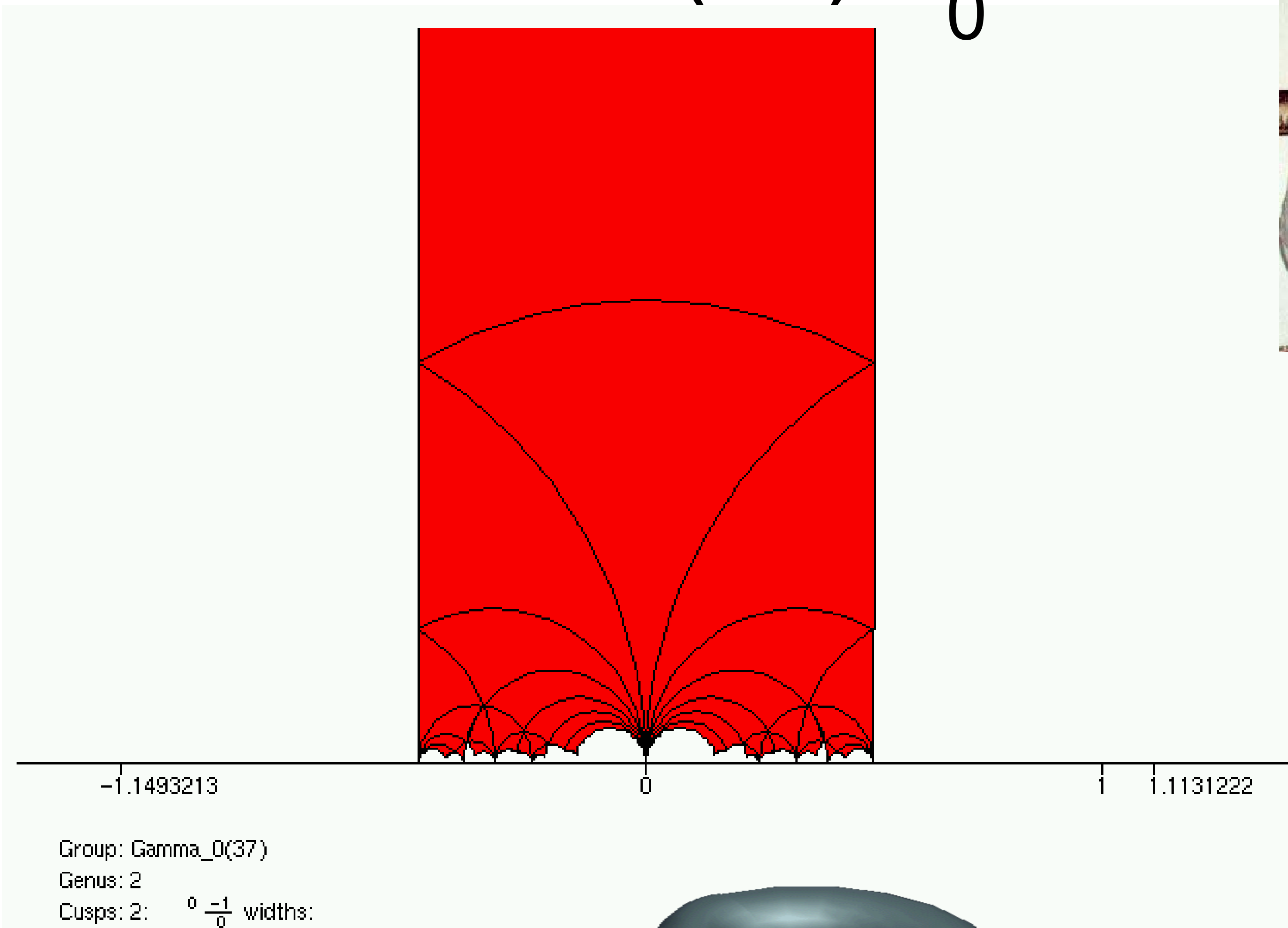
The quotient of $\mathfrak{h} \cup \mathbf{Q} \cup \{\infty\}$ by the action of $\Gamma_0(N)$ is a compact Riemann surface $X_0(N)$.

