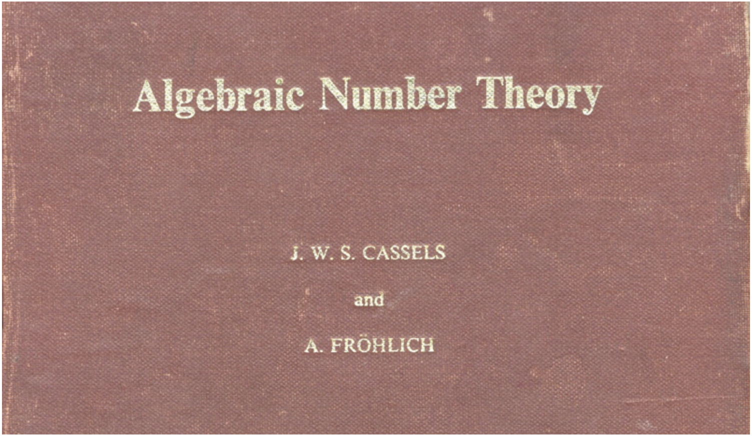
Counting points on elliptic curves over finite fields and beyond

René Schoof
Università di Roma "Tor Vergata"

Prehistory



Algebraic Number Theory

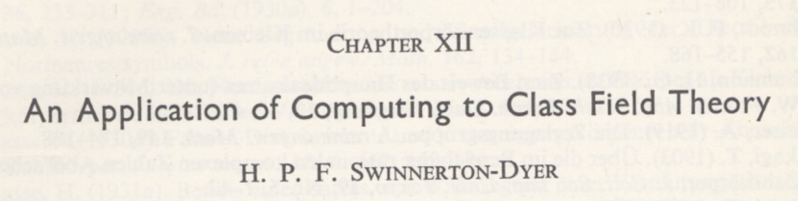
J. W. S. CASSELS

and

A. FRÖHLICH

In his article in the 1967 Cassels-Fröhlich volume on class field theory, Swinnerton-Dyer reports on the famous calculations with Birch concerning elliptic curves over **Q**.

Footnote



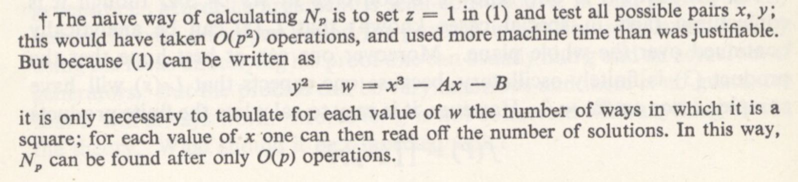
CHAPTER XII

An Application of Computing to Class Field Theory

H. P. F. SWINNERTON-DYER

$$Y^2Z = X^3 - AXZ^2 - BZ^3, \qquad (1)$$

On page 284 there is the following footnote



† The naive way of calculating N_p is to set $z = 1$ in (1) and test all possible pairs x, y; this would have taken $O(p^2)$ operations, and used more machine time than was justifiable. But because (1) can be written as

$$y^2 = w = x^3 - Ax - B$$

it is only necessary to tabulate for each value of w the number of ways in which it is a square; for each value of x one can then read off the number of solutions. In this way, N_p can be found after only $O(p)$ operations.

Henri's Question

Spring 1982: Henri Cohen visits Hendrik Lenstra in Amsterdam

Henri's Question

How quickly can one compute the number of points on elliptic curve modulo a prime p?

Hendrik's answer

Let E be the elliptic curve with equation

$$Y^2 = X^3 + AX + B, \qquad \text{over } \mathbf{F}_p.$$

Then the group of points $E(\mathbf{F}_p)$ is the class group of the ring $\mathbf{F}_p[X, Y]/(Y^2 - X^3 - AX - B)$. This ring is the ring of integers of the quadratic function field

$$\mathbf{F}_p(X)(\sqrt{X^3 + AX + B}).$$

The class group can be computed with the same methods that one uses for quadratic number fields. For instance, using Shanks' baby-step-giant-step algorithm. Time $O(p^{0.25})$.

