The background features a complex pattern of overlapping circles in various colors (white, orange, yellow) that create a sense of depth and movement. A bright, glowing green and yellow point is located at the center of the pattern, from which the circles appear to radiate.

Number Theory

Book 2

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

If R is any ring with identity then $R^* = \{\text{units in } R\} = \{\text{invertible elements in } R\} = \{u \in R : \text{the units in the ring of } n \times n \text{ matrices over } R \text{ form a mult. gp. } GL_n(R)\}$.
 The units R^* the unit group of R .

$uv = vu = 1$ for some $v \in R$

If R is a commutative ring with identity then R^* is abelian.

Take $\mathcal{O} = \{\text{alg. integers in } K\}$ $K \supseteq \mathbb{Q}$ finite extension. We want to describe $\mathcal{O}^* = \text{unit group of the extension, an abelian multiplicative group.}$

eg. $\mathbb{Z}^* = \{\pm 1\}$. $|\mathcal{O}^*| \geq 2$ since $\pm 1 \in \mathcal{O}^*$.
 In a real quadratic field, $\mathcal{O}^* = \underbrace{\{\pm 1\}}_{\text{torsion part: the elements of finite order in } \mathcal{O} \text{ (roots of unity in } \mathcal{O})} \times \underbrace{\langle \alpha \rangle}_{\text{infinite cyclic group with generator } \alpha}$

eg. $K = \mathbb{Q}[\sqrt{2}]$, $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$,
 $\mathcal{O}^* = \{\pm (1+\sqrt{2})^k : k \in \mathbb{Z}\}$

$\alpha = 1+\sqrt{2}$ is a generator of the "infinite" part of \mathcal{O}^* \uparrow fundamental unit.

Note: $\alpha^{-1} = -1+\sqrt{2}$

$\mathcal{O}^* = \{\pm 1, \pm 1 \pm \sqrt{2}, \pm 3 \pm 2\sqrt{2}, \dots\}$ Solutions of $x^2 - 2y^2 = \pm 1$, are $\{(\pm 1, 0), (\pm 1, \pm 1), (\pm 3, \pm 2), \dots\}$.
 $\langle \alpha \rangle = \langle 1+\sqrt{2} \rangle = \text{positive elements in } \mathcal{O}^*$

$\mathcal{O}^* = \{\text{units}\} = \{\text{solutions of Pell's equation } x^2 - dy^2 = \pm 1\}$

$\{\pm 1\} \times \langle -1-\sqrt{2} \rangle = \{\pm 1\} \times \langle 1+\sqrt{2} \rangle = \mathcal{O}^*$
 (Note: $\langle -1-\sqrt{2} \rangle$ is not canonical)

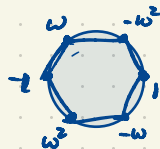
Imaginary quadratic fields $K = \mathbb{Q}[\sqrt{d}]$, $d < 0$

\mathcal{O}^* is finite since the equation $x^2 - dy^2 = \pm 1$ has only finitely many solutions

If $K = \mathbb{Q}[\sqrt{5}]$ then $\mathcal{O} = \mathbb{Z}[\sqrt{5}]$, $\mathcal{O}^* = \{\pm 1\}$.

... $\mathbb{Q}[\sqrt{3}]$ $\mathcal{O} = \mathbb{Z}[\omega]$, $\omega = \frac{-1+\sqrt{3}}{2}$ $\mathcal{O}^* = \{\pm 1, \pm \omega, \pm \omega^2\}$
 $\mathbb{Q}[\sqrt{-1}] = \mathbb{Q}[i]$ $\mathcal{O} = \mathbb{Z}[i]$ $\mathcal{O}^* = \{\pm 1, \pm i\}$
 Sixth roots of unity

$\omega^2 = \bar{\omega} = \frac{-1-\sqrt{3}}{2}$



Dirichlet's Unit Theorem If \mathcal{O} is the ring of integers in a number field $K \supseteq \mathbb{Q}$ ($[K:\mathbb{Q}] < \infty$)

then $\mathcal{O}^\times = \{ \text{roots of unity in } \mathcal{O} \} \times \text{free abelian group of rank } r_1 + r_2 - 1$

(torsion part of \mathcal{O}^\times)
finite cyclic group of even order

$$\cong \mathbb{Z}^{r_1 + r_2 - 1} = \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{r_1 + r_2 - 1}$$

written additively,
 $r_1 + r_2 - 1 = \text{number of generators.}$

Every number field K can be embedded $K \hookrightarrow \mathbb{C}$ (one-to-one homomorphism of rings) in $n = [K:\mathbb{Q}]$ distinct ways. r_1 of these embeddings have their image $\subset \mathbb{R}$; the other $2r_2$ such embeddings non-real. K has r_1 real and $2r_2$ non-real embeddings.

