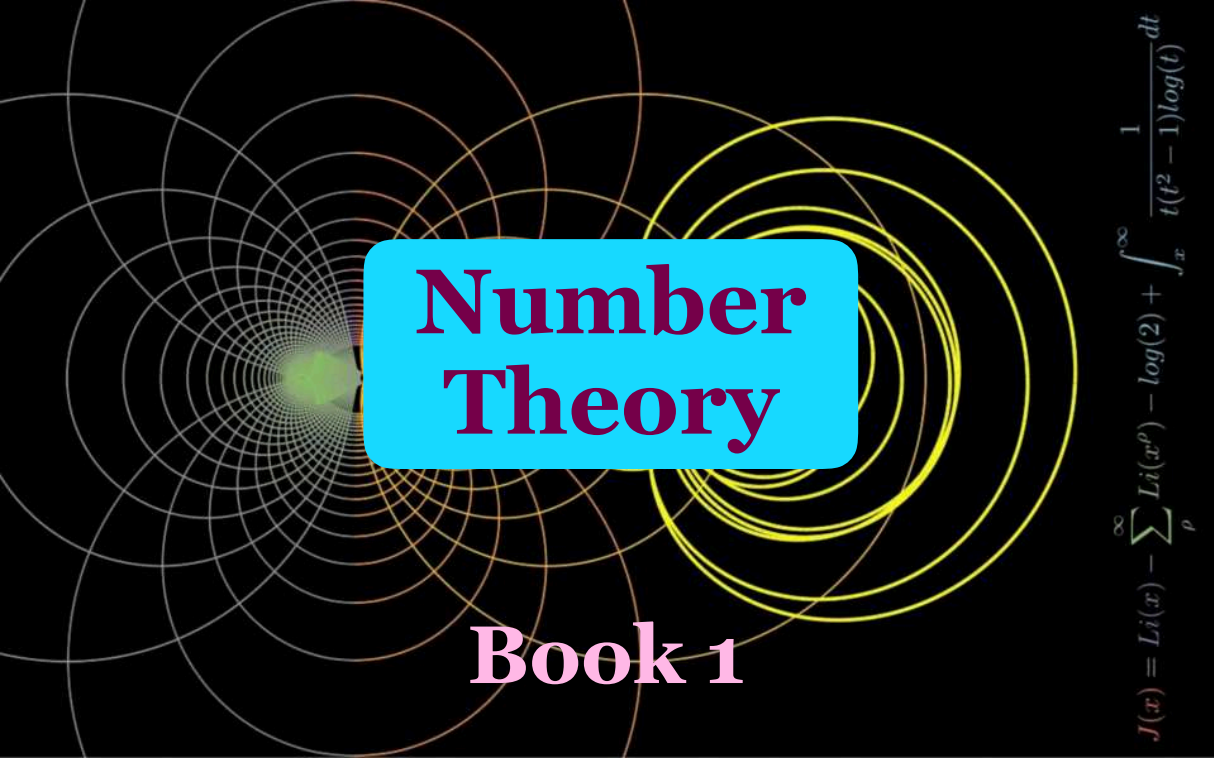
Number
Theory
Book 1
$J(x) = Li(x) - \sum_{\rho}^{\infty} Li(x^{\rho}) - log(2) + \int_{x}^{\infty} \frac{1}{t(t^2-1)log(t)} dt$

Rational integers ("ordinary integers") $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$

(Algebraic) integers: A number $\alpha \in \mathbb{C}$ is <u>algebraic</u> if it is a root of a nonzero poly. with coefficients in $\mathbb{Q}$

i.e. $f(\alpha) = 0$ for some $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $a_i \in \mathbb{Q}$ i.e. $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $a_i \in \mathbb{Z}$ not all zero.

eg. $\frac{\sqrt{2}}{7}$ is algebraic since it's a root of $x^2 - \frac{2}{49} \in \mathbb{Q}[x]$ or $49x^2 - 2 \in \mathbb{Z}[x]$.

We say α is an (<u>algebraic</u>) <u>integer</u> if α is a root of a <u>monic</u> poly. with coefficients in $\mathbb{Z}$ ie.

$f(\alpha) = 0$ for some $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $a_i \in \mathbb{Z}$.

eg. $\sqrt{2}$ is integral (it's an (algebraic) integer)

If $\mathcal{O} = \{\alpha \in \mathbb{C} : \alpha \text{ is an algebraic integer}\} \subset \mathcal{A} \subset \mathbb{C}$

$\mathcal{A} = \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic}\} \subset \mathbb{C}$

$\mathcal{O}$ is the <u>ring</u> of alg. int.

$\mathcal{A}$ is the <u>field</u> of alg. numbers.

$\mathcal{O} \cap \mathbb{Q} = \mathbb{Z}$ (the rational integers are the ordinary integers).

x	y
± 1	0
± 9	± 4
± 161	± 72
± 2889	± 1292
$\vdots$	$\vdots$

Pell's equation: $x^2 - 5y^2 = 1$ has infinitely many (ordinary) integer solutions.

$x^2 - 5y^2 = 1 \iff (x + y\sqrt{5})(x - y\sqrt{5}) = 1$ where $x + y\sqrt{5} \in \mathcal{O}$ has Norm is $N(x + y\sqrt{5}) = (x + y\sqrt{5})(x - y\sqrt{5}) = x^2 - 5y^2$

$N(\alpha\beta) = N(\alpha)N(\beta)$ so if $\alpha = 9 + 4\sqrt{5}$ then $N(\alpha) = 9^2 - 5 \cdot 4^2 = 1$ so $N(\alpha^k) = N(\alpha)^k = 1^k = 1$

eg. $(9 + 4\sqrt{5})^2 = 81 + 80 + 72\sqrt{5} = 161 + 72\sqrt{5}$ also has norm 1 so $161^2 - 5 \cdot 72^2 = 1$

$(9 + 4\sqrt{5})^3 = (161 + 72\sqrt{5})(9 + 4\sqrt{5}) = 2889 + 1292\sqrt{5}$

$\mathcal{A}$ is the fraction field of $\mathcal{O}$ ie. $\mathcal{A} = \{\frac{\alpha}{\beta} : \alpha, \beta \in \mathcal{O}, \beta \neq 0\}$

$\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$.

eg. $\sqrt{2}, \sqrt{3} \in \mathcal{O}$ (root of $x^2 - 2$, $x^2 - 3$ espectively)

$\Rightarrow \sqrt{2} \cdot \sqrt{3} = \sqrt{6} \in \mathcal{O}$ (root of $x^2 - 6$)

$\sqrt{2} + \sqrt{3} \in \mathcal{O}$ (root of $x^4 - 10x^2 + 1$)

the min. poly. of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.

$x = \sqrt{2} + \sqrt{3}$

$x^2 = 5 + 2\sqrt{6}$

$x^2 - 5 = 2\sqrt{6}$

$x^4 - 10x^2 + 25 = 24$

$x^4 - 10x^2 + 1 = 0$

Let $\alpha \in \mathbb{C}$. If α is algebraic then it has a minimal ~~poly~~. over $\mathbb{Q}$ i.e. $m(x) \in \mathbb{Q}[x]$ is monic with $m(\alpha) = 0$ and $\deg m(x)$ is as small as possible. In this case $m(x)$ is unique. All polynomials in $\mathbb{Q}[x]$ having α as a root are multiples of $m(x)$.

$$(m(x)) = \{ h(x) m(x) : h(x) \in \mathbb{Q}[x] \}$$