Modular curve for N=3:

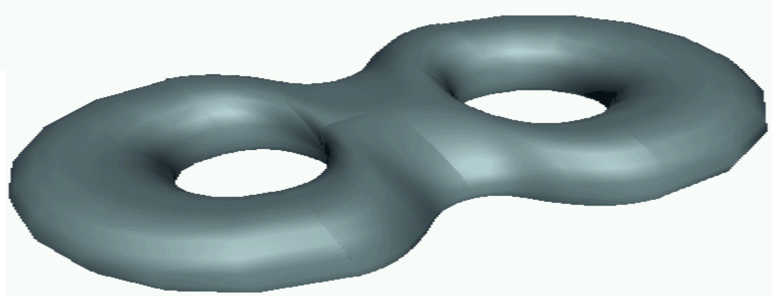


Helena Verrill

Modular curve $X_0(37)$:



Helena Verrill



$$y^2 = x^6 + 14x^5 + 35x^4 + 48x^3 + 35x^2 + 14x + 1$$

Modular Forms

A *modular form* for $\Gamma_0(N)$ (of weight 2) is a holomorphic function $f(z)$ on $\mathfrak{h}$ such that

$$f(\gamma(z))d(\gamma(z)) = f(z)dz$$

for all $\gamma \in \Gamma_0(N)$.

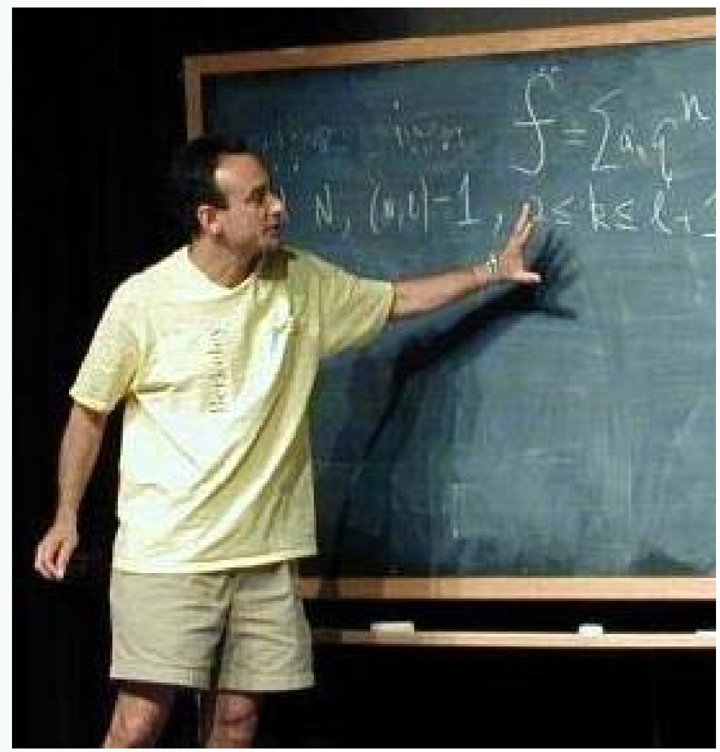
Since $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N)$,

$$f(z+1) = f(z),$$

so $f(z)$ has a *Fourier expansion*

$$f(z) = a_0 + a_1 q + a_2 q^2 + a_3 q^3 + \cdots$$

where $q = e^{2\pi i z}$.



Ribet

Examples of modular forms

Use Magma to compute some modular forms:

