# GEOMETRY AND NUMBERS

Ching-Li Chai

Institute of Mathematics Academia Sinica and Department of Mathematics University of Pennsylvania

National Chiao Tung University, July 6, 2012

GEOMETRY AND NUMBERS Ching-Li Chai

Sample arithmetic statements Diophantine equations Counting solutions of a diophantine equation Counting congruence solution L-functions and diotribution of prime numbers Zeta and L-values

Sample of geometric structures and symmetries Eligaic curve basic Modular forms, modular curves and Hecke symmetry Complex multiplication Probenius symmetry Monochemy Fine structure in characteristic

#### Outline

#### 1 Sample arithmetic statements

- Diophantine equations
- Counting solutions of a diophantine equation
- Counting congruence solutions
- L-functions and distribution of prime numbers
- Zeta and L-values

#### 2 Sample of geometric structures and symmetries

- Elliptic curve basics
- Modular forms, modular curves and Hecke symmetry
- Complex multiplication
- Frobenius symmetry
- Monodromy
- Fine structure in characteristic p

#### EOMETRY AND NUMBERS

#### Ching-Li Chai

Sample arithmetic statements Diophawine equations Counting solutions of a diophastics congruence solution Counting congruence solution L-functions and distribution prime members Zona and Londow

ample of geometric tructures and ymmetries liptic curve basics Modular forms, modular rarws and Hecke symmetry Complex multiplication Wobenias symmetry Monodromy

Pine structure in characteristi p

#### The general theme

# Geometry and symmetry influences arithmetic through zeta functions and modular forms

Remark. (i) zeta functions = L-functions; modular forms = automorphic representations.

(ii) There are two kinds of L-functions, from harmonic analysis and arithmetic respectively.

# Fermat's infinite descent

#### I. Sample arithmetic questions and results

#### 1. Diophantine equations

**Example**. Fermat proved (by his *infinite descent*) that the diophantine equation

$$x^4 - y^4 = z^2$$

does not have any non-trivial integer solution.

Remark. (i) The above equation can be "projectivized" to  $x^4 - y^4 = x^2 z^2$ , which gives an elliptic curve *E* with *complex multiplication* by  $\mathbb{Z}[\sqrt{-1}]$ .

#### GEOMETRY ANI NUMBERS

#### Ching-Li Chai

Diophantine equations Diophantine equations Counting conjunction Counting comparation Counting comparation solution L-Americans and distribution o prime mambers Zeta and L-values

sample of geometric dructures and symmetries Elliptic curve basics Modular forms, modular curves and Bicke symmetry Complex multiplication Probenius symmetry Monodromy Pine structure in characteristic

BEOMETRY AN NUMBERS

#### Ching-Li Chai

Diophantine equation

opparation equation founting congruence solutions -functions and distribution of rime numbers eta and L-values

ample of geometric ructures and /mmetrics liptic curve basics foldear feras, modular urves and Hecke symmetry lengtes multiplication tobestas symmetry fonodromy ion structure in characteristic



Figure: Fermat

# Fermat's infinite descent continued

(ii) Idea: Show that every non-trivial rational point  $P \in E(\mathbb{Q})$  is the image  $[2]_E$  of another "smaller" rational point.

(Construct another rational variety X and maps  $f: E \to X$  and  $g: X \to E$  such that  $g \circ f = [2]_E$  and descent in two stages. Here X is a twist of E, and f, g corresponds to  $[1 + \sqrt{-1}]$  and  $[1 - \sqrt{-1}]$  respectively.)

GEOMETRY AND NUMBERS

Ching-Li Chai

Diophantine equations Counting solutions of a diophantine equation Counting congruence soluti

-rancesons and distribution of rime numbers leta and L-values

sample of geometric dructures and symmetries Elliptic carve basics Modular forens, modular carves and Hecke symmetry Complex multiplication Probablas symmetry Monocomy

NUMBERS Ching-Li Chai

tophantine equatio

oppartance equation founting congruence solution -functions and distribution o rime numbers

iample of geometric tructures and ymmetries Elliptic curve basics Modular forms, nodular curves and Hecke symmetry Complex multiplication Probabalas symmetry Monodromy

