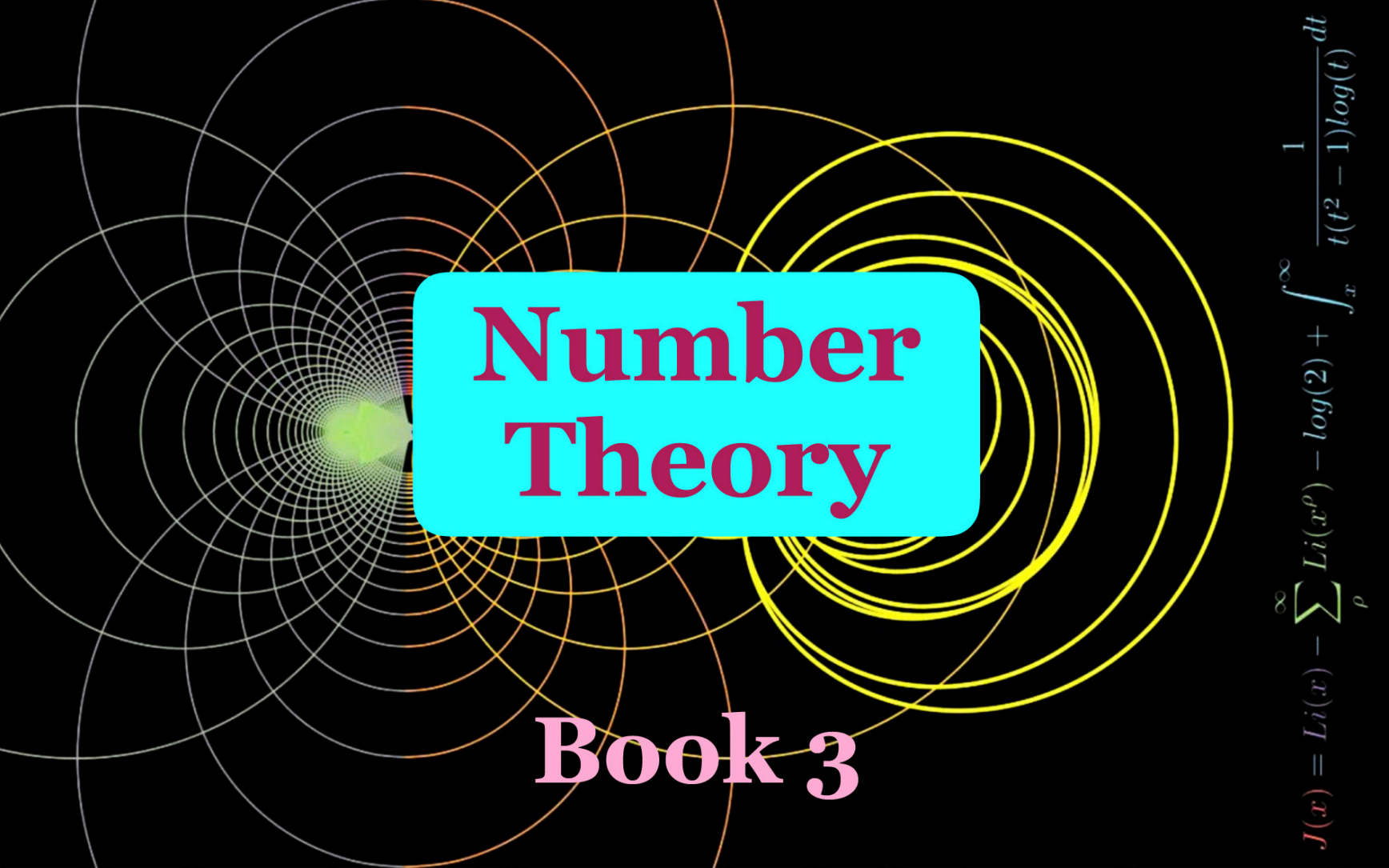
Number
Theory
Book 3
$J(x) = Li(x) - \sum_{\rho}^{\infty} Li(x^{\rho}) - log(2) + \int_{x}^{\infty} \frac{1}{t(t^2-1)log(t)} dt$

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

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 $c \cdot (\log n)^b$.
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 if 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.