A polynomial time algorithm

There exists a deterministic polynomial time algorithm to compute the number of points on an elliptic curve E over $\mathbf{F}_p$. The running time is $O(\log^8 p)$.

May 1982: a special case

Let E be the elliptic curve with equation

$$Y^2 = X^3 - X.$$

Then $(-x, iy)$ is a point of E whenever (x, y) is. This means that E admits *complex multiplication* by the ring $\mathbf{Z}[i]$.

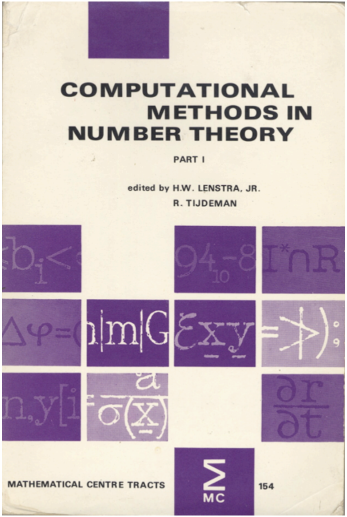
For $p \equiv 3 \pmod 4$ we have $\#E(\mathbf{F}_p) = p + 1$.

For $p \equiv 1 \pmod 4$ we have $p = a^2 + b^2$ and $\#E(\mathbf{F}_p) = p + 1 - 2a$.

Computing $\#E(\mathbf{F}_p)$ $\Leftrightarrow$ Computing a and b.

Note: a/b is the square root of $-1 \pmod p$.

1980 CWI meeting

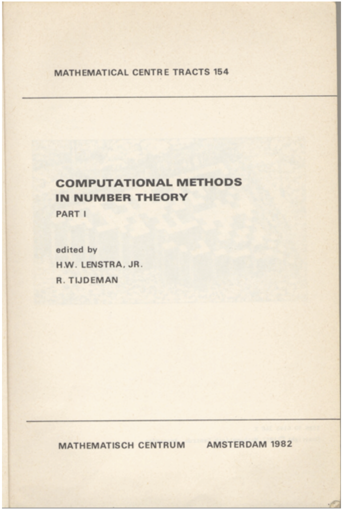


COMPUTATIONAL METHODS IN NUMBER THEORY

PART I

edited by H.W. LENSTRA, JR.
R. TIJDEMAN

MATHEMATICAL CENTRE TRACTS 154



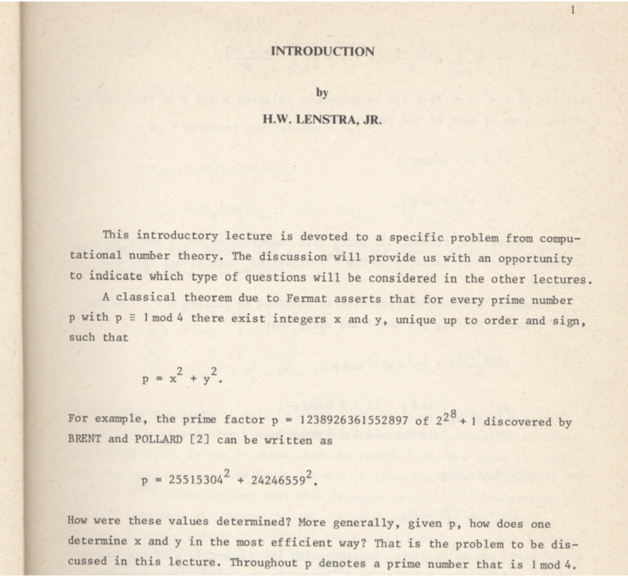
MATHEMATICAL CENTRE TRACTS 154

COMPUTATIONAL METHODS
IN NUMBER THEORY
PART I

edited by
H.W. LENSTRA, JR.
R. TIJDEMAN

MATHEMATISCH CENTRUM AMSTERDAM 1982

The 1982 preface



INTRODUCTION

by

H.W. LENSTRA, JR.

