The background features a complex pattern of overlapping circles in various colors (white, orange, yellow) on a black field. A bright, multi-colored spot (green, yellow, orange) is located at the center of the pattern, from which the circles appear to radiate.

# Number Theory

## Book 3

$$J(x) = Li(x) - \sum_{\rho}^{\infty} Li(x^{\rho}) - \log(2) + \int_x^{\infty} \frac{1}{t(t^2 - 1)\log(t)} dt$$

An elliptic curve  $E(\mathbb{F}_q)$  over a finite field is an additive abelian group which is either cyclic  $C_n$  or a direct sum  $C_n \oplus C_m$  (typically  $n|m$  with  $n$  small).

The order  $|E(\mathbb{F}_q)| \in [q+1-2\sqrt{q}, q+1+2\sqrt{q}]$  by the Hasse bound or HW bound.

$x^2+y^2=-1$  is a curve of genus 0 (nonsingular conic)

Over  $\mathbb{F}_q$  ( $q$  odd) we have  $q+1$  points.

For curves of genus  $g \geq 2$ :  $X(\mathbb{Q})$  is a finite set. Mordell's Conjecture, proved by Gerd Faltings (1983).

eg. for any fixed  $n \geq 3$ , the equation  $x^n + y^n = 1$  has at most finitely many rational points. (For  $n=3$ ,  $g=1$ , elliptic curve, Fermat curve with finitely many rational points. For  $n \geq 7$ ,  $g > 1$ .) This precedes the proof by Wiles & others of Fermat's Last Theorem.

---

Elliptic curves have applications in cryptography and primality testing and integer factorization.

AKS: There is a deterministic poly. time algorithm for deciding whether or not a given integer is a prime. Given  $n$ , the running time is bounded by  $c \cdot (\log n)^6$ .

For practical implementation, however, we almost always still use probabilistic algorithms.

Fermat test: Given  $n$ , pick  $a \in \{2, \dots, n-1\}$  randomly. Compute  $a^{n-1} \pmod n$ .

If  $a^{n-1} \not\equiv 1 \pmod n$ , return " $n$  is composite."

If  $a^{n-1} \equiv 1 \pmod n$ , pick a different  $a \in \{2, \dots, n-1\}$  and repeat.

If we stop after  $100$  trials (say) then we have a one-sided error ("false positive").

Rabin-Miller: improvement of Fermat test. Less likelihood of error but it still has one-sided errors (false positives).

The Elliptic curve test for primality: given  $n$  we do a certain computation.

If  $n$  passes the test then  $n$  is guaranteed to be prime

If  $n$  fails the test, repeat the test with a different point on a different curve.

One-sided error (false negative) if we decide to stop after 100 trials, say.

Combining Rabin-Miller with Elliptic curve test (alternately) it is extremely unlikely to not get a guarantee in 100 trials.

Example using Elliptic Curves to prove primality of  $n = 10^{10} + 19 = 10,000,000,019$  using the Goldwasser-Kilian algorithm (1986?) believed to be poly. time (probabilistic).

We take an elliptic curve over  $\mathbb{Z}/n\mathbb{Z}$  chosen randomly but with a known point

$$P \in E(\mathbb{Z}/n\mathbb{Z}).$$

What can we do with  $F = \mathbb{Z}/n\mathbb{Z}$ ? If  $n = \text{prime}$  then  $F$  is a field.

If  $n = pq$ ,  $p \neq q$  large primes (say hundreds of digits) then  $F$  is not a field.

Imagine  $n = pq$  composite but very difficult to factor if  $p, q$  large.

Given  $a, b \in F$ ,  $\frac{a}{b}$  is practically defined if  $b \neq 0$ .  $\gcd(b, n) \in \{1, p, q\}$

The case  $\gcd(b, n) \in \{p, q\}$  only arises if we are able to factor  $n$ , so we return "n is not a prime". Otherwise  $\gcd(b, n) = 1 = rb + sn$  for some  $r, s \in \mathbb{Z}$  by Euclid's Algorithm

so  $\frac{a}{b} = r$  in  $F$ . The computation proceeds.

If  $n$  is not prime and  $n = kq$ ,  $k > 1$ ,  $q$  prime,

$$\underbrace{E(\mathbb{Z}/n\mathbb{Z})}_{\text{"elliptic curve over } \mathbb{Z}/n\mathbb{Z}} \xrightarrow{\text{almost-homo}} \underbrace{E(\mathbb{Z}/q\mathbb{Z})}_{\text{actual elliptic curve}}$$

meaning: if  $P, Q \in E(\mathbb{Z}/n\mathbb{Z})$  where  $P+Q \in E(\mathbb{Z}/n\mathbb{Z})$  is well-defined then  $\overline{P+Q} = \overline{P+Q}$  where "bar" is "mod  $q$ ".

but not strictly speaking an elliptic curve since  $\mathbb{Z}/n\mathbb{Z}$  is not a field.

Example Show  $n = 10^{10} + 19 = 10000000019$  is prime. Proof by contradiction.

Supposing  $n$  is composite  $n$  has a prime factor  $p \leq \sqrt{n}$  so  $p < 10^5 = 100,000$ .

This will lead to a contradiction.

Randomly I choose elliptic curves  $y^2 = x^3 + ax + b$  containing a point  $P(3, 5)$ . To check that this is an elliptic curve, need  $4a^3 + 27b^2 \not\equiv 0 \pmod{n}$  discriminant of  $x^3 + ax + b$

$E$	$ E(\mathbb{Z}/n\mathbb{Z}) $
$y^2 = x^3 + x - 5$	$9999935488 = 2^3 \cdot 3 \cdot 19 \cdot 1761 \cdot 7649$
$y^2 = x^3 + 2x - 8$	$1000162104 = 2^3 \cdot 3 \cdot 29 \cdot 547 \cdot 26267$
$y^2 = x^3 + 3x - 11$	$10000053492 = 2^3 \cdot 3 \cdot 11 \cdot 13 \cdot 37 \cdot 239 \cdot 659$
$y^2 = x^3 + 4x - 14$	$9999892527 = \underbrace{3 \cdot 19 \cdot 89}_k \cdot \underbrace{1771199}_q = n$

Corrected!

$$4a^3 + 27b^2 = (27b - 18ax)(x^3 + ax + b) + (4a^2 - 9bx + 6ax^2)(3x + a)$$

To prove that  $n$  is prime, we argue by contradiction. If not there is a prime  $p \leq \sqrt{n}$ ,  $p | n$ .