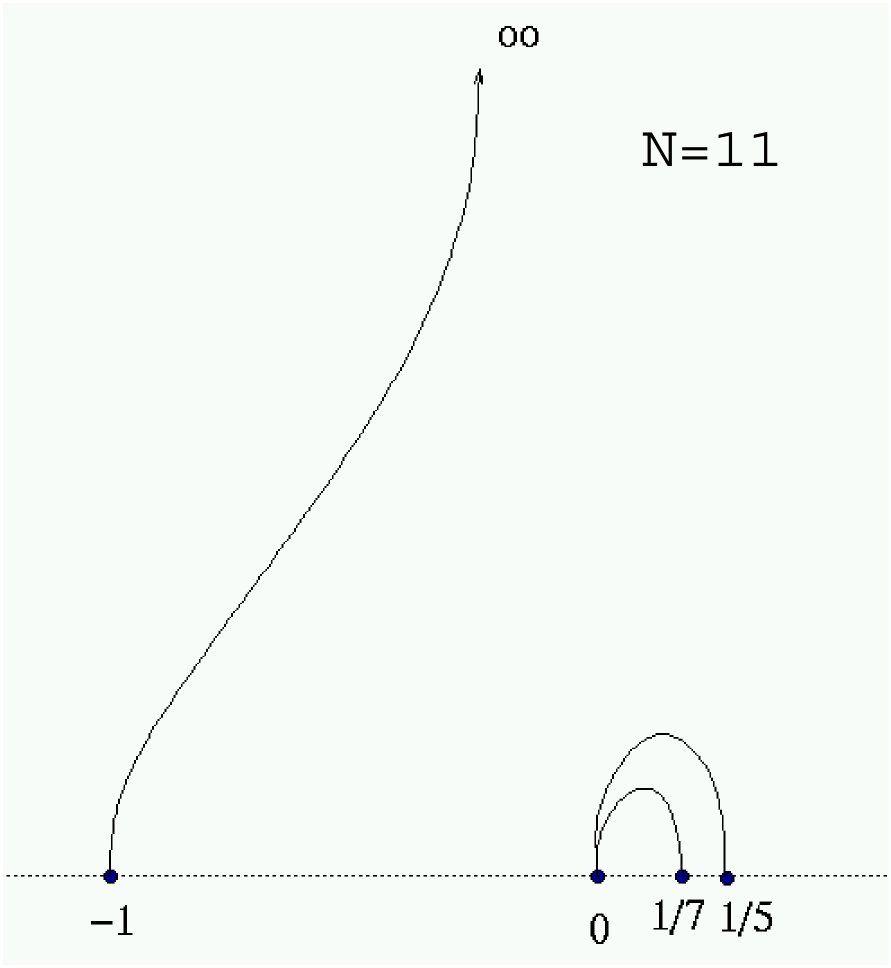
```
> qEigenform(ModularSymbols("11A"),7);
> qEigenform(ModularSymbols("23A"),6);
> qEigenform(ModularSymbols("37A"),7);
```

$$q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 + \cdots$$

$$q + \frac{\sqrt{5}-1}{2}q^2 - \sqrt{5}q^3 - \frac{\sqrt{5}+1}{2}q^4 + (\sqrt{5}-1)q^5 + \cdots$$

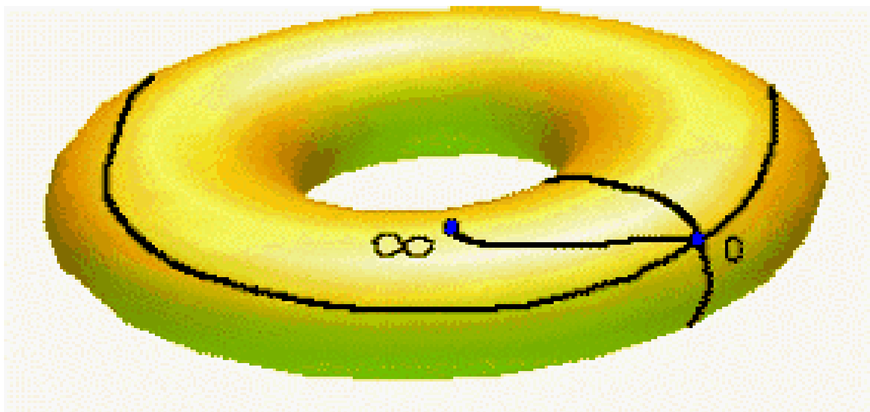
$$q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + 6q^6 + \cdots$$

Modular Symbols



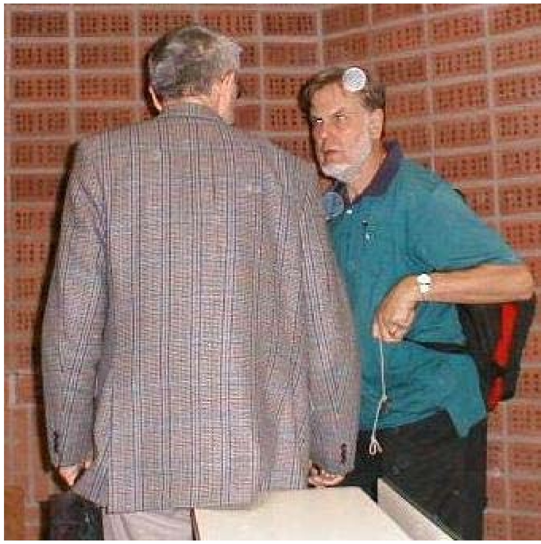
A modular symbol {a,b} is the homology class (relative to cusps) of the image of a geodesic path from the cusp a to the cusp b.