This introductory lecture is devoted to a specific problem from computational number theory. The discussion will provide us with an opportunity to indicate which type of questions will be considered in the other lectures.

A classical theorem due to Fermat asserts that for every prime number p with $p \equiv 1 \bmod 4$ there exist integers x and y, unique up to order and sign, such that

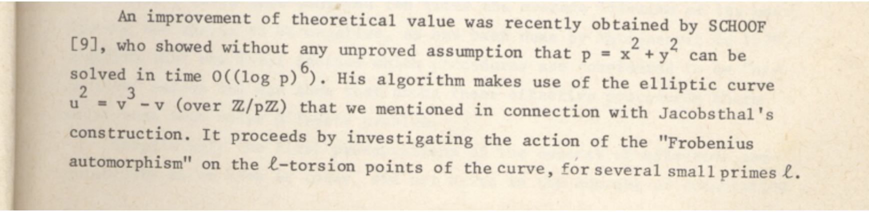
$$p = x^2 + y^2.$$

For example, the prime factor $p = 1238926361552897$ of $2^{2^8} + 1$ discovered by BRENT and POLLARD [2] can be written as

$$p = 25515304^2 + 24246559^2.$$

How were these values determined? More generally, given p, how does one determine x and y in the most efficient way? That is the problem to be discussed in this lecture. Throughout p denotes a prime number that is $1 \bmod 4$.

The 1982 preface

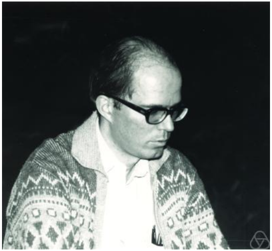


An improvement of theoretical value was recently obtained by SCHOOF [9], who showed without any unproved assumption that $p = x^2 + y^2$ can be solved in time $O((\log p)^6)$. His algorithm makes use of the elliptic curve $u^2 = v^3 - v$ (over $\mathbb{Z}/p\mathbb{Z}$) that we mentioned in connection with Jacobsthal's construction. It proceeds by investigating the action of the "Frobenius automorphism" on the ℓ-torsion points of the curve, for several small primes ℓ.

Number Theory day. Amsterdam, March 11, 1983

LENSTRA

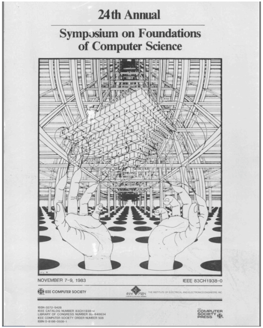
OORT



ODLYZKO

MANDERS

November 1983. The 24th FOCS meeting



24th Annual

Symposium on Foundations of Computer Science

NOVEMBER 7–9, 1983

IEEE 83CH1938-0

IEEE COMPUTER SOCIETY

1884 1984

THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.

ISSN 0272-5428
IEEE CATALOG NUMBER 83CH1938-0
LIBRARY OF CONGRESS NUMBER 80-646634
IEEE COMPUTER SOCIETY ORDER NUMBER 508
ISBN 0-8186-0508-1