So  $p < 100,000$ .

Then there is an almost-homomorphism  $\hat{E}(\mathbb{Z}/n\mathbb{Z}) \rightarrow E(\mathbb{F}_p)$

The point  $kP \in E(\mathbb{Z}/n\mathbb{Z})$  has order  $q$ .

We have presumably checked recursively that  $q$  is prime.

"elliptic curve" over  $\mathbb{Z}/n\mathbb{Z}$

actual elliptic curve over  $\mathbb{F}_p$ .

So  $E(\mathbb{F}_p)$  has a point of order  $q$ .

Check:  $mP = 0$   
 $kP \neq 0$ .

$E(\mathbb{F}_p)$  has order  $\leq p+1+2\sqrt{p} \leq 100,632$  but  $q$  is bigger than this, contradiction.

A revised version of Goldwasser-Kilian algorithm replaces the arbitrary elliptic curves with special curves called CM curves where the group order is easier to compute.

Elliptic Curve Factorization Method (Lenstra)

Given  $n$  large integer which is known to be composite, we want to split  $n = ab$ ,  
 $1 < a, b < n$  (nontrivial factorization).

Choose random elliptic curves  $E(\mathbb{Z}/n\mathbb{Z})$  with known point  $P$ .

Do extensive sums in  $\langle P \rangle = \{kP : k \in \mathbb{Z}\}$  until we find a failure of chord-tangent method where division by  $b \in \mathbb{Z}/n\mathbb{Z}$  fails,  $\gcd(b, n) \in \{2, \dots, n-1\}$  giving a splitting of  $n$ .

This is subexponential time in practice, like the best sieve methods.

Applications to public key cryptography:

Classical Diffie-Hellman protocol for key distribution: This allows two parties to agree on a secret key (typically, <sup>long</sup> alphanumeric string) while communicating over an insecure channel.

We want to generate a secret key over an open channel: a secret number which should be hundreds of digits long. How to do this:

Alice and Bob first choose a large prime  $p$  (probably a few hundred digits long). They also agree on a primitive element  $g \pmod p$  i.e. all nonzero elements of  $\mathbb{F}_p$  are powers of  $g$ . (Eg. if  $p=1009$ ,  $g=11$  is primitive. In  $\mathbb{F}_{1009}$

$$\begin{aligned} 11^0 &= 1 \\ 11^1 &= 11 \\ 11^2 &= 121 \\ 11^3 &= 1331 = 322 \\ 11^4 &= 515 \\ 11^5 &= 620 \\ &\vdots \\ 11^{1007} &= 367 \\ 11^{1008} &= 1 \\ 11^{1009} &= 11 \\ &\vdots \end{aligned}$$

where is  $186 \in \mathbb{F}_{1009}$  in this list?

$$11^k = 186 \text{ in } \mathbb{F}_{1009} \text{ for some unique } k \in \{0, 1, 2, \dots, 1007\}$$

What is  $k$ ?  $k=543$  is the answer.

Why is the set of nonzero elements of a finite field a cyclic group?

eg.  $\mathbb{F}_5$  has four nonzero elements forming a multiplicative group of order 4. If this group is a Klein 4-group then the poly.  $x^2-1$  has four roots in  $\mathbb{F}_5$ .

Alice and Bob agree on  $p$  and  $g$  (as above) over the open channel (not secure).

Secretly, Alice chooses  $a \in \{1, 2, \dots, p-2\}$  at random. She computes  $g^a \in \mathbb{F}_p$  and sends this to Bob (over the open channel).

Bob (secretly) chooses  $b \in \{1, 2, \dots, p-2\}$  and computes  $g^b \in \mathbb{F}_p$  and sends this to Alice.

The information  $p, g, g^a, g^b$  have been shared over the open channel;  $a, b$  are secret.

The secret key known to Alice and Bob is  $g^{ab}$ .

Alice computes  $(g^b)^a = g^{ab}$

Bob computes  $(g^a)^b = g^{ab}$

Is there a shortcut to computing  $g^{ab}$  without first finding  $a$  or  $b$ ?  
Not as far as we know.

ElGamal uses Diffie-Hellman

Other groups in place of  $\mathbb{F}_q^* = \{a \in \mathbb{F}_q : a \neq 0\}$

However elliptic curves over finite field can provide the same amount of security with shorter key length

Substitute the group of the curve for  $\mathbb{F}_q^*$

Fix curve,  $P$  point.

Alice chooses large integer  $a$ , computes  $aP$ , sends this to Bob.

Bob chooses large integer  $b$ , computes  $bP$ , sends this to Alice.

The secret key is  $abP = a(bP) = b(aP)$ .

# Modular Forms (and Elliptic Curves) - Neal Koblitz

Example: the  $j$ -invariant,  $j(\tau)$  is usually expressed as a function of  $q = e^{2\pi i \tau}$

First define  $g_2(\tau) = 60 \sum_{(m,n) \neq (0,0) \in \mathbb{Z}^2} \frac{1}{(m+n\tau)^4}$

$$g_3(\tau) = 140 \sum_{(m,n) \neq (0,0) \in \mathbb{Z}^2} \frac{1}{(m+n\tau)^6}$$

$$\eta(\tau) = q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n)$$

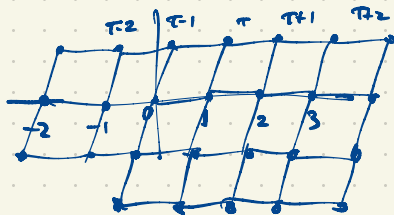
$$j(\tau) = \frac{1728 \frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2}}{1728} = \frac{1728 g_2(\tau)^3}{(2\pi)^{12} \eta(\tau)^{24}}$$

$1728 = 12^3$

$$= \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + 20245856256q^4 + \dots$$

$g_2(\tau), g_3(\tau)$  depend only on the lattice

$$\{m+n\tau : m, n \in \mathbb{Z}\} \subset \mathbb{C}$$



So  $j(\tau)$  only depends on this lattice

The Monster (largest sporadic finite simple group)  $M = F_4$  can be written as a subgroup (isomorphic to) of  $GL_{196883}(\mathbb{C})$

Monstrous Moonshine

$$\mathbb{C} / \{m+n\tau : m, n \in \mathbb{Z}\} \cong \text{torus } T^2 \cong S^2 \cong S^1 \times S^1$$

$\cong$  the elliptic curve  $y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$ .