What are r_1, r_2 ?

$K \supseteq \mathbb{Q}$ is a number field. $K = \mathbb{Q}[x]$ for some $\alpha \in K$. (Not canonical.)

$$\cong \mathbb{Q}[x] / (m(x))$$

$m(x) \in \mathbb{Q}[x]$ irreducible

has r_1 real roots, $2r_2$ non-real roots (r_2 complex conjugate roots)

eg. $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \{ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q} \}$
degree 4 over \mathbb{Q}
 $= \mathbb{Q}[\sqrt{2} + \sqrt{3}]$

K can be embedded in \mathbb{C} in $n = [K:\mathbb{Q}]$ ways (not canonically), $n = r_1 + 2r_2$.

by mapping $x \mapsto$ any of the roots of $m(x)$.

Dirichlet's Unit Theorem applies to all number fields, Galois or not.

$|\text{Aut } K| \leq n$.
Equality iff K is a Galois extension.

Eg. $K = \mathbb{Q}[\sqrt{d}]$, d squarefree, $d \neq 0, 1$. $K \cong \mathbb{Q}[x] / (x^2 - d)$

If $d > 0$ then $r_1 = 2, r_2 = 0, n = r_1 + 2r_2 = 2, \text{rank } r_1 + r_2 - 1 = 2 + 0 - 1 = 1$.

If $d < 0$ then $r_1 = 0, r_2 = 1, n = r_1 + 2r_2 = 2, \text{rank } r_1 + r_2 - 1 = 0 + 1 - 1 = 0$.

Another example with Dirichlet's Unit Theorem

$$K = \mathbb{Q}[\sqrt{2}, \sqrt{3}] = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}\} \supset \mathbb{Q} \quad \text{degree } [K:\mathbb{Q}] = 4$$

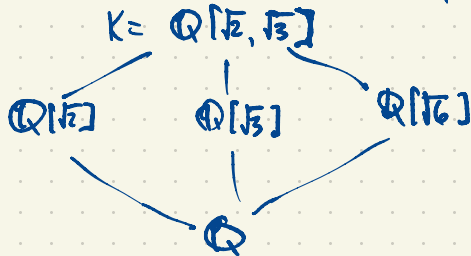
Every embedding $K \hookrightarrow \mathbb{C}$ is real ($K \hookrightarrow \mathbb{R}$) i.e. $r_1 = 4, r_2 = 0, n = r_1 + 2r_2 = 4 + 0 = 4$.

Dirichlet's unit theorem: $\mathcal{O}^\times \cong \{\pm 1\} \times \mathbb{Z}^3$ i.e. $\mathcal{O}^\times = \{\pm \alpha^i \beta^j \gamma^k : i, j, k \in \mathbb{Z}\}$

the only roots of \mathbb{R} are ± 1

$$r_1 + r_2 - 1 = 4 + 0 - 1 = 3 \text{ gives the rank.}$$

What are the generators α, β, γ unity in this case? (fundamental units)



There are all the five subfields of K by Galois theory.

$$\pm (1 + \sqrt{2})^k \text{ units in } \mathbb{Q}[\sqrt{2}]$$

$$\pm (2 + \sqrt{3})^k \text{ --- } \mathbb{Q}[\sqrt{3}]$$

$$\pm (5 + 2\sqrt{6})^k \text{ --- } \mathbb{Q}[\sqrt{6}]$$

$$x^2 - 2y^2 = \pm 1 = (1 + \sqrt{2})(1 - \sqrt{2}) = -1$$

$$(1 + \sqrt{2})^k (-1 + \sqrt{2})^k = 1$$

$$(2 + \sqrt{3})(2 - \sqrt{3}) = 1$$

$$x^2 - 6y^2 = \pm 1 \quad (5, 2) \text{ fundamental solution}$$

$$(5 + 2\sqrt{6})(5 - 2\sqrt{6}) = 1$$

$$\mathbb{Z} \mathcal{O}^\times = \pm (1 + \sqrt{2})^k (2 + \sqrt{3})^l (5 + 2\sqrt{6})^m, \quad k, l, m \in \mathbb{Z} ?$$

No, these are only 25% of the units in K .