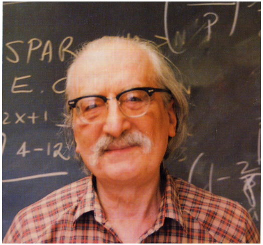
COMPUTER SOCIETY PRESS

November 1983. The 24th FOCS meeting

MEXICO
National capital
State capital
City
Major airport
International boundary
State boundary
Expressway
Main road
Railroad
USA
Phoenix
San Diego
Yuma
Tucson
Tijuana
Mexicali
Ensenada
San Felipe
Puerto Peñasco
Nogales
Ciudad Juarez
El Paso
Fort Worth
Dallas
Birmingham
Jackson
Austin
Houston
Baton Rouge
New Orleans
San Antonio
Corpus Christi
Hermosillo
Chihuahua
Guaymas
Bahia Sebastian Vizcaino
Gulf of California
Rio Yaqui
Rio Conchos
Rio Fuerte
Rio Grande
Rio Bravo del Norte
Nuevo Laredo
Saltillo
Monterrey
Matamoros
Culiacán
La Paz
Durango
Cabo San Lucas
Mazatlan
Zacatecas
Ciudad Victoria
Gulf of Mexico
Tropic of Cancer
San Luis Potosí
Tampico
Tepic
Aguascalientes
Guanajuato
Querétaro
Puerto Vallarta
Guadalajara
Pachuca
México
Xalapa
Morelia
Toluca
Tlaxcala
Veracruz
Manzanillo
Colima
Cuernavaca
Puebla
Rio Balsas
Chilpancingo
Acapulco
Oaxaca
Villahermosa
Rio Trinidad
Tuxtla Gutiérrez
Tapachula
Campeche
Mérida
Cancun
Chichen -Itzá
Playa del Carmen
Cozumel
Chetumal
BELIZE
BELMOPAN
Rio Usumacinta
GUATEMALA
San Pedro Sula
HONDURAS
TEGUCIGALPA
SLV
NORTH PACIFIC OCEAN
N
28°
24°
20°
18°
114°
110°
106°
102°
98°
94°
0 100 200 400 km
0 100 200 300 mi

1983-1984 University of Maryland

ZAGIER



SHANKS

SCHOOF, WASHINGTON, KRAFT

1983-1984 University of Maryland

MATHEMATICS OF COMPUTATION

Send it to Williams . . .

Elliptic curve factoring

February 1985

Hendrik Lenstra explains his student Wieb Bosma that algorithms that depend on properties of $p - 1$ have elliptic analogues.

LENSTRA

BOSMA

Then he realizes that he has invented a new factoring algorithm . . .

The algorithm

Let E be an elliptic curve over $\mathbf{F}_p$. The Frobenius endomorphism $\varphi \in \mathrm{End}(E)$ satisfies

$$\varphi^2 - [t]\varphi + [p] \; = \; 0, \qquad \text{in } \mathrm{End}(E).$$

for some integer t satisfying $|t| \leq 2\sqrt{p}$. The number of points in $E(\mathbf{F}_p)$ is given by

$$\#E(\mathbf{F}_p) \; = \; p + 1 - t.$$

The algorithm proceeds by checking the relation $\varphi^2 - [t]\varphi + [p] = 0$ on the ℓ-torsion points $E[\ell]$ for various small primes ℓ. In this way one obtains $t \pmod{\ell}$. Then one applies the Chinese Remainder Theorem.

See Karl Rubin: AMS Review 86e:11122.

The SEA algorithm

ATKIN

ELKIES

The original algorithm computes the action of Frobenius on the ℓ-torsion points $E[\ell]$ of E. This object is described by an $\mathbf{F}_p$-algebra of dimension ℓ^2. It is of interest to replace $E[\ell]$ by *smaller* objects.

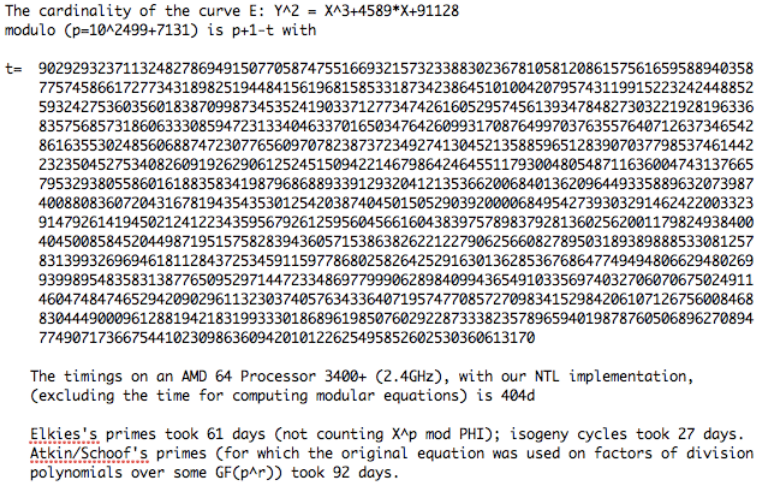
This approach leads to a non-deterministic algorithm that is **much** more efficient.