Two such curves are equivalent up to analytic isomorphism iff they have the same  $j$ -invariant.

Scaling a lattice  $L \subset \mathbb{C}$  by  $\alpha \neq 0$  ( $\alpha \in \mathbb{C}$ ) gives  $\alpha L$  with  $\mathbb{C}/\alpha L \cong \mathbb{C}/L$   
 elliptic curves are essentially the same.

$$L = \mathbb{Z}u + \mathbb{Z}v \quad (u, v \text{ base for } L)$$

$$= \{au + bv : a, b \in \mathbb{Z}\}$$

WLOG  $u=1$  otherwise scale the entire lattice by  $u^{-1}$ .

Then  $L = \mathbb{Z} + \mathbb{Z}\tau = \langle 1, \tau \rangle$

Also we may assume  $\tau$  is in the upper half-plane ( $\text{Im } \tau > 0$ ) otherwise pick new basis.

$\{1, 1+\tau\}$  generates the same lattice hence the same elliptic curve  $\mathbb{C}/\langle 1, \tau \rangle$

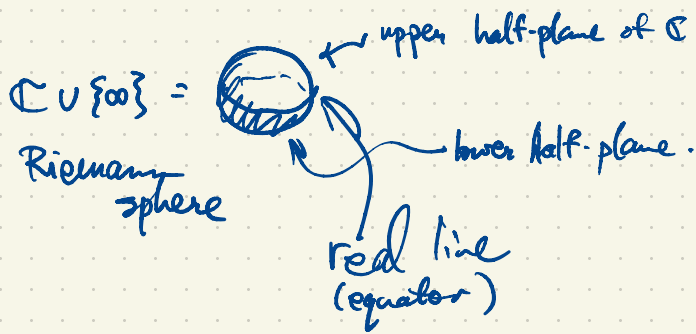
Also  $\langle 1, \tau^{-1} \rangle$  gives essentially the same curve  
 $\downarrow$  scale by  $\tau$   
 $\langle \tau, 1 \rangle$

More generally, the group  $SL_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{Z}) : ad-bc=1 \right\}$  acts on  $\mathbb{C} \cup \{\infty\}$  by fractional linear transformations  
 $g(z) = \frac{az+b}{cz+d}$ ,  $g^{-1}(z) = \frac{dz-b}{-cz+a}$

The map  $\tau \mapsto \tau+1$  is really  $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}(\tau) = \frac{1\tau+1}{0\tau+1} = \tau+1$   
 $\tau \mapsto -\tau^{-1}$  is  $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}(\tau) = \frac{0\tau+1}{-\tau+0} = -\frac{1}{\tau}$

But  $\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \rangle = SL_2(\mathbb{Z})$  (generate as group)  
 Actually  $SL_2(\mathbb{Z}) \rightarrow PSL_2(\mathbb{Z})$  is 2-to-1 homomorphism

$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$  and  $\begin{bmatrix} a & -b \\ c & -d \end{bmatrix}$   
 $g, -g \in SL_2(\mathbb{Z})$   
 give the same fractional linear transformation



$SL_2(\mathbb{Z})$  maps  $\mathbb{R} \cup \{\infty\} \rightarrow \mathbb{R} \cup \{\infty\}$  (equator)

upper half-plane  $\rightarrow$  upper half-plane

lower  $\dots \rightarrow$  lower half-plane

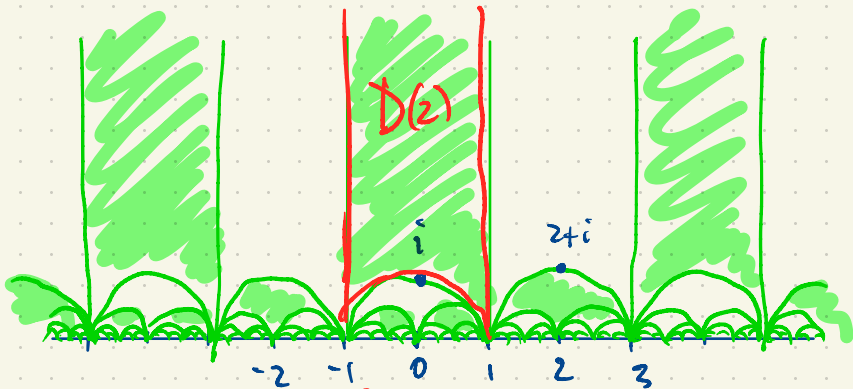
$PSL_2(\mathbb{Z})$  has no subgroup of index 2 (using a simplicity argument)

$j(\tau) = j(\tau+1) = j(\bar{\tau}^{-1})$  so  $j\left(\frac{a\tau+b}{c\tau+d}\right) = j(\tau)$  for all  $a, b, c, d \in \mathbb{Z}$ ,  $ad-bc=1$ .

$j(\tau)$  is invariant under the modular group  $PSL_2(\mathbb{Z})$ .

We construct a fundamental domain  $\mathcal{D} \subset \mathbb{H} = \{\tau \in \mathbb{C} : \text{Im} \tau > 0\}$  upper half-plane:

for every point in  $\mathbb{H}$  there is a unique  $g \in PSL_2(\mathbb{Z})$  mapping it into  $\mathcal{D}$



$\mathcal{D}(2)$  is a fund.