Pine structure in characteristi n

# Interlude: Euler's addition formula

In 1751, Fagnano's collection of papers *Produzioni Mathematiche* reached the Berlin Academy. Euler was asked to examine the book and draft a letter to thank Count Fagnano. Soon Euler discovered the addition formula

$$\int_{0}^{r} \frac{d\rho}{\sqrt{1-\rho^{4}}} = \int_{0}^{u} \frac{d\eta}{\sqrt{1-\eta^{4}}} + \int_{0}^{v} \frac{d\psi}{\sqrt{1-\psi^{4}}},$$

where

$$r = \frac{u\sqrt{1-v^4} + v\sqrt{1-u^4}}{1+u^2v^2}.$$





Figure: Euler



Ching-Li Chai

Diophantine equation

ophantine equation ounting congruence solutio dunctions and distribution

a and L-values.

sample of geometric functures and symmetries Modular form, nodular carves and flecke symmetry Complex multiplication Probesias symmetry Monodromy

Nine structure in characteristic

# Counting sums of squares

#### 2. Counting solutions of a diophantine equation

**Example**. Counting sums of squares. For  $n, k \in \mathbb{N}$ , let

$$r_k(n) := #\{(x_1, \dots, x_k) \in \mathbb{Z}^n : x_1^2 + \dots + x_k^2 = n\}$$

be the number of ways to represent n as a sum of k squares.

(i) 
$$r_2(n) = 4 \cdot \sum_{d|n, n \text{ odd}} (-1)^{(d-1)/2} = \begin{cases} 0 & \text{if } n_2 \neq \Box \\ \sum_{d|n_1} 1 & \text{if } n_2 = \Box \end{cases}$$

where  $n = 2^f \cdot n_1 \cdot n_2$ , and every prime divisor of  $n_1$  (resp.  $n_2$ ) is  $\equiv 1 \pmod{4}$  (resp.  $\equiv 3 \pmod{4}$ ).

(ii) 
$$r_4(n) = \begin{cases} 8 \cdot \sum_{d|n} d & \text{if } n \text{ is odd} \\ 24 \cdot \sum_{d|n,d \text{ odd}} d & \text{if } n \text{ is even} \end{cases}$$

#### How to count number of sum of squares

Method. Explicitly identify the theta series

$$heta^k( au) = ig(\sum_{m\in\mathbb{N}} q^{m^2}ig)^k \qquad ext{where } q = e^{2\pi\sqrt{-1}\, au}$$

with modular forms obtained in a different way, such as Eisenstein series.

NUMERS

Chig-JCAN

Sequences

Chig-JCAN

Chig-Sequences

Chig-Sequences
Chig-Sequences

Chig-Sequences

Chig-Sequences

Chig-Sequences
Chig-Sequences

Chig-Sequences
Chig-Sequences

Chig-Sequences

Chig-Sequences

Chig-Seq

#### Counting congruence solutions

#### 3. Counting congruence solutions and L-functions

(a) Count the number of congruence solutions of a given diophantine equation modulo a (fixed) prime number p

(b) Identify the L-function for a given diophantine equation (basically the generating function for the number of congruence solutions modulo p as p varies) with an L-function coming from harmonic analysis. (The latter is associated to a modular form).

Remark. (b) is an essential aspect of the Langlands program.

# Generation and a second second

#### The Riemann zeta function

#### 4. L-functions and the the distribution of prime numbers for a given diophantine problem

**Examples.** (i) The Riemann zeta function  $\zeta(s)$  is a meromorphic function on  $\mathbb{C}$  with only a simple pole at s = 0,

$$\zeta(s) = \sum_{n \ge 1} n^{-s} = \prod_p (1 - p^{-s})^{-1} \quad \text{for } \operatorname{Re}(s) > 1,$$

such that the function  $\xi(s) = \pi^{-s/2} \cdot \Gamma(s/2) \cdot \zeta(s)$  satisfies

$$\xi(1-s) = \xi(s)$$

#### GEORETRY AND NUMERAL Ching: Li Chai Ching: Li Chai Ching: Li Chai Ching: Ching: China Chin



Figure: Riemann

# **Dirichlet L-functions**

(ii) Similar properties hold for the Dirichlet L-function

$$L(\boldsymbol{\chi}, s) = \sum_{n \in N, (n,N)=1} \boldsymbol{\chi}(n) \cdot n^{-s} \qquad \operatorname{Re}(s) > 1$$

for a *primitive* Dirichlet character  $\chi : (\mathbb{Z}/N\mathbb{Z})^{\times} \to \mathbb{C}^{\times}$ .

