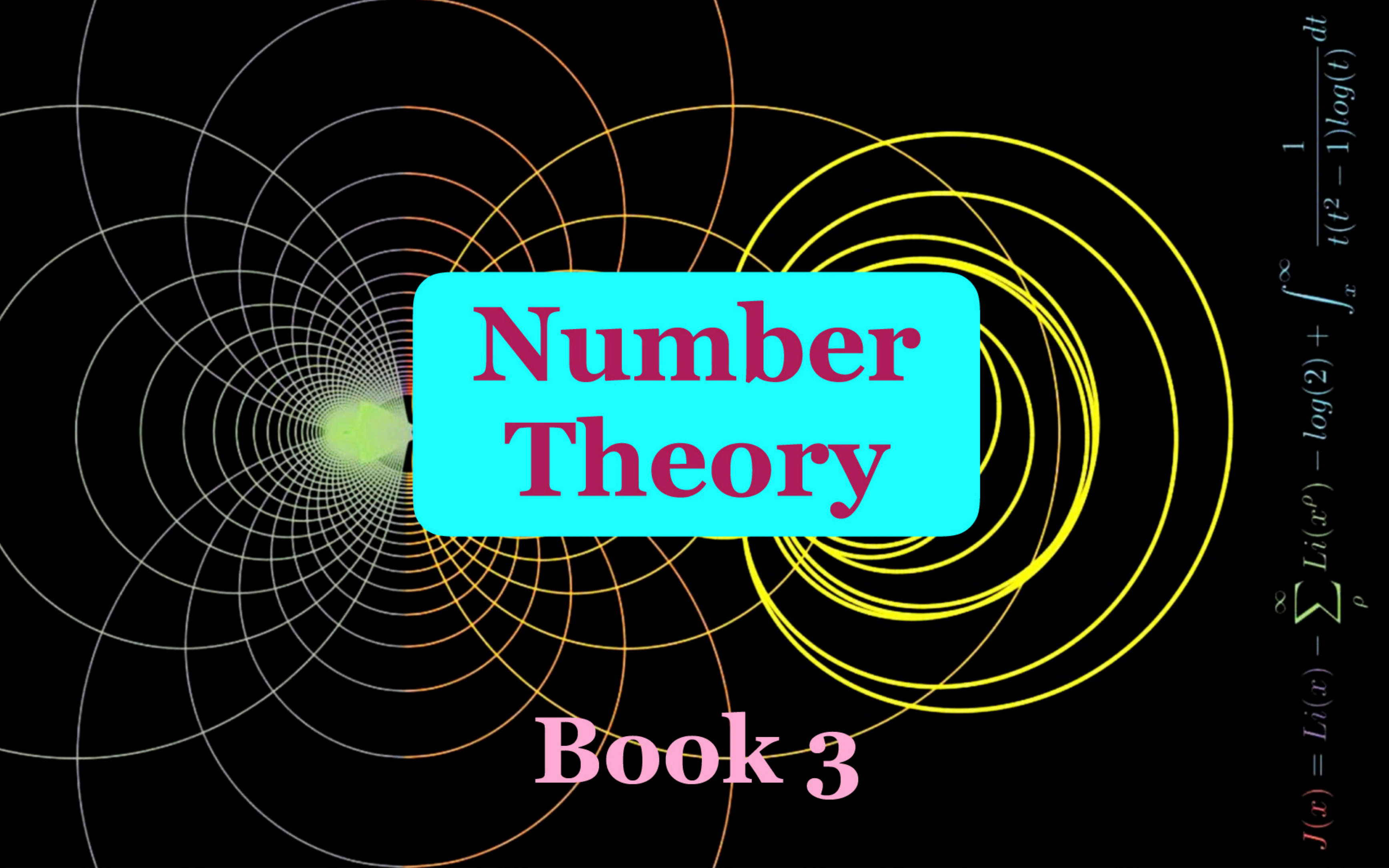

Number Theory
Book 3
$J(x) = Li(x) - \sum_{\rho}^{\infty} Li(x^{\rho}) - log(2) + \int_{x}^{\infty} \frac{1}{t(t^2-1)log(t)} dt$

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 $n \mid m$ 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 $g \geq 2$: $\underbrace{X(\mathbb{Q})}_{\text{set of rational points}}$ 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 curve with finitely many rational points.
For $n \geq 4$, $g>1$.) 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 $a^{n-1} \bmod n$.