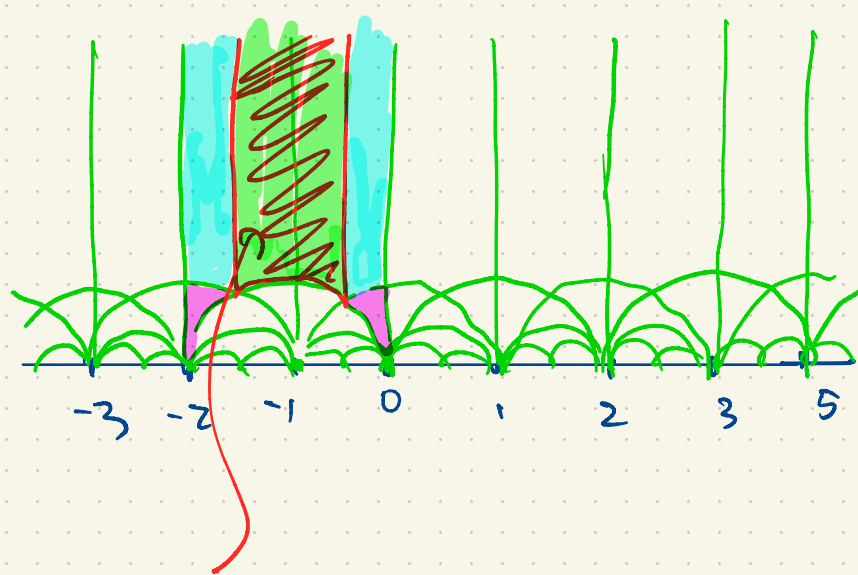
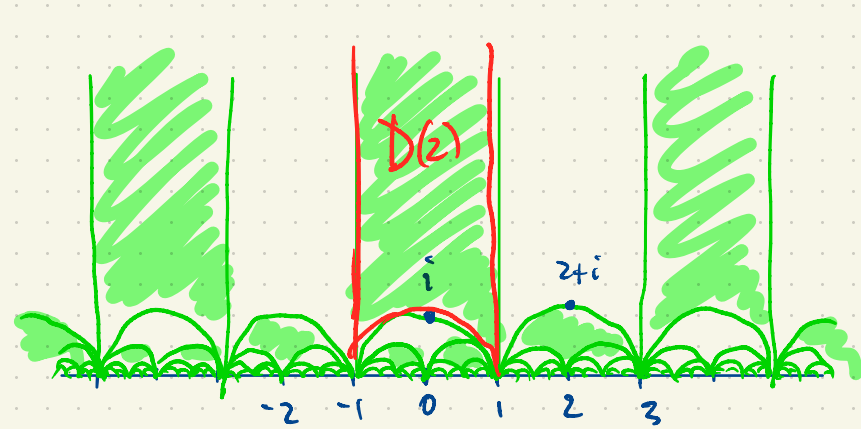
domain for

$\tilde{\Gamma}(2) < \Gamma$  generated

by  $\tau \mapsto \tau+2$ ,  $\tau \mapsto -\frac{1}{\tau}$

$\begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix} \in \tilde{\Gamma}(2)$ ,  $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in \Gamma(2)$

$$\mathcal{D}(2) = \{\tau \in \mathbb{C} : \text{Im} \tau > 0, -1 < \text{Re} \tau < 1, |\tau| > 1\}$$



$$D = \left\{ \tau \in \mathbb{C} : \text{Im} \tau > 0, -\frac{1}{2} < \text{Re} \tau < \frac{1}{2}, |\tau| > 1 \right\}$$

$$\begin{aligned} \mathrm{PSL}_2(\mathbb{Z}) &= \{ \text{fractional linear transformations } g(z) = \frac{az+b}{cz+d} : a, b, c, d \in \mathbb{Z}, ad-bc=1 \} \\ &= \mathrm{SL}_2(\mathbb{Z}) / \{ \pm I \} = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}, ad-bc=1 \} / \{ \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \} \end{aligned}$$

$$\Gamma(p) = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{p} \}, \quad p \text{ prime}$$

$\mathbb{Z} = \mathbb{Z}(\mathrm{SL}_2(\mathbb{Z}))$

(principal congruence subgroup)

normal subgroup of  $\mathrm{SL}_2(\mathbb{Z}) =$

$$\mathrm{PSL}_2(\mathbb{Z}) / \Gamma(p) \cong \mathrm{PSL}_2(\mathbb{F}_p)$$

$\mathrm{PSL}_2(\mathbb{Z}) \xrightarrow{\text{onto}} \mathrm{PSL}_2(\mathbb{F}_p)$  by taking all entries mod  $p$ ; its kernel is  $\Gamma(p)$ .

simple group for  $p > 3$ .

$$\Gamma(2) = \begin{bmatrix} 0 & \mathbb{E} \\ \mathbb{E} & 0 \end{bmatrix} = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{PSL}_2(\mathbb{Z}) : a, d \text{ odd}; b, c \text{ even} \} = \text{"identity mod 2"}$$

$$\Gamma = \begin{bmatrix} 0 & \mathbb{E} \\ \mathbb{E} & 0 \end{bmatrix} \cup \begin{bmatrix} \mathbb{E} & 0 \\ 0 & \mathbb{E} \end{bmatrix} \cup \begin{bmatrix} 0 & 0 \\ \mathbb{E} & 0 \end{bmatrix} \cup \begin{bmatrix} 0 & \mathbb{E} \\ 0 & 0 \end{bmatrix} \cup \begin{bmatrix} 0 & 0 \\ 0 & \mathbb{E} \end{bmatrix} \cup \begin{bmatrix} \mathbb{E} & 0 \\ 0 & 0 \end{bmatrix}$$

$$\mathrm{PSL}_2(\mathbb{F}_2) = \{ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \} \cong \mathrm{SL}_2(\mathbb{F}_2) \cong \mathrm{GL}_2(\mathbb{F}_2) \cong \mathrm{PGL}_2(\mathbb{F}_2)$$

$[\Gamma : \Gamma(2)] = 6$  so a fundamental domain for  $\Gamma(2)$  has six copies of  $D$  (fund. domain for  $\Gamma$ ).

