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, red) is located at the center of the pattern, from which the circles appear to radiate.

Number Theory

Book 3

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

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 ^{log}protocol for key distribution: This allows two parties to agree on a secret key (typically, ^{long} 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 $g_2(\tau) = 60 \sum_{(m,n) \neq (0,0) \in \mathbb{Z}^2} \frac{1}{(m+n\tau)^4}$

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

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

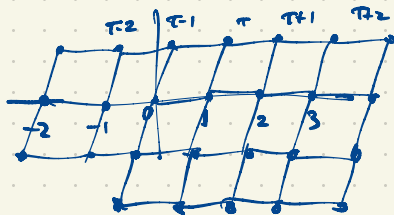
$$j(\tau) = \frac{1728 \frac{g_2(\tau)^3}{g_2(\tau)^3 - 27g_3(\tau)^2}}{1728} = \frac{1728 g_2(\tau)^3}{(2\pi)^{12} \eta(\tau)^{24}}$$

$1728 = 12^3$

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

$g_2(\tau)$, $g_3(\tau)$ 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 αL 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 τ 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 $\mathbb{C}/\langle 1, \tau \rangle$

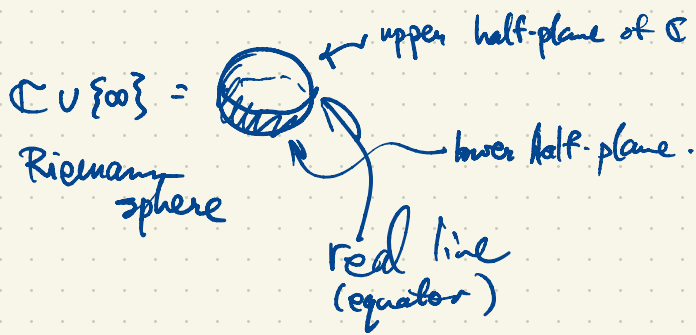
Also $\langle 1, \tau^{-1} \rangle$ gives essentially the same curve
 \downarrow scale by τ
 $\langle \tau, 1 \rangle$

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



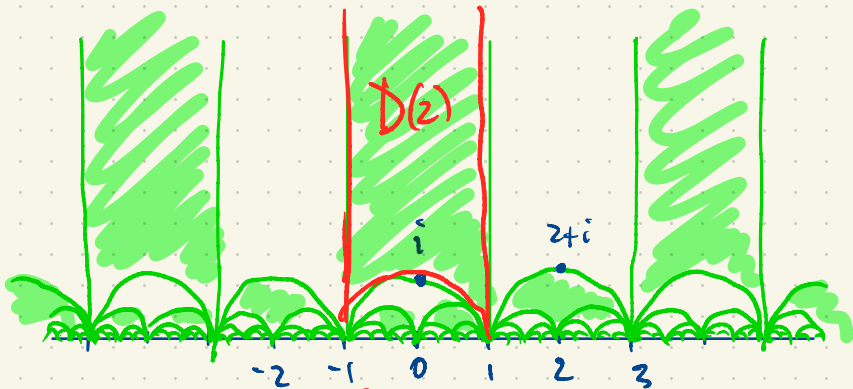
$SL_2(\mathbb{Z})$ maps $\mathbb{R} \cup \{\infty\} \rightarrow \mathbb{R} \cup \{\infty\}$ (equator)
 upper half-plane \rightarrow upper half-plane
 lower $\dots \rightarrow$ lower half-plane

$PSL_2(\mathbb{Z})$ 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}



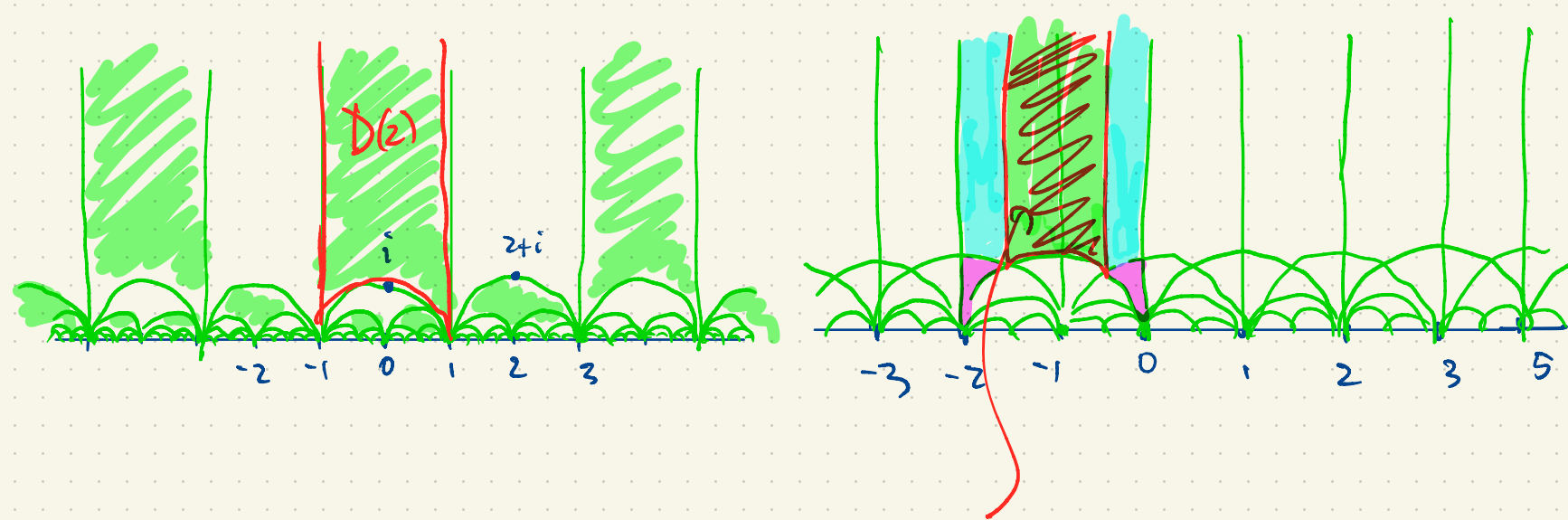
$\mathcal{D}(2)$ is a fund.

domain for

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

by $\tau \mapsto \tau+2$, $\tau \mapsto -\frac{1}{\tau}$
 $\begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix} \in \tilde{\Gamma}(2)$, $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in \Gamma(2)$

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



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

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

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

$a \equiv d \equiv 1 \pmod{p}$
 $c \equiv d \equiv 0 \pmod{p}$

(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 Γ).

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 Γ 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 ± 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^{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.

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

The shortest nonzero vectors in E_8 are the 240 root vectors

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

If L is any integral lattice then Θ_L and Θ_{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 Θ_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,

"Can you hear the shape of a drum?"