Subobjects: 1-dimensional eigenspaces of $E[\ell]$ (Elkies 1986)

Quotient objects: the $\mathbf{P}^1$ of lines in $E[\ell]$ (Atkin 1987)

2006 Record

The following result was posted by François Morain on November 26, 2006.



```
The cardinality of the curve E: Y^2 = X^3+4589*X+91128
modulo (p=10^2499+7131) is p+1-t with

t=  9029293237113248278694915077058747551669321573233883023678105812086157561659588940358
    7757458661727734318982519448415619681585331873423864510100420795743119915223242448852
    5932427536035601838709987345352419033712773474261605295745613934784827303221928196336
    8357568573186063330859472313340463370165034764260993170876499703763557640712637346542
    8616355302485606887472307765609707823873723492741304521358859651283907037798537461442
    2323504527534082609192629061252451509422146798642464551179300480548711636004743137665
    7953293805586016188358341987968688933912932041213536620068401362096449335889632073987
    4008808360720431678194354353012542038740450150529039200006849542739303291462422003323
    9147926141945021241223435956792612595604566160438397578983792813602562001179824938400
    4045008584520449871951575828394360571538638262212279062566082789503189389888533081257
    8313993269694618112843725345911597786802582642529163013628536768647749494806629480269
    93998954835831387765095297144723348697779990628984099436549103356974032706070675024911
    4604748474652942090296113230374057634336407195747708572709834152984206107126756008468
    8304449000961288194218319933301868961985076029228733382357896594019878760506896270894
    77490717366754410230986360942010122625495852602530360613170

   The timings on an AMD 64 Processor 3400+ (2.4GHz), with our NTL implementation,
   (excluding the time for computing modular equations) is 404d

   Elkies's primes took 61 days (not counting X^p mod PHI); isogeny cycles took 27 days.
   Atkin/Schoof's primes (for which the original equation was used on factors of division
   polynomials over some GF(p^r)) took 92 days.
```

p-adic methods

When q is a large power of a small prime p, there are better methods to count the number of points on elliptic curves E over $\mathbf{F}_q$.

One computes the action of the Frobenius endomorphism on the differentials rather than the groups $E[\ell]$ of ℓ-torsion points.

$\geq$ 2000 Carls, Castryk, Denef, Fouquet, Gaudry, Gerkmann, Gürel, Harley, Hubrechts, Kedlaya, Kohel, Lauder, Lercier , Lubicz, Mestre, Satoh, Vercauteren, Wan …

and … Kato and Lubkin: Zeta matrices of elliptic curves, *Journal of Number Theory* **15** (1982), 318–330.

Application to modular forms of weight 2

Let $N \geq 1$ and let f be a normalized eigenform of weight 2 for the group

$$\Gamma_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) : c \equiv 0 \pmod{N}\}.$$

Then f admits a Fourier expansion

$$f(\tau) = \sum_{n=1}^{\infty} a(n) q^n, \qquad \mathrm{Im}\,\tau > 0,$$

where $q = e^{2\pi i \tau}$ and $a(1) = 1$. We have

$$a(nm) = a(n)a(m), \quad \text{if } \gcd(n,m) = 1;$$

$$a(p^{r+1}) = a(p)a(p^r) - pa(p^{r-1}), \quad \text{for } r \geq 1.$$

Application to modular forms of weight 2

If the Fourier coefficients a_k of the weight 2 eigenform f are in $\mathbb{Z}$, there exists by Shimura an elliptic curve E over $\mathbb{Q}$ with the property that for each prime $p \not| N$, the number of points in $E(\mathbf{F}_p)$ is given by $p+1-t$ with

$$t \;=\; a_p.$$

Therefore, computing the Fourier coefficient a_p of the modular form f is the same as counting points on the elliptic curve E over $\mathbf{F}_p$.