Counting representations of  $n$  as a sum of squares:

$$\theta(q) = \sum_{k \in \mathbb{Z}} q^{k^2} = \dots + q^9 + q^4 + q + 1 + q + q^4 + q^9 + \dots = 1 + 2q + 2q^4 + 2q^9 + 2q^{16} + \dots$$

Generating function for the number of ways of writing  $n$  as a sum of two squares:

$$\begin{aligned} \theta(q)^2 &= 1 + 4q + 4q^2 + 4q^4 + 8q^5 + 4q^8 + 4q^9 + 8q^{10} + \dots \\ &= (1 + 2q + 2q^4 + 2q^9 + \dots)(1 + 2q + 2q^4 + 2q^9 + \dots) \end{aligned}$$

$$\theta(q)^4 = 1 + 8q + 24q^2 + 32q^3 + 24q^4 + \dots = \sum_{n=0}^{\infty} \left( \underbrace{\hspace{10em}} \right) q^n$$

$$5 = a^2 + b^2 \text{ for } (a,b) \in \{(\pm 1, \pm 2), (\pm 2, \pm 1)\}$$

$$(\pm 1, 0, 0, 0), (0, \pm 1, 0, 0), \dots$$

$$(\pm 1, \pm 1, 0, 0), \dots$$

$$(\pm 1, \pm 1, \pm 1, 0), (\pm 1, \pm 1, \pm 1, \pm 1), (\pm 2, 0, 0, 0)$$

For  $n > 0$ ,  $8\sigma(n) - 32\sigma\left(\frac{n}{4}\right)$

$$\sigma(1) = 1$$

$$\sigma(2) = 1 + 2 = 3$$

$$\sigma(3) = 1 + 3 = 4$$

$$\sigma(4) = 1 + 2 + 4 = 7$$

$\sigma(n)$  = Sum of pos. divisors of  $n$  (if  $n$  pos. int.)

$\sigma(mn) = \sigma(m)\sigma(n)$  whenever  $\gcd(m,n) = 1$

$$8 \cdot 7 - 32 \cdot 1 = 56 - 32 = 24$$

$\theta(q)^n$  are examples of modular functions. (not for the full modular group  $\Gamma$  but for certain of its subgroups)

A lattice  $L \subset \mathbb{R}^n$  is the set of  $\mathbb{Z}$ -linear combinations of a basis  $v_1, \dots, v_n$ .

$L$  is integral if  $x \cdot y \in \mathbb{Z}$  for all  $x, y \in L$ .

eg. in  $\mathbb{R}^8$ ,  $\mathbb{Z}^8 = \{(a_1, \dots, a_8) : a_i \in \mathbb{Z}\} \subset \mathbb{R}^8$  is integral

$E_8 = \{\frac{1}{2}(a_1, \dots, a_8) : a_i \in \mathbb{Z}, a_1 \equiv \dots \equiv a_8 \pmod{2}, \sum a_i \equiv 0 \pmod{4}\}$  is also integral.

Moreover both  $\mathbb{Z}^8$  and  $E_8$  are self-dual:

Given a lattice  $L \subset \mathbb{R}^n$ , the dual lattice  $L^* \subset \mathbb{R}^n$  is  $L^* = \{v \in \mathbb{R}^n : v \cdot L \in \mathbb{Z}\}$   
 $= \{v \in \mathbb{R}^n : v \cdot x \in \mathbb{Z} \text{ for all } x \in L\}$

$L$  an integral  $\Rightarrow L \subseteq L^*$   
 $L$  is self-dual iff  $L = L^*$

iff the  $v_1, \dots, v_n$  form the rows of an  $n \times n$  matrix of determinant  $\pm 1$ .

Assume  $L$  is an integral lattice. The theta series of  $L$  is  $(q = e^{\pi i \tau})$   
 $\Theta_L(\tau) = \sum_{v \in L} q^{v \cdot v} = \sum_{n=0}^{\infty} N_L(n) q^n$  where  $N_L(n)$  = number of vectors  $v \in L$  of norm  $n$ .

eg.  $\Theta_{\mathbb{Z}}(\tau) = 1 + 2q + 2q^4 + 2q^9 + \dots = \theta(\tau)$  (or use  $q$  as argument)

$\Theta_{\mathbb{Z}^8}(\tau) = \theta(\tau)^8 = 1 + 16q + 112q^2 + \dots$  16 vectors of norm 1:  $(\pm 1, 0, \dots, 0), \dots$

Vectors of norm 2:  $(\pm 1, \pm 1, 0, \dots, 0), \dots$

$\Theta_{E_8}(\tau) = 1 + 240q^2 + 2160q^4 + \dots$

All  $v \in E_8$  have even norm

$4 \binom{8}{2} = 4 \cdot \frac{8 \cdot 7}{2} = 112$  such vectors

$= 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^{2n}$

where  $\sigma_k(n)$  = sum of  $k^{\text{th}}$  powers of the positive integer divisors of  $n$ .

$\sigma_1(n) = \sigma(n)$

$\sigma_k(mn) = \sigma_k(m) \sigma_k(n)$

$\sigma_3(1) = 1^3 = 1$

$\sigma_3(2) = 1^3 + 2^3 = 9$ ,  $9 \cdot 240 = 2160$

when  $m, n$  rel. prime.

$E_8 = \left\{ \frac{1}{2}(a_1, \dots, a_8) : a_i \in \mathbb{Z}, a_1 \equiv \dots \equiv a_8 \pmod{2}, \sum a_i \equiv 0 \pmod{4} \right\}$  is also integral.