First of all, $\mathcal{O} = \{\text{alg. int. in } K\} \cong \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Z}\}$.

Since $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ are alg. int.

If $x = \frac{\sqrt{2} + \sqrt{6}}{2}$ then $x^2 = \frac{2 + 6 + 4\sqrt{3}}{4} = 2 + \sqrt{3}$, $x^2 - 2 = \sqrt{3}$, $x^4 - 4x^2 + 1 = 0 \Rightarrow x$ is an alg. int.

In fact $\alpha \in \mathcal{O}^\times$.

$$\beta = \sqrt{2} + \sqrt{3} \text{ then } \beta^2 = (\sqrt{2} + \sqrt{3})^2 = 2 + 3 + 2\sqrt{6} = 5 + 2\sqrt{6}$$

$$\beta^2 - 5 = 2\sqrt{6} \Rightarrow \beta^4 - 10\beta^2 + 1 = 0$$

$$\gamma = 1 + \sqrt{2}$$

$$(1 + \sqrt{2})(-1 + \sqrt{2}) = 1$$

$$1 = 10\beta^2 - \beta^4 = \beta \cdot (10\beta - \beta^3)$$

Checked using PARI/GP.

$f: \mathbb{C} \rightarrow \mathbb{C}$ is analytic in a region $\Omega \subset \mathbb{C}$ (open set) if f' exists in Ω .

In this case at every point $z_0 \in \Omega$ there is a series expansion $f(z) = \sum_{n=0}^{\infty} a_n (z-z_0)^n$ in some disk $|z-z_0| < r$ in Ω .



A function f is meromorphic in Ω if at every point $z_0 \in \Omega$ it has a Laurent expansion $f(z) = \sum_{n=-k}^{\infty} a_n (z-z_0)^n$, $k \in \mathbb{Z}$.
When $a_{-k} \neq 0$ with $k < 0$, we have a pole of order k (assuming k is the largest such).

f has a simple pole at z_0 if $e^{\frac{1}{z}}$ has an essential singularity at 0 ("worse" than a pole)
 $f(z) = \frac{a_{-1}}{z-z_0} + a_0 + a_1(z-z_0) + a_2(z-z_0)^2 + \dots$ $0 < |z-z_0| < r$ in Ω
 a_{-1} = Residue of f at z_0 .



$$\frac{1}{2\pi i} \int_{\gamma} f(z) dz = a_{-1} = \lim_{z \rightarrow z_0} (z-z_0) f(z)$$

$\zeta(s), \zeta_K(s)$ is meromorphic in \mathbb{C} with a simple pole at $s=1$.

Class number formula

$$\lim_{s \rightarrow 1} (s-1) \zeta_K(s) = \frac{2^{r_1} (2\pi)^r \text{Reg}_K h_K}{w_K \sqrt{|\text{disc } K|}}$$

residue of $\zeta_K(s)$ at its simple pole

Reg_K = regulator of K

h_K = class number

w_K = number of roots of unity in K .

r_1 = no. of real embeddings $K \hookrightarrow \mathbb{R}$

$2r_2$ = non-real embeddings $K \hookrightarrow \mathbb{C}$

$$n = [K:\mathbb{Q}] = r_1 + 2r_2$$

Every number field $K \supseteq \mathbb{Q}$ has the form $K = \mathbb{Q}[\alpha] \cong \mathbb{Q}[x] / (m(x))$ $m(x) = \text{min. poly. of } \alpha \text{ over } \mathbb{Q}$

eg. $K = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ has $r_1 = 4$ real embeddings $K \hookrightarrow \mathbb{R}$
 $r_2 = 0$ non-real \dots $K \hookrightarrow \mathbb{C}$

eg. $\alpha = \sqrt{2} + \sqrt{3}$ is a generator

$$K = \mathbb{Q}[\alpha] = \mathbb{Q}[x] / (x^4 - 10x^2 + 1)$$

\uparrow
 $r_1 = 4$ real roots $\pm\sqrt{2} \pm \sqrt{3}$
 $r_2 = 0$ non-real roots.