When $a_k \notin \mathbf{Z}$, Shimura associates an abelian variety of dimension > 1 to the modular form f. In this case one can use Pila's algorithm to compute the Fourier coefficients a_p.

Example

There is a unique normalized eigenform of weight 2 for the group $\Gamma_0(11)$. Its Fourier expansion is given by

$$\begin{aligned} f(\tau) &= q\prod_{m=1}^{\infty}((1-q^m)(1-q^{11m}))^2 = \sum_{n=1}^{\infty} a(n)q^n. \\ &= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 + \dots \end{aligned}$$

The elliptic curve associated to f by Shimura is

$$Y^2 + Y = X^3 - X^2.$$

Generalization

$\approx$ 1997 **Question** raised by Cohen, Elkies, Schoof . . .

Can we generalize this to a polynomial time algorithm for modular forms of weight **larger** than 2?

2005 – 2010 **Affirmative answer** by Couveignes and Edixhoven (and Bosman, De Jong, Merkl).

EDIXHOVEN

COUVEIGNES

Ramanujan τ

The famous Ramanujan τ-function is defined by

$$\sum_{n=1}^{\infty} \tau(n) q^n \; = \; q \prod_{m=1}^{\infty} (1-q^m)^{24},$$

$$= q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 + \dots$$

It is a weight 12 modular form for the modular group $\mathrm{SL}_2(\mathbf{Z})$.

Counting pointed cubic curves

THEOREM. Let $n \geq 1$ and let p be a prime. Put

$$F_n(p) = \#\{(C, P_1, \ldots, P_n) : C \text{ is a smooth cubic in } \mathbf{P}^2$$
$$\text{and } P_i \in C(\mathbf{F}_p) \text{ for } i = 1, \ldots, n.\}/\#\mathrm{PGL}_3(\mathbf{F}_p)$$

Then for $n = 1, 2, \ldots, 9$ there is a polynomial f_n so that

$$F_n(p) = f_n(p).$$

On the other hand we have

$$F_{10}(p) = -\tau(p) + f_{10}(p))$$

for some polynomial f_{10}.

Counting pointed cubic curves

0. $f_0 = x;$
1. $f_1 = x^2 + x;$
2. $f_2 = x^3 + 3x^2 + x - 1;$
3. $f_3 = x^4 + 6x^3 + 6x^2 - 2x - 3;$
4. $f_4 = x^5 + 10x^4 + 20x^3 + 4x^2 - 14x - 74;$

$\vdots$

10. $f_{10} = x^{11} + 55x^{10} + 825x^9 + 4905x^8 + 12870x^7 + 12264x^6 + \dots$

Ramanujan τ

Some properties

- $\tau(nm) \;=\; \tau(n)\tau(m), \qquad \text{when } \gcd(n, m) = 1;$
- $\tau(p^{k+1}) \;=\; \tau(p)\tau(p^k) - p^{11}\tau(p^{k-1}), \quad \text{for } k \geq 1;$
- $\tau(p) \equiv p + p^4 \pmod 7, \qquad \text{for every prime } p;$

  $$\vdots$$

  $\equiv 1 + p^{11} \pmod{691}, \qquad \text{for every prime } p;$
- $|\tau(p)| \;\leq\; 2p^{11/2}, \qquad\qquad \text{for every prime } p.$

Couveignes-Edixhoven

A deterministic polynomial time algorithm to compute $\tau(p)$.

The algorithm computes $\tau(p)$ modulo several small primes l and then applies the Chinese Remainder Theorem.

For the special primes $l = 2, 3, 5, 7, 23, 691$ this can easily be done using the classical congruences satisfied by the τ-function. For $l = 11$ see below. For the other primes l this is harder.