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

If $a^{n-1} \equiv 1 \bmod n$, 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 $n =$ 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 $\frac{1}{b} = r$ in F. The computation proceeds.

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

$\underbrace{E(\mathbb{Z}/n\mathbb{Z})} \xrightarrow[\text{almost-homo}]{} E(\mathbb{Z}/q\mathbb{Z})$ meaning: if $P, Q \in E(\mathbb{Z}/n\mathbb{Z})$ where $P+Q \in E(\mathbb{Z}/n\mathbb{Z})$ is well-defined

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

$E(\mathbb{Z}/q\mathbb{Z})$: actual elliptic curve

then $\overline{P} + \overline{Q} = \overline{P+Q}$ where "bar" is "mod q".

<u>Example</u> Show $n = 10^{10}+19 = 10000000019$ is prime. Proof by contradiction.
Supposing n is composite, n has a prime factor $p \le \sqrt{n}$ 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 $\underbrace{4a^3 + 27b^2}_{\text{discriminant of } x^3+ax+b} \not\equiv 0 \bmod n$

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

E	$\lvert E(\mathbb{Z}/n\mathbb{Z})\rvert$
$y^2 = x^3 + x - 5$	$9999935488 = 2^3 \cdot 3 \cdot 19 \cdot 4761 \cdot 7649$
$y^2 = x^3 + 2x - 8$	$10000162104 = 2^3 \cdot 3 \cdot 29 \cdot 547 \cdot 26267$
$y^2 = x^3 + 3x - 11$	$10000053492 = 2^2 \cdot 3 \cdot 11 \cdot 13 \cdot 37 \cdot 239 \cdot 659$
$y^2 = x^3 + 4x - 14$	$9999842527 = \underbrace{3 \cdot 19 \cdot 89}_{k} \cdot \underbrace{1971199}_{q} = m$

To prove that n is prime, we argue by contradiction. If not there is a prime $p \le \sqrt{n}$, $p \mid n$.
So $p < 100{,}000$. Then there is an almost-homomorphism $E(\mathbb{Z}/n\mathbb{Z}) \to E(\mathbb{F}_p)$

$E(\mathbb{Z}/n\mathbb{Z})$: "elliptic curve" over $\mathbb{Z}/n\mathbb{Z}$

$E(\mathbb{F}_p)$: actual elliptic curve over $\mathbb{F}_p$.

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

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

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

We have presumably checked recursively that q is prime.

$E(\mathbb{F}_p)$ 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 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 mod p i.e. all nonzero elements of $\mathbb{F}_p$ are powers of g. (Eg. if $p = 1009$, $g = 11$ is primitive. In $\mathbb{F}_{1009}$

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

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

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

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 $a \in \{1, 2, \cdots, p-2\}$ at random. She computes $g^a \in \mathbb{F}_p$ and sends this to Bob (over the open channel).
Bob (secretly) chooses $b \in \{1, 2, \cdots, p-2\}$ 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 $\mathbb{F}_q^\times = \{a \in \mathbb{F}_q : a \neq 0\}$

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

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

Fix curve, P point.

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

Bob - - - - - - b, computes bP, - - - - 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 $$g_2(\tau) = 60 \sum_{(0,0) \neq (m,n) \in \mathbb{Z}^2} \frac{1}{(m+n\tau)^4}$$

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

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

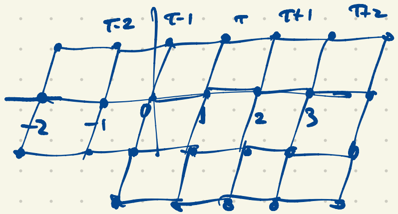
$$j(\tau) = 1728 \frac{g_2(\tau)^3}{g_2(\tau)^3 - 27 g_3(\tau)^2} = \frac{1728\, g_2(\tau)^3}{(2\pi)^{12}\, \eta(\tau)^{24}}$$

$12^3 = 1728$

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

$g_2(\tau)$, $g_3(\tau)$ 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) $M = FG$ can be written as a subgroup (isomorphic to) of $GL_{196883}(\mathbb{C})$

Monstrous Moonshine

$\mathbb{C} / \{m + n\tau : m, n \in \mathbb{Z}\} \cong$ 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.