

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

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

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,

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

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 $P(3, 5)$.

$$y^2 = x^3 + x - 5$$

To check that this is an elliptic curve, need $4a^3 + 27b^2 \not\equiv 0 \pmod{n}$
discriminant of $x^3 + ax + b$

Corrected!

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