The shortest nonzero vectors in  $E_8$  are the 240 root vectors

$$\left. \begin{aligned} \frac{1}{2}(\pm 2, \pm 2, 0, \dots, 0) &= (\pm 1, \pm 1, 0, \dots, 0) && 112 \text{ such} \\ \frac{1}{2}(\pm 1, \pm 1, \pm 1, \dots, \pm 1) & \text{ (even numbers of } +1 \text{'s), } && 128 \text{ such} \end{aligned} \right\} 240 \text{ root vectors}$$

If  $L$  is any integral lattice then  $\Theta_L$  and  $\Theta_{L^*}$  are related by the Jacobi theta-function identity

$$\Theta_{L^*}(\tau) = \sqrt{|\text{disc } L|} \left(\frac{i}{\tau}\right)^{n/2} \Theta_L\left(-\frac{1}{\tau}\right)$$

For self-dual (integral) lattices in  $\mathbb{R}^8$  ( $n=8$ ),  $\Theta_L(\tau) = \frac{1}{\tau^4} \Theta_L\left(-\frac{1}{\tau}\right)$

i.e.  $\Theta_L(\tau)$  is a modular form of weight 4 for the subgroup of index 3 in  $\Gamma = \text{PSL}_2(\mathbb{Z})$  namely the subgroup  $G(2) = \left\{ z \mapsto \frac{az+b}{cz+d} : a, b, c, d \in \mathbb{Z}, ad-bc=1, \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ is } \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ or } \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$

$$[\Gamma : G(2)] = 3.$$

$$\tau \mapsto -\frac{1}{\tau} \text{ is in } G(2)$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}(\tau) = \frac{0\tau+1}{-\tau+0}$$

$G(2)$  is generated by  $\tau \mapsto -\frac{1}{\tau}$  and  $\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}(\tau) = \frac{\tau+2}{0\tau+1} = \tau+2$

$\tau \mapsto \tau+2$  which satisfies  $\Theta_L(\tau+2) = \Theta_L(\tau)$

More generally, a modular form of weight  $k$  for a subgroup  $G \leq \Gamma = \text{PSL}_2(\mathbb{Z})$  is a  $\mathbb{C}$ -valued function  $f(z)$  defined and holomorphic (complex analytic) in the upper half-plane  $\{z \in \mathbb{C} : \text{Im } z > 0\}$  such that

(i)  $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$  for every  $z \mapsto \frac{az+b}{cz+d}$  in  $G$ ; and

(ii) the Laurent expansion of  $f(z)$  in  $q = e^{2\pi iz}$  has no negative powers of  $q$  i.e.  $f(\tau) = \sum_{n=0}^{\infty} a_n q^n$ .

Restricting to a subgroup  $G \leq \Gamma$  of (small) finite index, the set of modular forms of weight  $k$  for  $G$  is a finite dimensional vector space over  $\mathbb{C}$ . The dimension for certain  $G, k$  have been computed ( Ogg et al). Eg. for the group  $G = G(2) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1, a \equiv d \pmod{2}, b \equiv c \pmod{2} \right\}$ ,  $[\Gamma : G] = 3$ , modular forms of weight 4 for  $G$  satisfy

$$f(z+2) = f(z), \quad f\left(-\frac{1}{z}\right) = z^4 f(z)$$

(2 is a period)

and the modular forms form a 2-dimensional vector space. Two examples of modular forms are known:

$$\left. \begin{aligned} \Theta_{\mathbb{Z}}(\tau) &= 1 + 240q^2 + 2160q^4 + \dots \\ \Theta_{\mathbb{Z}^2}(\tau) &= 1 + 16q + 112q^2 + \dots \end{aligned} \right\} \text{basis}$$

We also know that  $g_2(\tau) = 60 \sum_{(m,n) \in \mathbb{Z}^2, (m,n) \neq (0,0)} \frac{1}{(m+n\tau)^2}$  is a modular form for  $G$ .

$$g_2(\tau+2) = 60 \sum_{m,n} \frac{1}{(m+n(\tau+2))^2} = 60 \sum_{m,n} \frac{1}{(m+n\tau)^2} = g_2(\tau) \text{ by change of dummy variable.}$$

$$g_2\left(-\frac{1}{\tau}\right) = 60 \sum_{m,n} \frac{1}{(m - \frac{n}{\tau})^2} = 60 \sum_{m,n} \frac{\tau^2}{(\tau m - n)^2} = \tau^4 g_2(\tau)$$

← not quite

Actually the Laurent expansion  $g_2(z) = \underbrace{2\zeta(4)}_{\text{not quite}} \left[ 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^{2n} \right]$  is not hard to prove

$$\zeta(2) = \frac{\pi^2}{6}, \quad \zeta(4) = \frac{\pi^4}{90}, \quad \zeta(2k) = \frac{(-1)^{k+1} (2\pi)^{2k} B_{2k}}{2(2k)!} \leftarrow \text{Bernoulli numbers}$$

$\frac{1}{(4\pi)^2} g_2(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^{2n}$  is a  $\mathbb{C}$ -linear combination of  $\Theta_{\mathbb{Z}}(\tau)$  and  $\Theta_{\mathbb{Z}^2}(\tau)$ . Solve 2 eqns in 2 unknowns to get

$$\Theta_{\mathbb{Z}}(\tau) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^{2n} \quad \text{Can we prove this without using any analysis? Probably but... try!}$$

Can you find two lattices  $L, L' \subset \mathbb{R}^n$  with the same theta series?

Theta series  $\Theta_L$  are invariants: if  $\Theta_L(\tau) \neq \Theta_{L'}(\tau)$  then  $L, L'$  cannot be isometric. What about the converse? The converse fails in general.