#### onginario opiani Conting companies olations Tennis nankon Zen and Leuhos Sample of geometric structures and symmetrics Elliptic conv haios Mohafer from, mahar conva adf. Bicko symony Conforcentifications Probasio symony Monotomy P. Ber encuent in characteristic p

GEOMETRY AND NUMBERS Ching-Li Chai

GEORETRY AND NUMBERS Ching-Li Chai Uning-Li Chai Ching-Li Chai Chaine and the second prime and the second prime and the second second prime and the second p



Figure: Dirichlet

# L-functions and distribution of prime numbers

- (a) Dirichlet's theorem for primes in arithmetic progression  $\leftrightarrow L(\chi, 1) \neq 0 \quad \forall$  Dirichlet character  $\chi$ .
- (b) The prime number theorem  $\leftrightarrow$  zero free region of  $\zeta(s)$  near {Re(s) = 1}.
- (c) Riemann's hypothesis  $\leftrightarrow$  the first term after the main term in the asymptotic expansion of  $\zeta(s)$ .



NUMBERS
Ching-Li Chai
arappia arithmetic
alcenerit
alcen

#### Bernoulli numbers and zeta values

#### 5. Special values of L-functions

**Examples.** (a) zeta and L-values for  $\mathbb{Q}$ . Recall that the Bernoulli numbers  $B_n$  are defined by

$$\frac{x}{e^x - 1} = \sum_{n \in \mathbb{N}} \frac{B_n}{n!} \cdot x^n$$

 $B_0 = 1, B_1 = -1/2, B_2 = 1/6, B_4 = -1/30, B_6 = 1/42, B_8 = -1/30, B_{10} = 5/66, B_{12} = -691/2730.$ 

- (i) (Euler)  $\zeta(1-k) = -B_k/k \quad \forall \text{ even integer } k > 0.$
- (ii) (Leibniz's formula, 1678; Madhava, ~ 1400)  $1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots = \frac{\pi}{4}$

## Content of L-values

(b) L-values often contain deep arithmetic/geometric information.

(i) Leibniz's formula:  $\mathbb{Z}[\sqrt{-1}]$  is a PID (because the formula implies that the class number  $h(\mathbb{Q}(\sqrt{-1}))$  is 1).

(ii)  $B_k/k$  appears in the formula for the number of (isomorphism classes of) exotic (4k - 1)-spheres.



#### GEOREM TRAY AND NOMMERS Ching: J i Chai Scape at attacted Composition of the Compo

# Kummer congruence

(c) (Kummer congruence)

(i) 
$$\zeta(m) \in \mathbb{Z}_p$$
 for  $m \le 0$  with  $m \not\equiv 1 \pmod{p-1}$ 

(ii)  $\zeta(m) \equiv \zeta(m') \pmod{p}$  for all  $m, m' \leq 0$  with  $m \equiv m' \not\equiv 1 \pmod{p-1}$ .

Examples.

- $\zeta(-1) = -\frac{1}{2^2 \cdot 3^2}$ ;  $-1 \equiv 1 \pmod{p-1}$  only for p = 2, 3.
- $\zeta(-11) = \frac{691}{2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13}; -11 \equiv 1 \pmod{p-1} \text{ holds}$ only for p = 2, 3, 5, 7, 13.

■ 
$$\zeta(-5) = -\frac{1}{2^2 \cdot 3^2 \cdot 7} \equiv \zeta(-1) \pmod{5}$$
.  
Note that  $3 \cdot 7 \equiv 1 \pmod{5}$ .





Figure: Kummer



## Elliptic curves basics

#### II. Sample of geometric structures and symmetries

#### 1. Review of elliptic curves

Equivalent definitions of an elliptic curve E:

- a projective curve with an algebraic group law;
- a projective curve of genus one together with a rational point (= the origin);
- over  $\mathbb{C}$ : a complex torus of the form  $E_{\tau} = \mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}$ , where  $\tau \in \mathfrak{H} :=$  upper-half plane;
- over a field F with  $6 \in F^{\times}$ : given by an affine equation

$$y^2 = 4x^3 - g_2x - g_3, \quad g_2, g_3 \in F.$$

## Weistrass theory

For  $E_{\tau} = \mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}$ , let

$$\begin{array}{rcl} x_{\tau}(z) & = & \wp(\tau,z) \\ & = & \frac{1}{z^2} + \sum_{(m,n) \neq (0,0)} \left( \frac{1}{(z-m\tau-n)^2} - \frac{1}{(m\tau+n)^2} \right) \end{array}$$