I worked this out with $K = \mathbb{Q}[\sqrt{5}]$ $\text{Reg}_K = 1$ in this case $h_K = 2$.

Remarks about computation:

$$\xi_K(2) \approx 1.855557$$

$$1/\xi_K(2) \approx 0.53892$$

$\frac{\xi_K(s)}{\xi(s)}$ has no pole at 1. It's a Dirichlet L-function. $= (1 - \frac{1}{3^s})^{-1} (1 - \frac{1}{7^s})^{-1} (1 + \frac{1}{11^s})^{-1} (1 + \frac{1}{13^s})^{-1} (1 + \frac{1}{17^s})^{-1} (1 + \frac{1}{19^s})^{-1} (1 - \frac{1}{23^s})^{-1} \dots$

The Riemann zeta function $\zeta(s) = \frac{1}{s-1} + O(1)$ as $s \rightarrow 1$ i.e. Residue of $\zeta(s)$ at $s=1$ is 1.

$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x}$ converges by comparison with $\int_1^{\infty} \frac{1}{t^x} dt = \frac{1}{x-1}$ $\frac{1}{x-1} < \zeta(x) < \frac{1}{x-1} + 1$

($x > 1$)
real

Remarks about class number h_K of a quadratic number field $K = \mathbb{Q}[\sqrt{d}]$:

We know only finitely many imaginary quadratic fields have class number 1, for
 $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$ eg. $h_{\mathbb{Q}[\sqrt{-5}]} = 2$

In fact $h_K \rightarrow \infty$ as $d \rightarrow -\infty$

We know much less about the real quadratic fields.

We think there are infinitely many real quadratic fields with class number 1.

$$e^{\pi\sqrt{163}} = 262\,537\,412\,640\,768\,743.999\,999\,999\,999\,250\,725\,9\dots$$

$x^2 + x + 41$ has prime values for $x = 0, 1, 2, 3, \dots, 39$

There is no nonconstant polynomial $f(x) \in \mathbb{Z}[x]$ having only prime values.

There is no known polynomial $f(x) \in \mathbb{Z}[x]$ of degree > 1 which is prime infinitely often.

Is $x^2 + 1$ prime infinitely often? Open problem.

$$\text{disc}(x^2 + x + 41) = 1 - 4 \cdot 41 = -163.$$

$$640320^3 + 744 = 262\,537\,412\,640\,768\,744$$

The polynomial $x^2 + x + k$ has prime values for $x = 0, 1, 2, \dots, k-2$ ($k > 0$)

$$\iff k \in \{1, 2, 3, 5, 11, 17, 41\}$$

$$\iff h_{\mathbb{Q}[\sqrt{d}]} = 1, \quad d = 1 - 4k$$

$$\iff d \in \{-3, -7, -11, -19, -43, -67, -163\}$$

Where do Dirichlet L-functions come from?

Dirichlet characters are functions $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ satisfying $\chi(ab) = \chi(a)\chi(b)$ and some additional properties $\chi(1) = 1$, $\chi(0) = 0$ unless $\chi = 1$ identically (we usually ignore this case)

$\chi(1) = \chi(1)\chi(1) \Rightarrow \chi(1) = 0$ or 1 .

χ should be a function on $\mathbb{Z}/n\mathbb{Z}$ i.e. $\chi(a) = \chi(b)$ whenever $a \equiv b \pmod{n}$.

$$\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \xrightarrow{\chi} \mathbb{C}$$

(χ is a Dirichlet character mod n in this case)

The Dirichlet L-function corresponding to χ is

$$L_\chi(s) = L(\chi, s) = \sum_{k=1}^{\infty} \frac{\chi(k)}{k^s} = \prod_p \left(\frac{1}{1 - \frac{\chi(p)}{p^s}} \right)$$

$$= \frac{\zeta_\chi(s)}{\zeta(s)}$$

proof: use FTA (Fund. Thm. of Arithmetic: unique factorization in \mathbb{Z})

$$\frac{1}{1 - \frac{a}{p^s}} = 1 + \frac{a}{p^s} + \frac{a^2}{p^{2s}} + \frac{a^3}{p^{3s}} + \dots$$