Examples:

$$\begin{aligned}
\tau(10^{1000} + 1357) &\equiv \pm 4 \pmod{19}. \\
\tau(10^{1000} + 7383) &\equiv \pm 2 \pmod{19}. \\
\tau(10^{1000} + 21567) &\equiv \pm 3 \pmod{19}. \\
\tau(10^{1000} + 27057) &\equiv 0 \pmod{19}.
\end{aligned}$$

Action of Frobenius

To compute $\tau(p)$, Couveignes and Edixhoven make use of a certain 2-dimensional $\mathbf{F}_\ell$-vector space V_ℓ. This is the analogue of the 2-dimensional space $E[\ell]$ of ℓ-torsion points of an elliptic curve E.

For several small primes ℓ they compute the action of the Frobenius endomorphism φ on V_ℓ.

The characteristic polynomial of φ has the form

$$X^2 - tX + p^{11},$$

where

$$t \equiv \tau(p) \pmod{\ell}.$$

Etale cohomology

By Deligne (1969) the space V_ℓ is the 11-th étale cohomology group of the 10-fold symmetric product $E^{(10)}$ of the universal elliptic curve with values in $\mathbf{Z}/\ell\mathbf{Z}$.

$$V_\ell \; = \; H^{11}_{et}(E^{(10)}, \mathbf{Z}/\ell\mathbf{Z})$$

which, somewhat more explicitly, is also equal to

$$V_\ell \; = \; H^{1}_{et}(\mathbf{P}^1, F)$$

for some étale sheaf F.

This is the analogue of the 2-dimensional space of ℓ-torsion points of an elliptic curve.

Problem

The definition of the higher étale cohomology groups is very abstract and, it seems, unsuitable for direct use in explicit computations.

The **first** étale cohomology of a curve X with values in $\mathbf{Z}/\ell\mathbf{Z}$ is more explicit. It is the group of ℓ-torsion points on the Jacobian of X. It is a suitable object to do explicit computations with.

Couveignes and Edixhoven relate the group $H^{11}_{et}(E^{(10)}, \mathbf{Z}/\ell\mathbf{Z})$ to the cohomology group $H^1_{et}(X_1(\ell), \mathbf{Z}/\ell\mathbf{Z})$ of the modular curve $X_1(\ell)$.

Congruences

For every prime number $\ell \geq 11$ there are congruences

$$\tau(n) \equiv a(n) \pmod{\ell}$$

where $a(n)$ are the Fourier coefficients of a normalized weight 2 eigenform for the modular group

$$\Gamma_1(N) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \}$$

This means that for the 2-dimensional $\mathbf{F}_\ell$-vector space V_ℓ we have the inclusion

$$V_\ell \subset H^1_{et}(X_1(\ell), \mathbf{Z}/\ell\mathbf{Z}).$$

In other words, V_ℓ is a subspace of the ℓ-torsion points of the Jacobian $J_1(\ell)$ of the modular curve $X_1(\ell)$.

Example $\ell = 11$.

For $\ell = 11$, we have

$$\tau(p) \equiv a(p) \pmod{11}, \qquad \text{for all } p \neq 11.$$

where $a(p)$ is the Fourier coefficient of the weight 2 modular form

$$f(\tau) = q \prod_{m=1}^{\infty} ((1-q^m)(1-q^{11m}))^2 = \sum_{n=1}^{\infty} a(n)q^n$$

for the group $\Gamma_1(11) \subset \Gamma_0(11)$.

Example $\ell = 11$.

The Jacobian $J_1(11)$ is isogenous to the elliptic curve E

$$Y^2 - Y \;=\; X^3 - X^2,$$

associated to f by Shimura. Therefore we have

$$V_{11} \;=\; H^1_{\mathrm{et}}(X_1(11), \mathbf{Z}/11\mathbf{Z}) \;=\; E[11]$$

and one can compute the characteristic polynomial of φ modulo 11 and hence $\tau(p) \pmod{11}$ by determining the characteristic polynomial

$$X^2 - [t]X + p$$

of the Frobenius endomorphism acting on $E[11]$.