First known example ( $n=16$ ): There are two lattices  $E_8 \oplus E_8$  and  $D_{16}$  in  $\mathbb{R}^{16}$  which are not isometric but they have the same theta-series

$$1 + 180 \sum_{n=1}^{\infty} \sigma_7(n) q^{2n} \quad \sigma_7(n) = \sum d^7 \quad (\text{sum over positive integers } d|n).$$

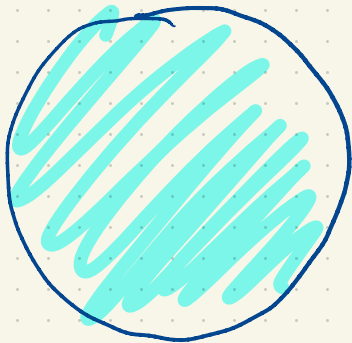
This appears in J.P. Serre, A Course in Arithmetic and in a very short paper J. Milnor, (1964)

"Can you hear the shape of a drum?" (question by Mark Kac)

$$\Delta = \sum_{i=1}^2 \frac{\partial^2}{\partial x_i^2}$$

Spectrum of a domain  $\Omega \subset \mathbb{R}^2$  is the set of eigenvalues of  $\Delta$

$$\Delta f = \lambda f \\ f|_{\partial\Omega} = 0 \quad (\text{Dirichlet boundary conditions})$$



$\mathbb{R}^n / L$

$L \subset \mathbb{R}^n$  lattice

The eigenvalues of the Laplacian for the  $n$ -dimensional torus  $\mathbb{R}^n / L$  can be immediately read off from the theta series of the lattice  $L$ .



Another similar construction: Given  $p \equiv 1 \pmod{4}$  prime, list all vectors  $x = (x_1, \dots, x_6) \in \mathbb{Z}^6$  satisfying

- $x_1^2 + \dots + x_6^2 = p$
- $x_1 \equiv x_2 \equiv x_3 \equiv x_4 \equiv x_5 \equiv x_6 \pmod{2}$

We only care about pairs of vectors  $\pm x$

$$p=5: \begin{array}{l} \pm (0|1, \pm 1^4) \\ \pm (1|\pm 2, 0^4) \end{array} \quad \begin{array}{l} (16 \text{ such}) \\ (10 \text{ such}) \end{array} \quad \begin{array}{l} \text{i.e. } 16 \text{ pairs } \pm x \\ \text{i.e. } 10 \text{ pairs } \pm x \end{array}$$


---

26 pairs

$$p=13: \begin{array}{l} \pm (0|3, \pm 1^4) \\ \pm (1|\pm 2^3, 0^2) \\ \pm (3|\pm 2, 0^4) \end{array} \quad \begin{array}{l} 5 \times 16 = 80 \text{ such} \\ \binom{5}{2} \times 2^3 = 80 \text{ such} \\ 5 \times 2 = 10 \text{ such} \end{array}$$


---

170 such

In general there are  $p^2+1$  solutions.

The proof in each case relies on modular forms. We can prove the formula using

$$\Theta_{\mathbb{E}^8}(\tau) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^{2n}. \quad \text{The connection uses geometry in } \mathbb{F}_p/\mathbb{F}_p, \text{ an 8-dimensional vector space over } \mathbb{F}_p. \text{ An ovoid is a set of } p^2+1 \text{ points } x_i \text{ (} i=1, 2, \dots, p^2+1 \text{) such that } x_i \cdot x_i = 0; \quad x_i \cdot x_j \neq 0 \text{ for } i \neq j. \quad \sigma_3(p) = 1 + p^3 = p^2 + 1.$$

Why do we care about ovoids? Every ovoid in  $\mathbb{F}_p^8$  gives rise to "many" ovoids in  $\mathbb{F}_p^6$  by "slicing". An ovoid in  $\mathbb{F}_p^6$  has  $p^2+1$  points. These give projective planes of order  $p^2$ .

$p^2+p^2+1$  points / lines  
 Every pt on  $p^2+1$  lines  
 " line has  $p^2+1$  pts



"Most" of the known finite planes arise from this construction. This is a heuristic argument only.  
 explicitly constructed.

Original construction of ovoids in  $\mathbb{F}_p^3$  from  $E_8$  is due to Conway, Kleidman, Wilson (1988?)

Conway conjectured that  $\lim_{n \rightarrow \infty} \frac{\text{no. of known planes of order } \leq n \text{ arising from } E_8\text{-type ovoids}}{\text{m. of known planes of order } \leq n} = 1$

M. (1991) generalized Conway's construction giving many more ovoids from  $E_8$ .

Used  $\textcircled{1} j(\tau) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^{2n}$  and  $\textcircled{2} \sum_{E_8 \oplus E_8} (r) = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^{2n}$

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

$$j\left(\frac{1 + \sqrt{-163}}{2}\right) = -640320^3 = -262537412640768000$$

$$q = e^{\pi i \tau}$$

gives rise  $e^{\pi \sqrt{-163}} \approx 640320^3 + 744 + 0.999999999999250\dots$

$\mathbb{Q}[\sqrt{-163}]$  has unique factorization

(Today) Monday: applications of modular forms to elliptic curves

Eg.  $E: y^2 + y = x^3 - x$  is not in Weierstrass normal form  $y^2 = x^3 + ax + b$ .

In char  $\neq 2, 3$ , the equation of a nonsingular <sup>plane</sup> cubic can always be put in Weierstrass normal form.

$E(\mathbb{F}_p)$  is nonsingular for  $p \neq 37$ . The discriminant of  $y^2 = x^3 + ax + b$  is

$$\Delta = 4a^3 + 27b^2$$

$$\left(y + \frac{1}{2}\right)^2 = y^2 + y + \frac{1}{4} = x^3 - x + \frac{1}{4}$$

$$\Delta = 4(-1)^3 + 27\left(\frac{1}{4}\right)^2 = -4 + \frac{27}{16} = \frac{-37}{16}$$

$|E(\mathbb{F}_p)| = p+1 - a_p$ ,  $|a_p| \leq 2\sqrt{p}$  by Hasse-Weil for  $p \neq 37$ .

The values  $a_n$  ( $n \in \mathbb{N}$ ) are defined as the coefficients of a modular form

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

$q = e^{2\pi i \tau}$   
(Power series in  $q$ ;  
Fourier series in  $\tau$ )

$$= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} + 4q^{14} - q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + 2q^{20} + 2q^{21} - 2q^{22} - q^{23} - 4q^{25} - 8q^{26} + 5q^{27} - 4q^{28} + \dots$$

eg.  $|E(\mathbb{F}_{13})| = 13+1 - a_{13} = 14 - 4 = 10$

$a_{mn} = a_m a_n$  whenever  $\gcd(m, n) = 1$ .