Euler factorization

eg. There are $\phi(20) = 8$ Dirichlet characters mod 20 including

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	...
$\chi(k)$	0	1	0	1	0	0	0	1	0	1	0	-1	0	-1	0	0	0	-1	0	-1	0	1	0	1	0	0	

$$L(\chi, s) = 1 + \frac{1}{3^s} + \frac{1}{7^s} + \frac{1}{9^s} - \frac{1}{11^s} - \frac{1}{13^s} - \frac{1}{17^s} + \frac{1}{21^s} + \frac{1}{23^s} + \frac{1}{27^s} + \frac{1}{29^s} - \frac{1}{31^s} - \frac{1}{33^s} - \dots$$

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}$$

For $p=2$, $(2) = \mathfrak{p}_2^2$, $\mathfrak{p}_2 = (2, 1 + \sqrt{5})$, $N(\mathfrak{p}_2) = 2$,
Same at $p=5$.

$$\zeta_\chi(s) = \prod_p \frac{1}{1 - \frac{\chi(p)}{p^s}}$$

For $p=3$, $(3) = \mathfrak{p}_3 \bar{\mathfrak{p}}_3$, $\mathfrak{p}_3 = (3, 1 + \sqrt{5})$, $N(\mathfrak{p}_3) = 3$
Same for $p \equiv 1, 3, 7, 9 \pmod{20}$ (p splits)

For $p=11$, $(11) = \mathfrak{p}_{11}$, $N(\mathfrak{p}_{11}) = 11^2 = 121$

Same for $p \equiv 1, 13, 17, 19 \pmod{20}$ (p remains prime)

$$\frac{\zeta_\chi(s)}{\zeta(s)} \text{ has Euler factors at } 2: \frac{1/(1 - \frac{1}{2^s})}{1/(1 - \frac{1}{2^s})} = 1 = \frac{1}{1 - \frac{1}{2^s}}$$

$$\dots 3: \frac{1/(1 - \frac{1}{3^s})^2}{1/(1 - \frac{1}{3^s})} = \frac{1}{1 - \frac{1}{3^s}}$$

$$\frac{\zeta_\chi(s)}{\zeta(s)} \dots 11: \frac{1/(1 - \frac{1}{11^s})}{1/(1 - \frac{1}{11^s})} = \frac{1}{1 + \frac{1}{11^s}}$$

Why do we care about Dirichlet L-functions?

These are essential for proving:

Dirichlet's Theorem: Every arithmetic progression $a, a+k, a+2k, a+3k, a+4k, \dots$ contains infinitely many primes i.e. there are infinitely many primes $\equiv k \pmod{a}$.

$$\begin{aligned} a, k &\in \mathbb{Z} \\ k &> 0 \\ \gcd(a, k) &= 1 \end{aligned}$$

The number of Dirichlet characters mod 5 is $4 = \phi(5)$

Let χ be a Dirichlet character mod 5:

$\chi(a)$ only depends on $a \pmod{5}$.

$$\chi(ab) = \chi(a)\chi(b)$$

$$\chi(1) = 1.$$

$$\chi(2)^4 = \chi(2^4) = \chi(16) = \chi(1) = 1 \Rightarrow \chi(2) \in \{ \pm 1, \pm i \}$$

$$\chi(4) = \chi(2)^2$$

$$\chi(3) = \chi(2)^3$$

$$\chi(i) = 1$$

n	0	1	2	3	4	5	6	7	...
$\chi_0(n)$	0	1	1	1	1	0	1	1	...
$\chi_1(n)$	0	1	i	-i	1	0	1	i	...
$\chi_2(n)$	0	1	-1	-1	1	0	1	-1	...
$\chi_3(n)$	0	1	-i	i	-1	0	1	-i	...

$\chi(k)$ is either 0 or a root of unity

(if $\gcd(k, n) > 1$)

(if $\gcd(k, n) = 1$)

We'll discuss the special case of Dirichlet's Theorem for $n=4$:

There are infinitely many primes $\equiv 1 \pmod{4}$ and $\equiv 3 \pmod{4}$.