 $y_{\tau}(z) = \frac{d}{dz} \mathcal{O}(\tau, z)$ 

Then  $E_{\tau}$  satisfies the Weistrass equation

$$y_{\tau}^2 = 4x_{\tau}^3 - g_2(\tau)x_{\tau} - g_3(\tau)$$

with

$$\begin{array}{l} \bullet \ g_2(\tau) = 60 \sum_{(0,0) \neq (m,n) \in \mathbb{Z}^2} \frac{1}{(m\tau + n)^4} \\ \\ \bullet \ g_3(\tau) = 140 \sum_{(0,0) \neq (m,n) \in \mathbb{Z}^2} \frac{1}{(m\tau + n)^6} \end{array}$$



NUMBERS Ching-Li Chai

Elliptic curve basics

#### The j-invariant

Elliptic curves are classified by their j-invariant

$$j = 1728 \frac{g_2^3}{g_2^3 - 27g_3^2}$$

Over  $\mathbb{C}$ ,  $j(E_{\tau})$  depends only on the lattice  $\mathbb{Z}\tau + \mathbb{Z}$  of  $E_{\tau}$ . So  $j(\tau)$  is a modular function for SL<sub>2</sub>( $\mathbb{Z}$ ):

$$j\left(\frac{a\tau+b}{c\tau+d}\right) = j(\tau)$$

for all  $a, b, c, d \in \mathbb{Z}$  with ad - bc = 1.

We have a Fourier expansion

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots$$

where  $q = q_{\tau} = e^{2\pi\sqrt{-1}\tau}$ .

# Modular forms, modular curves and Hecke symmetry

#### 2. Modular forms and modular curves

Let  $\Gamma \subset SL_2(\mathbb{Z})$  be a congruence subgroup of  $SL_2(\mathbb{Z})$ , i.e.  $\Gamma$  contains all elements which are  $\equiv I_2 \pmod{N}$  for some N.

(a) A holomorphic function  $f(\tau)$  on the upper half plane  $\mathbb{H}$  is said to be a *modular form* of weight *k* and level  $\Gamma$  if

$$f((a\tau+b)(c\tau+d)^{-1}) = (c\tau+d)^k \cdot f(\tau) \quad \forall \gamma = \left( \begin{array}{c} a & b \\ c & d \end{array} \right) \in \Gamma$$

and has moderate growth at all cusps.

(b) The quotient  $Y_{\Gamma} := \Gamma \setminus \mathbb{H}$  has a natural structure as an (open) algebraic curve, definable over a natural number field; it parametrizes elliptic curves with suitable level structure.

GEOUTERYADES LINEAREZA UNERREZA SEGUERADES ALEGUERADES ALEGUERADES

NUMBERS Ching-Li Chai

#### Modular curves and Hecke symmetry

(c) Modular forms of weight *k* for  $\Gamma = H^0(X_{\Gamma}, \omega^k)$ , where  $X_{\Gamma}$  is the natural compactification of  $Y_{\Gamma}$ , and  $\omega$  is the Hodge line bundle on  $X_{\Gamma}$ 

$$\omega|_{[E]} = \text{Lie}(E)^{\vee} \quad \forall [E] \in X_{\Gamma}$$

(d) The action of  $GL_2(\mathbb{Q})_{det>0}$  on  $\mathbb{H}$  "survives" on the modular curve  $Y_{\Gamma} = \Gamma \setminus \mathbb{H}$  and takes a reincarnated form as a family of algebraic correspondences.

The L-function attached to a cusp form which is a *common eigenvector* of all Hecke correspondences admits an Euler product.





Figure: Hecke

NUMBERS

NUMBERS

Ching-Li Chai

remple artitements

remple artite

#### The Ramanujan $\tau$ function

**Example.** Weight 12 cusp forms for  $SL_2(\mathbb{Z})$  are constant multiples of

$$\Delta = q \cdot \prod_{m \ge 1} (1 - q^m)^{24} = \sum_n \tau(n) q'$$

and

$$T_p(\Delta) = \tau(p) \cdot \Delta \quad \forall p,$$

where  $T_p$  is the Hecke operator represented by  $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ .

Let  $L(\Delta, s) = \sum_{n \ge 1} a_n \cdot n^{-s}$ . We have

$$L(\Delta, s) = \prod_{p} (1 - \tau(p)p^{-s} + p^{11-2s})^{-1}.$$

Giosense and a second a second

NUMBERS Ching-Li Chai

# CM elliptic curves

#### 3. Complex multiplication

An elliptic E over  $\mathbb{C}$  is said to have complex multiplication if its endomorphism algebra  $\text{End}^0(E)$  is an imaginary quadratic field.

Example. Consequences of

- j(ℂ/𝒫<sub>K</sub>) is an algebraic integer
- K · j(ℂ/𝒪<sub>K</sub>) = the Hilbert class field of K.

$$e^{\pi\sqrt{67}} = 147197952743.9999986624542245068292613\cdots$$
  
$$j\left(\frac{-1+\sqrt{-67}}{2}\right) = -147197952000 = -2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$$

$$\begin{split} e^{\pi\sqrt{163}} &= 262537412640768743.99999999999999992007259719\ldots \\ j\left(\frac{-1+\sqrt{-163}}{2}\right) &= -262537412640768000 = \\ &-2^{18}\cdot 3^3\cdot 5^3\cdot 23^3\cdot 29^3 \end{split}$$

## Mod p points for a CM curve

A typical feature of CM elliptic curves is that there are explicit formulas: Let *E* be the elliptic curve

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

which has CM by  $\mathbb{Z}[\sqrt{-1}]$ . We have

$$#E(\mathbb{F}_p) = 1 + p - a_p$$

and for odd p we have

$$\begin{aligned} a_p &= \sum_{u \in \mathbb{F}_p} \left( \frac{u^3 + u}{p} \right) \\ &= \begin{cases} 0 & \text{if } p \equiv 3 \pmod{4} \\ -2a & \text{if } p = a^2 + 4b^2 \text{ with } a \equiv 1 \pmod{4} \end{cases} \end{aligned}$$

# A CM curve and its associated modular form, continued

The L-function L(E,s) attached to E with

$$\prod_{p \text{ odd}} (1 - a_p p^{-s} + p^{1-2s})^{-1} = \sum_n a_n \cdot n^{-s}$$

is equal to a Hecke L-function  $L(\psi, s)$ , where the Hecke character  $\psi$  is the given by

$$\psi(\mathfrak{a}) = \begin{cases} 0 & \text{if } 2|N(\mathfrak{a}) \\ \lambda & \text{if } \mathfrak{a} = (\lambda), \ \lambda \in 1 + 4\mathbb{Z} + 2\mathbb{Z}\sqrt{-1} \end{cases}$$

The function  $f_E(\tau) = \sum_n a_n \cdot q^n$  is a modular form of weight 2 and level 4, and

$$f_E( au) = \sum_{\mathfrak{a}} \psi(\mathfrak{a}) \cdot q^{\operatorname{N}(\mathfrak{a})} = \sum_{a \equiv 1 \pmod{4} \ b \equiv 0 \pmod{2}} a \cdot q^{a^2 + b^2}$$

NUMBERS Ching-Li Chai

Complex multiplication

#### Frobenius symmetry

#### 4. Frobenius symmetry

Every algebraic variety X over a finite field  $\mathbb{F}_q$  has a map  $\operatorname{Fr}_q : X \to X$ , induced by the ring endomorphism  $f \mapsto f^q$  of the function field of X.

Deligne's proof of Weil's conjecture implies that

$$\tau(p) \le 2p^{11/2} \quad \forall p$$

Idea: Step 1. Use Hecke symmetry to cut out a 2-dimensional Galois representation inside  $H^1_{et}(\overline{X}, Sym^{10}(\underline{H}(\mathscr{E}/X)))$ , which "contains" the cusp form  $\Delta$  via the Eichler-Shimura integral.

Step 2. Apply the Eichler-Shimura congruence relation, which relates  $Fr_p$  and the Hecke correspondence  $T_p$ ; invoke the Weil bound.

#### A hypergeometric differential equation

#### 5. Monodromy

(a) The hypergeometric differential equation

$$4x(1-x)\frac{d^2y}{dx^2} + 4(1-2x)\frac{dy}{dx} - y = 0$$

has a classical solution

$$F(1/2, 1/2, 1, x) = \sum_{n \ge 0} {\binom{-1/2}{n}} x^n$$

The global monodromy group of the above differential is the principal congruence subgroup  $\Gamma(2)$ .