Problem

The genus g of the modular curve $X_1(\ell)$ is approximately

$$g \approx \frac{\ell^2}{24}.$$

This implies that the Jacobian $J_1(\ell)$ of $X_1(\ell)$ is an abelian variety of dimension $\ell^2/24$. Therefore the vector space $H^1_{\text{et}}(X_1(\ell), \mathbf{Z}/\ell\mathbf{Z})$ that contains V_ℓ satisfies

$$\dim_{\mathbf{F}_\ell} H^1_{\text{et}}(X_1(\ell), \mathbf{Z}/\ell\mathbf{Z}) \approx \frac{\ell^2}{12}$$

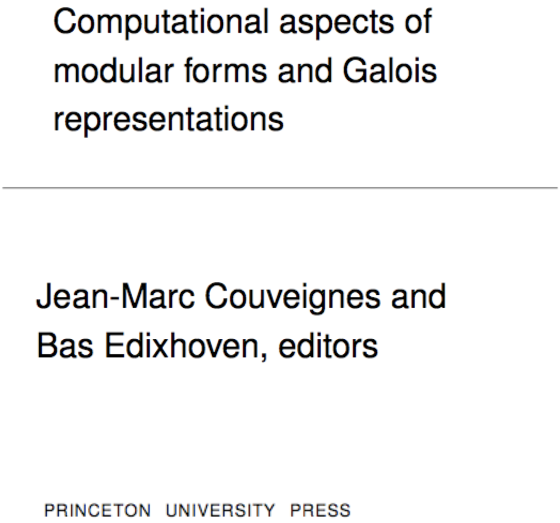
and this becomes **too large** when ℓ grows.

Solution

Couveignes and Edixhoven work with the complex analytic description of the Jacobian $J_1(\ell)$ as a complex torus. They then "cut out" the 2-dimensional subspace V_ℓ inside the $\ell^2/12$-dimensional space $H^1_{\mathrm{et}}(X_1(\ell), \mathbf{Z}/l\mathbf{Z})$ using Hecke operators T_m for small m. In fact, V_ℓ is the intersection of sufficiently many kernels of the endomorphisms $T_m - a_m$.

In order to control the size of the numbers and the accuracy that is needed for the numerical calculations, they use *Arakelov Theory*.

2010 Book



Computational aspects of modular forms and Galois representations

Jean-Marc Couveignes and
Bas Edixhoven, editors

PRINCETON UNIVERSITY PRESS

2010 Thesis Peter Bruin

Couveignes and Edixhoven actually have an algorithm that can handle eigenforms for the full modular group $\mathrm{SL}_2(\mathbf{Z})$ of **arbitrary** weight.

Recently this was generalized by Peter Bruin to eigenforms for the subgroups $\Gamma_1(N)$ of arbitrary weight **and** arbitray level N.

BRUIN

Sums of squares

Bruin's algorithm is probabilistic. Under the assumption of GRH it runs in polynomial time.

An spin-off of Bruin's algorithm is an algorithm to compute the number of ways a prime number p can be written as the sum of m squares

$$p = a_1^2 + a_2^2 + \ldots + a_m^2, \qquad \text{with } a_i \in \mathbf{Z}.$$

Here m should be **even**. This algorithm runs in time polynomial in $\log p$.

For even m, the number of ways n can be writtenas the sum of m squares is the n-th Fourier coefficient of a modular form of weight $m/2$.

For odd m there is no good algorithm.

Half integral weight

For negative $d \equiv 0$ or 1 modulo 4, let $H(d)$ denote the *Hurwitz class number* of the quadratic order of discriminant d.

Fourier series of the form

$$\sum_{\substack{n \geq 1 \\ n \equiv a \pmod{b}}} H(-n) q^n$$

are modular forms of weight 3/2.

The theory of modular forms of half integral weight is rather different from the theory that is concerned with modular forms of integral weight.

It would be interesting to have an efficient algorithm to compute Fourier coefficients of half integral weight.