Warm-up: There are infinitely many primes.

- Euclid's proof

- Euler's proof: $\sum_p \frac{1}{p}$ diverges. (sum over primes p)

$$= \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \dots$$

Compare: Let $A \subseteq \mathbb{N}$ be the set of all positive integers not having 7 as any of its digits.

$$A = \{1, 2, 3, 4, 5, 6, 8, 9, 10, 11, \dots, 16, 18, 19, \dots\}$$

$\sum_{n \in A} \frac{1}{n} < \infty$. So A is in some sense less dense than $\{\text{primes}\} = \{2, 3, 5, 7, 11, 13, \dots\}$

Start with $\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x}$, $x > 1$. Comparison with $\int_1^{\infty} \frac{1}{t^x} dt$ gives $\frac{1}{x-1} < \zeta(x) < \frac{1}{x-1} + 1$

$$\zeta(x) \rightarrow \infty \text{ as } x \rightarrow 1^+$$

$$\frac{1}{1-u} = 1 + u + u^2 + u^3 + \dots \text{ for } |u| < 1.$$

$$-\ln(1-u) = \ln\left(\frac{1}{1-u}\right) = u + \frac{u^2}{2} + \frac{u^3}{3} + \frac{u^4}{4} + \dots, \text{ for } |u| < 1.$$

$$\zeta(x) = \prod_p \frac{1}{1-p^{-x}} \text{ for } x > 1 \quad p \in \{\text{primes}\}$$

$$\begin{aligned} \ln \zeta(x) &= \sum_p \ln\left(\frac{1}{1-p^{-x}}\right) \\ &= \sum_p \sum_{k=1}^{\infty} \frac{1}{k p^{kx}} = \underbrace{\sum_p \frac{1}{p^x}}_{\text{large}} + \underbrace{\sum_{k=2}^{\infty} \sum_p \frac{1}{k p^{kx}}}_{\text{small}} \end{aligned}$$

Helpful in HW1 #6:
If $N(\alpha) = -1$ then

$$N(\alpha^2) = 1$$

eg. in $K = \mathbb{Q}[\sqrt{101}]$, solve $x^2 - 101y^2 = -1$
 $x^2 + 1 = 101y^2$

$$(x, y) = (10, 1)$$

$$N\left(\frac{10 + \sqrt{101}}{\alpha}\right) = -1$$

$$\alpha^2 = (10 + \sqrt{101})^2 = 100 + 101 + 20\sqrt{101}$$

$(x, y) = (201, 20)$ is a solution of $x^2 - 101y^2 = 1$
 $= 201 + 20\sqrt{101}$

For all $x > 1$ (uniformly)

$$u^2 + u^3 + u^4 + \dots = \frac{u^2}{1-u}$$

$\text{for } |u| < 1$
 $u = \frac{1}{p^x}$

$$\sum_p \sum_{k=2}^{\infty} \frac{1}{k p^{kx}} \leq \frac{1}{2} \sum_p \sum_{k=2}^{\infty} \frac{1}{p^{kx}} = \frac{1}{2} \sum_p \left(\frac{1}{p^{2x}} + \frac{1}{p^{3x}} + \frac{1}{p^{4x}} + \dots \right) = \frac{1}{2} \sum_p \frac{\frac{1}{p^{2x}}}{1 - \frac{1}{p^x}} = \frac{1}{2} \sum_p \frac{1}{p^x(p^x - 1)}$$

$$\leq \frac{1}{2} \sum_p \frac{2}{p^{2x}} = \sum_p \frac{1}{p^{2x}} \leq \sum_p \frac{1}{p^2} \leq \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} < \infty$$

So $\sum_p \frac{1}{p^x} = \ln \zeta(x) - (\text{small terms in } [0, \frac{\pi^2}{6}])$ for all $x > 1$.

As $x \rightarrow 1^+$, $\ln \zeta(x) \rightarrow \infty$ but ("small terms") $\rightarrow \infty$ so $\sum_p \frac{1}{p^x} \rightarrow \infty$.

So there are infinitely many primes. And moreover, $\sum_p \frac{1}{p}$ diverges.