GEOMITRY AND NUMBERS Ching-LLChai Ching-LLCh

## Historic origin

Remark. The word "monodromy" means "run around singly"; it was (?first) used by Riemann in *Beiträge zur Theorie der* durch die Gauss'sche Reihe  $F(\alpha, \beta, \gamma, x)$  darstellbaren Functionen, 1857.

...; für einen Werth in welchem keine Verzweigung statfindet, heist die Function "einändrig order monodrom ...

#### GEOMETRY AND NUMBERS

Ching-Li Chai

statements Displantice equations Counting subtices of a displantice equation Counting congruence solution L-functions and distribution of prime numbers Zeta and L-values Sample of geometric structures and

Elliptic curve basics Modular forms, modular curves and Hecke symmetry Complex multiplication Probasius commetry

#### Fine structure in charac

#### The Legendre family of elliptic curves

The family of equations

$$y^2 = x(x-1)(x-\lambda)$$
  $0, 1, \infty \neq \lambda \in \mathbb{P}^1$ 

defines a family  $\pi : \mathscr{E} \to S = \mathbb{P}^1 - \{0, 1, \infty\}$  of elliptic curves, with

 $j(E_{\lambda}) = \frac{2^8 \left[1 - \lambda(1 - \lambda)\right]^3}{\lambda^2 (1 - \lambda)^2}$ 

This formula exhibits the  $\lambda$ -line as an  $S_3$ -cover of the *j*-line, such that the 6 conjugates of  $\lambda$  are

$$\lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda}$$

NUMBERS Ching-Li Chai ample arithmetic aternetis Xophanice optains Statig obtains of a phase of the statistic chains and division of the numbers and L-ulus ample of geometric ructures and

Illiptic curve basics fodular forms, modular urves and Hocke symmetr Temples multiplication

lonodromy

Tine structure in characteristic

# The Legendre family, continued

The formula

$$\left[4\lambda\left(1-\lambda\right)\frac{d}{d\lambda^{2}}+4\left(1-2\lambda\right)\frac{d}{d\lambda}-1\right]\left(\frac{dx}{y}\right)=-d\left(\frac{y}{(x-\lambda)^{2}}\right)$$

means that the global section [dx/y] of  $\underline{H}^{l}_{dR}(\mathscr{E}/S)$  satisfies the above hypergeometric ODE.

#### Monodromy and symmetry

1. Monodromy can be regarded as attainable symmetries among *potential symmetries*.

2. To say that the monodromy is "as large as possible" is an irreducibility statement.

 Maximality of monodromy has important consequences.
 E.g. the key geometric input in Deligne-Ribet's proof of *p*-adic interpolation for special values of Hecke L-functions attached to totally real fields.

#### NUMBERS Ching-Li Chai ample arithmetic tatements Copposition oparions Conting conjunctor obtains Conting compares obtains of prime rambos

GEOMETRY AND

ample of geometric tructures and ymmetries Eliptic curve basics Modular ferus, modular curves and Hecke symmetry Complex multiplication Probetikas symmetry Monodecrey

Pine structure in characteris

#### GEOMETRY AND NUMBERS

#### Ching-Li Chai

Sample arithmetic statements Diophastise equations Counting solutions of a diophastise equation Counting congruence solution L-functions and diorrhoutine optime numbers Zota and L-values

ample of geometric tructures and ymmetries Elliptic curve basics Modular forms, modular curves and Hecke symmetry Complex multiplication

#### Monodromy

Fine structure in characteristic p

#### Supersingular elliptic curves

#### 6. Fine structure in char. p > 0

**Example**. (ordinary/supersingular dichotomy) Elliptic curves over an algebraically closed field  $k \supset \mathbb{F}_p$  come in two flavors.

- Those with E(k) ≃ (0) are called supersingular.
  - There is only a *finite* number of supersingular *j*-values.
  - An elliptic curve E over a finite field 𝔽<sub>q</sub> is supersingular if and only if E(𝔽<sub>q</sub>) ≡ 0 (mod p).
- Those with  $E[p](k) \simeq \mathbb{Z}/p\mathbb{Z}$  are said to be ordinary.