$a_{26} = a_2 a_{13} = (-2)(4) = -8$


$a_{28} = a_4 a_7 = 2(-2) = -4$

$f(\tau)$  is a modular form of weight 2 for the subgroup  $\Gamma_0(11) < SL_2(\mathbb{Z})$  of finite index 12

$$\Gamma_0(11) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \pmod{11} \right\}$$

$$\begin{array}{ccc} SL_2(\mathbb{Z}) & \twoheadrightarrow & SL_2(\mathbb{11}) \\ \downarrow & & \downarrow \\ \Gamma_0(11) & \twoheadrightarrow & \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \end{array}$$

$SL_2(\mathbb{11})$  permutes the 12 1-dimensional subspaces of  $\mathbb{F}_{11}^2 = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} : x, y \in \mathbb{F}_{11} \right\}$   
 $\langle \begin{bmatrix} 1 \\ 0 \end{bmatrix} \rangle, \langle \begin{bmatrix} 1 \\ 1 \end{bmatrix} \rangle, \dots, \langle \begin{bmatrix} 1 \\ 10 \end{bmatrix} \rangle, \langle \begin{bmatrix} 0 \\ 1 \end{bmatrix} \rangle$

$$\frac{11^2 - 1}{11 - 1} = 11 + 1 = 12$$


A similar fact holds for any rational elliptic curve

Taniyama-Shimura-Weil Conjecture: every rational elliptic curve is modular  
Andrew Wiles had great interest in this conjecture but ... very hard!

Gerd Faltings observed a connection in 1985 between Taniyama-Shimura-Weil Conjecture and Fermat's Last Theorem.  
Serre & Ribet made this connection explicit.

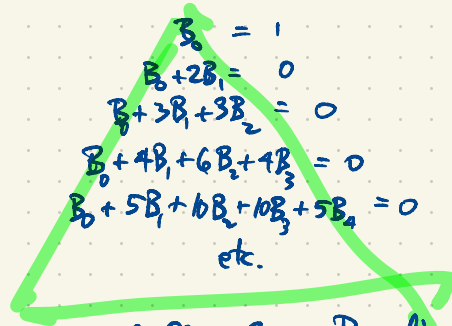
# Bernoulli Numbers (Jakob I Bernoulli, 1655-1705)

$$\frac{x}{e^x - 1} = 1 - \frac{x}{2} + \frac{x^2}{12} - \frac{x^4}{720} + \frac{x^6}{30240} - \frac{x^8}{1209600} + \frac{x^{10}}{47900160} - \frac{691x^{12}}{1387474368000} + \frac{x^{14}}{74724249600} - \frac{3617x^{16}}{10670622842880000} - \frac{43867x^{18}}{51909427170944000} + \dots$$

exponential generating function of  $B_n = n^{\text{th}}$  Bernoulli number

- $B_0 = 1$
- $B_1 = -\frac{1}{2}$
- $B_2 = \frac{1}{6}$
- $B_3 = B_5 = B_7 = \dots = 0$
- $B_4 = -\frac{1}{30}$
- $B_6 = \frac{1}{42}$
- $B_8 = -\frac{1}{30}$
- $B_{10} = \frac{5}{66}$

- $B_{12} = \frac{691}{2730}$
- $B_{14} = \frac{7}{6}$
- $B_{16} = -\frac{3617}{510}$
- $B_{18} = \frac{43867}{798}$
- $B_{20} = \dots$
- $B_{50} = \frac{495 \dots 25}{66}$



Coeffs. from Pascal's triangle.

(convergent for  $|x| < 2\pi$ )

Easy to explain:  $\frac{1}{e^x - 1} + \frac{1}{2} = \frac{(e^x - 1) + 2}{2(e^x - 1)} = \frac{e^x + 1}{2(e^x - 1)} = \frac{1}{2} \cdot \frac{e^{x/2} - e^{-x/2}}{e^{x/2} + e^{-x/2}}$

$\frac{x}{e^x - 1} + \frac{x}{2}$  is an even function

$\zeta(2k) = \frac{|B_{2k}| (2\pi)^{2k}}{2(2k)!}$  which generalizes  $\zeta(2) = \frac{\pi^2}{6}$

cot  $x = \sum_{n=0}^{\infty} (-1)^n \frac{2B_{2n} (2x)^{2n-1}}{(2n)!}$

coth  $x = \sum_{n=0}^{\infty} \frac{2B_{2n} (2x)^{2n-1}}{(2n)!}$

An odd prime  $p$  is regular if it does not divide the numerator of  $B_2, B_4, \dots, B_{p-3}$ .  
 The smallest irregular prime is 37 which divides the numerator of  $B_{32}$ .

$$B_{32} = \frac{-7909321041217}{510} = -\frac{208360028141}{510} \cdot 37$$

A cyclotomic field is an extension  $\mathbb{Q}[\zeta_n] \supseteq \mathbb{Q}$  where  $\zeta_n = e^{2\pi i/n}$  (primitive  $n^{\text{th}}$  root of unity).  
 (Galois extension of degree  $\phi(n)$ ).  
 $\uparrow$  Alg. int. in  $\mathbb{Q}[\zeta_n]$  are just  $\mathbb{Z}[\zeta_n]$   $\zeta = \zeta_n$

If  $x^n + y^n = z^n$  ( $x, y, z \in \mathbb{Z}$ ) then  $(x+y)(x+\zeta y)(x+\zeta^2 y) \dots (x+\zeta^{n-1} y) = z^n$ .

Restrict to  $n=p$  prime. We can make the naive approach work in certain cases whenever the class number of the extension  $\mathbb{Q}[\zeta_p] \supset \mathbb{Q}$  is not divisible by  $p$  (so if an ideal

$A \subset \mathbb{Z}[\zeta]$  has  $A^p = (1) = \mathbb{Z}[\zeta]$  then  $A = (1) = \mathbb{Z}[\zeta]$  i.e. ideal class group  
 $\{\text{all ideals}\} / \{\text{principal ideals}\}$  has no elements of order  $p$ .

For  $\mathbb{Q}[\zeta_p] \supset \mathbb{Q}$ , this happens iff  $p$  is a regular prime.