There are many proofs of the infinitude of primes; including

- Euclid
- Euler
- Farstenberg

Dirichlet's proof builds on Euler's proof

Mod 4 case: there are just two Dirichlet characters mod 4 since $\phi(4) = 2$

If $\chi: \mathbb{Z} \rightarrow \mathbb{C}$ is a Dirichlet character mod 4 then $\chi(k) = 1$ whenever $k \equiv 1 \pmod{4}$
 $\chi(k) = 0$ if $\gcd(k, 4) > 1$ (k even)

$$\chi(ab) = \chi(a)\chi(b) \text{ for all } a, b \in \mathbb{Z}$$

$$\chi(3) = \chi(9) = \chi(1) = 1$$

k	0	1	2	3	4	5	6	7	8	9	10	11	...
$\chi_0(k)$	0	1	0	1	0	1	0	1	0	1	0	1	...
$\chi_1(k)$	0	1	0	-1	0	1	0	-1	0	1	0	-1	...

Two Dirichlet series mod 4:

$$L_0(s) = L_{\chi_0}(s) = \sum_{n=1}^{\infty} \frac{\chi_0(n)}{n^s} = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \dots = \prod_p \frac{1}{1 - \frac{\chi_0(p)}{p^s}} = \prod_{p \text{ odd}} \frac{1}{1 - \frac{1}{p^s}}$$

$$(1 - \frac{1}{2^s}) L_0(s) = (1 + \frac{1}{2^s} + \frac{1}{4^s} + \dots) (1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \dots)$$

For $x > 1$, $L_0(x)$ converges; $L_0(x) \rightarrow \infty$ as $x \rightarrow 1^+$

$$= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \dots = \zeta(s)$$

$$\begin{array}{c} (1 - \frac{1}{2^x}) \zeta(x) \\ \downarrow \quad \downarrow \\ \frac{1}{2} \quad \infty \end{array}$$

$$L_1(x) = L_{\chi_1}(x) = \sum_{n=1}^{\infty} \frac{\chi_1(n)}{n^x} = 1 - \frac{1}{2^x} + \frac{1}{5^x} - \frac{1}{7^x} + \frac{1}{11^x} - \frac{1}{13^x} + \dots \quad \text{for } x > 1.$$

$$L_1(x) \rightarrow \boxed{\frac{\pi}{4}} \quad \text{when } x \rightarrow 1^+$$

we only care that this converges.

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \dots = \frac{\pi}{4}$$

$$\frac{1}{1+x^2} = 1 - x^2 + x^4 - x^6 + x^8 - x^{10} + \dots \quad (|x| < 1)$$

$$\tan^{-1} x = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \dots \quad (|x| \leq 1)$$

$$L_0(x) + L_1(x) = 2 \left(1 + \frac{1}{5^x} + \frac{1}{9^x} + \frac{1}{13^x} + \frac{1}{17^x} + \dots \right) = 2 \sum_{\substack{n=1 \\ n \equiv 1 \pmod{4}}} \frac{1}{n^x}$$

$$(x > 1)$$

$$L_0(x) - L_1(x) = 2 \left(\frac{1}{3^x} + \frac{1}{7^x} + \frac{1}{11^x} + \frac{1}{15^x} + \dots \right) = 2 \sum_{\substack{n=3 \\ n \equiv 3 \pmod{4}}} \frac{1}{n^x}$$

$$(x > 1)$$

$$\ln L_0(x) = \ln \prod_{p \text{ odd}} \frac{1}{1 - \frac{1}{p^x}} = \sum_{p \text{ odd}} \ln \left(1 - \frac{1}{p^x}\right) = \sum_{p \text{ odd}} \sum_{k=1}^{\infty} \frac{1}{k p^{kx}} = \sum_{p \text{ odd}} \frac{1}{p^x} + \sum_{p \text{ odd}} \sum_{k \geq 2} \frac{1}{k p^{kx}}$$

$\underbrace{\hspace{10em}}_{k=1}$ $\underbrace{\hspace{10em}}_{\text{uniformly bounded for } x > 1}$