An elliptic curve *E* over a finite field  $\mathbb{F}_q$  is supersingular if and only if  $E(\mathbb{F}_q) \not\equiv 0 \pmod{p}$ 

# The Hasse invariant

For the Legendre family, the supersingular locus (for p > 2) is the zero locus of

$$A(\lambda) = (-1)^{(p-1)/2} \cdot \sum_{j=0}^{(p-1)/2} \left(\frac{(1/2)_j}{j!}\right)^2 \cdot \lambda^j$$

where  $(c)_m := c(c+1)\cdots(c+m-1)$ .

Remark. The above formula for the coefficients  $a_i$  satisfy

$$a_1, ..., a_{(p-1)/2} \in \mathbb{Z}_{(p-1)/2}$$

and

$$a_{(p+1)/2} \equiv \cdots \equiv a_{p-1} \equiv 0 \pmod{p}$$
.

#### NUMBERS Ching-Li Chai

attements Sophamine oparions Country solutions of a Sophamine country Country solutions Country comparation Country of the country Country of the country Country of the country And the country of the country Sample of geometric Structures and Somple of geometric

ymmetrics Elliptic curve basics Modular forms, modular curves and Hecke symmetry Complex multiplication Probenius symmetry Monodromy

Fine structure in characterise p

NUMBERS Ching-Li Chai

Fine structure in chara

# Counting supersingular j-values

**Theorem.** (Eichler 1938) The number  $h_p$  of supersingular *j*-values is

$$h_p = \begin{cases} \lfloor p/12 \rfloor & \text{if } p \equiv 1 \pmod{12} \\ \lceil p/12 \rceil & \text{if } p \equiv 5 \text{ or } 7 \pmod{12} \\ \lceil p/12 \rceil + 1 & \text{if } p \equiv 11 \pmod{12} \end{cases}$$

Remark. (i) It is known that  $h_p$  is the *class number* for the quaternion division algebra over  $\mathbb{Q}$  ramified (exactly) at p and  $\infty$ .

(ii) Deuring thought that it is nicht leicht that the above class number formula can be obtained by counting supersingular *j*-invariants directly.

#### Igusa's proof

From the hypergeometric equation for F(1/2, 1/2, 1, x) we conclude that

$$\left[ 4\lambda \left(1-\lambda\right) \frac{d^2}{d\lambda^2} + 4\left(1-2\lambda\right) \frac{d}{d\lambda} - 1 \right] A(\lambda) \equiv 0 \pmod{p}$$

for all p > 3. It follows immediately that  $A(\lambda)$  has simple zeroes. The formula for  $h_p$  is now an easy consequence. (Hint: Use the formula 6-to-1 cover of the *j*-line by the  $\lambda$ -line.) Q.E.D.



NUMBERS Ching-Li Chai

Fine structure in chara

#### p-adic monodromy for modular curves

For the ordinary locus of the Legendre family

$$\pi : \mathscr{E}^{ord} \to S^{ord}$$

the monodromy representation

$$\rho: \pi_1\left(S^{\operatorname{ord}}\right) \to \operatorname{Aut}\left(\mathscr{E}^{\operatorname{ord}}[p^{\infty}](\overline{\mathbb{F}}_p)\right) \cong \mathbb{Z}_p^{\times}$$

(defined by Galois theory) is surjective.

#### *p*-adic monodromy for the modular curve

Sketch of a proof: Given any n > 0 and any  $\bar{u} \in (\mathbb{Z}/p^n\mathbb{Z})^{\times}$ , pick a representative  $u \in \mathbb{N}$  of  $\bar{u}$  with  $0 < u < p^n$  and let let

$$\iota : \mathbb{Q}[T]/(T^2 - u \cdot T + p^{4n}) \hookrightarrow \mathbb{Q}_p$$

be the embedding such that  $\iota(T) \in \mathbb{Z}_p^{\times}$ . Then

$$\iota(T) \equiv u \pmod{p^{2n}}.$$

By a result of Deuring, there exists an elliptic curve E over  $\mathbb{F}_{p^{2n}}$ whose Frobenius is the Weil number t(T). So the image of the monodromy representation contains t(T), which is congruent to the given element  $\tilde{u} \in \mathbb{Z}/p^{\sigma}\mathbb{Z}$ . Q.E.D.

#### GEOMETRY AND NUMBERS Ching-Li Chai Ching-Li Chai Chaines devices and Context and the second Context and the second

Fine structure in chara

COMMETRY AND NUMBERS Charge - L Char Service - Characteristic Char