The three modular symbols to the right, denoted {-1,oo}, {0,1/5}, and {0,1/7}, are a basis for the space of modular symbols for Gamma_0(11).



Compute some examples using MAGMA.

Computing the space of modular symbols



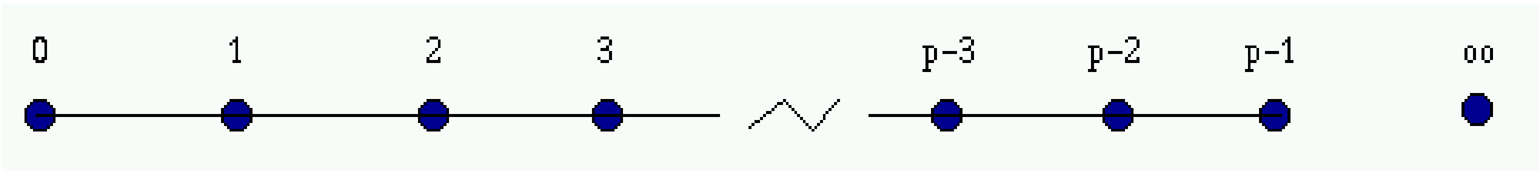
Assume for simplicity that N=p is prime.

Let $r_o, \ldots, r_p$ be coset representatives for $\Gamma_0(p)$ in $\mathrm{SL}_2(\mathbf{Z})$. So

$$\mathrm{SL}_2(\mathbf{Z}) = \Gamma_0(p) r_o \cup \Gamma_0(p) r_1 \cup \cdots \cup \Gamma_0(p) r_p.$$

E.g.,

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}, \ldots, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$



Explicit presentation of modular symbols

Let V be the $p+1$-dimensional vector space with basis

$$x_0, x_1, \ldots, x_p.$$

Theorem (Manin). There is an isomorphism

$$V/R = \text{ModSym}(\Gamma_0(p)),$$

where x_i maps to $r_i\{0,\infty\} = \{r_i(0), r_i(\infty)\}$, and the relations R are described explicitly below.

Relations

The subspace R of relations is the subspace generated by

$$x_i + x_i S$$

$$x_i + x_i T + x_i T^2,$$

where

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix},$$

and $i = 0, \ldots, p$.

Example: N=11

Generating modular symbols:

$$\{0,\infty\},\ \{0,1\},\ \{0,1/2\},\ldots,\{0,1/10\},\ \{\infty,0\}$$

Doing the linear algebra, we find that $\{0,\infty\}$, $\{0,1/5\}$, $\{0,1/7\}$ are a basis. And, e.g.,

$$\begin{aligned}\{0,1/2\} &= -\{0,1/5\}\\ \{0,1/3\} &= -\{0,1/7\}\\ \{0,1/4\} &= \{0,1/5\}-\{0,1/7\}\end{aligned}$$

Manins Trick

Manin's trick: Writes *any* symbol $\{\alpha, \beta\}$ as a linear combination of generating symbols of the form $r_i\{0, \infty\}$.

The trick implies that the symbols $r_i\{0, \infty\}$ generate

The trick:
Suffices to consider $\{0, b/a\}$. Expand b/a as a continued fraction and consider the successive convergents in lowest terms:

$$\frac{b}{a} = \frac{b_n}{a_n}, \quad \frac{b_{n-1}}{a_{n-1}}, \ \ldots, \quad \frac{b_0}{a_0} = \frac{b_0}{1}, \quad \frac{b_{-1}}{a_{-1}} = \frac{1}{0}, \quad \frac{b_{-2}}{a_{-2}} = \frac{0}{1}$$

(the last two are added formally).

The trick:
Suffices to consider $\{0, b/a\}$. Expand b/a as a continued fraction and consider the successive convergents in lowest terms:

$$\frac{b}{a}=\frac{b_n}{a_n}, \quad \frac{b_{n-1}}{a_{n-1}}, \ldots, \quad \frac{b_0}{a_0}=\frac{b_0}{1}, \quad \frac{b_{-1}}{a_{-1}}=\frac{1}{0}, \quad \frac{b_{-2}}{a_{-2}}=\frac{0}{1}$$

(the last two are added formally).

Then

$$b_k a_{k-1} - b_{k-1} a_k = (-1)^{k-1},$$

so that

$$g_k = \begin{pmatrix} b_k & (-1)^{k-1} b_{k-1} \\ a_k & (-1)^{k-1} a_{k-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}).$$

Hence

$$\left\{\frac{b_{k-1}}{a_{k-1}}, \frac{b_k}{a_k}\right\} = g_k\{0,\infty\} = r_i\{0,\infty\},$$

for some i, is of the required special form.

Example

Example: Let $N = 11$, and consider $\{0, 4/7\}$.

We have

$$\frac{4}{7} = 0 + \frac{1}{1 + \frac{1}{1+\frac{1}{1+\frac{1}{3}}}},$$

so partial convergents are

$$\frac{b_{-2}}{a_{-2}} = \frac{0}{1}, \quad \frac{b_{-1}}{a_{-1}} = \frac{1}{0}, \quad \frac{b_0}{a_0} = \frac{0}{1}, \quad \frac{b_1}{a_1} = \frac{1}{1}, \quad \frac{b_2}{a_2} = \frac{1}{2}, \quad \frac{b_3}{a_3} = \frac{4}{7}.$$

Thus

$$\begin{aligned}
\{0, 4/7\} &= \{0,\infty\} + \{\infty, 0\} + \{0,1\} + \{1, 1/2\} + \{1/2, 4/7\} \\
&= \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix}\{0,\infty\} + \begin{pmatrix} 4 & 1 \\ 7 & 2 \end{pmatrix}\{0,\infty\} \\
&= 2 \cdot \left[\begin{pmatrix} 1 & 4 \\ 1 & 5 \end{pmatrix}\{0,\infty\}\right]
\end{aligned}$$

The connection with modular forms

There is an amazing sequence $T_1, T_2, T_3, \ldots$ of commuting linear maps on modular symbols. The corresponding systems of eigenvalues

$$\{a_1, a_2, a_3, \ldots\}$$

are the coefficients a_n of the q-expansions of modular forms.

When $n = p$ is prime to N, we have

$$T_p(\{\alpha, \beta\}) = \left[\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} + \sum_{r \bmod p} \begin{pmatrix} 1 & r \\ 0 & p \end{pmatrix} \right] \{\alpha, \beta\}.$$

Example

Example: $N = 11$

$$\begin{aligned} T_2(\{0,1/5\}) &= \{0,2/5\} + \{0,1/10\} + \{1/2,3/5\} \\ &= -2\{0,1/5\} \\ &= a_2\{0,1/5\} \end{aligned}$$

Consequently, the modular form of level 11 is

$$f = q + a_2 q^2 + a_3 q^3 + \cdots,$$

where $T_\ell(\{0,1/5\}) = a_\ell\{0,1/5\}$.

There is a deep connection with elliptic curves (due to Shimura):

$$a_\ell = \ell + 1 - \#E(\mathbf{F}_\ell),$$

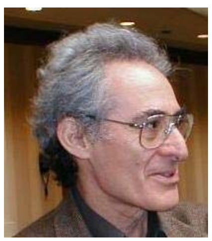
where E is $y^2 + y = x^3 - x^2 - 10x - 20$.

Some Applications of Modular Symbols

- Enumerate all elliptic curves of given conductor.
- Compute basis of modular forms of given weight and level.
- Proving theorems towards the BSD conjecture; e.g., that L(E,1)/Omega is a rational number.

Some References

- **Manin:** *Parabolic points and zeta-functions of modular curves, 1972.*



- ***Mazur:*** *Courbes elliptiques et symboles modulaires, 1972.*

- ***Cremona:*** *Algorithms for modular elliptic curves, 1997.*

- *My modular symbols package in Magma.*