When $x \rightarrow 1^+$, $\ln L_0(x) \rightarrow \infty$, $\sum_{p \text{ odd}} \frac{1}{p^x} \rightarrow \infty$, (small terms $\sum_{p \text{ odd}} \sum_{k \geq 2} \frac{1}{k p^{kx}} \not\rightarrow \infty$ stays bounded $\leq \frac{\pi^2}{6}$)

$$\ln L_1(x) = \ln \prod_{p \text{ odd}} \frac{1}{1 - \frac{\chi_1(p)}{p^x}} = \sum_{p \text{ odd}} \sum_{k=1}^{\infty} \frac{\chi_1(p)^k}{k p^{kx}} = \sum_{p \text{ odd}} \frac{\chi_1(p)}{p^x} + \sum_{p \text{ odd}} \sum_{k \geq 2} \frac{\chi_1(p)^k}{k p^{kx}}$$

\uparrow $\underbrace{\hspace{10em}}_{\text{stays bounded}}$

$$-\frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} - \frac{1}{19} - \frac{1}{23} + \frac{1}{29} - \frac{1}{31} + \dots$$

not alternating series $\sum_p \sum_k |(\cdot)| \leq \frac{\pi^2}{6}$

For all $x > 1$:

$$\ln L_0(x) + \ln L_1(x) = 2 \sum_{p \equiv 1 \pmod{4}} \frac{1}{p^x} + (\text{unif. bdd terms for all } x > 1)$$

$$= 2 \left(\frac{1}{5^x} + \frac{1}{13^x} + \frac{1}{17^x} + \frac{1}{29^x} + \dots \right) + \dots$$

$$\ln L_0(x) - \ln L_1(x) = 2 \sum_{p \equiv 3 \pmod{4}} \frac{1}{p^x} + (\text{unif. bdd terms for all } x > 1)$$

$$= 2 \left(\frac{1}{3^x} + \frac{1}{7^x} + \frac{1}{11^x} + \frac{1}{19^x} + \frac{1}{23^x} + \dots \right)$$

When $x \rightarrow 1^+$, $L_0(x) \rightarrow \infty$, $L_1(x) \rightarrow \text{pos. constant}$ so $\ln L_0(x) + \ln L_1(x) \rightarrow \infty$ $\Rightarrow \sum_{p \equiv 1 \pmod{4}} \frac{1}{p^x} \rightarrow \infty$
 $\ln L_0(x) - \ln L_1(x) \rightarrow \infty \Rightarrow \sum_{p \equiv 3 \pmod{4}} \frac{1}{p^x} \rightarrow \infty$.

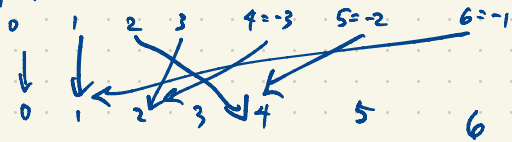
Reciprocity Laws, starting with quadratic reciprocity

Let p be an odd prime; $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \dots, p-1\}$ is a field.

Excluding 0, half of the elements of $\mathbb{F}_p - \{0\}$ are squares; half are nonsquares i.e. $\frac{p-1}{2} = \left| \begin{array}{l} \text{nonzero squares} \\ \text{non-squares} \end{array} \right|$

The map $\mathbb{F}_p \rightarrow \mathbb{F}_p, x \mapsto x^2$ is 2-to-1.

eg. $p=7$



$S = \{1, 2, 4\}$: nonzero squares

$N = \{3, 5, 6\}$: nonsquares

If $0 \neq s \in \mathbb{F}_p$ is a square then $s = a^2$ for some $a \in \mathbb{F}_p - \{0\}$ so $x^2 = s$ has two roots $\pm a$

$$x^2 = a^2$$

$$(x+a)(x-a) = x^2 - a^2 = 0$$

The only roots are $x = \pm a$.

Since $p \neq 2, a \neq -a$.

$$a = -a \iff 2a = 0$$

It's convenient to denote

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ 1 & \text{if } a = \text{square} \pmod{p} \\ -1 & \text{if } a = \text{nonsquare} \pmod{p} \end{cases}$$

(quadratic Dirichlet character mod p)

Legendre symbol

for p odd prime;
 $a \in \mathbb{Z}$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

One proof: use Euler's Criterion.

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} \\ \equiv 0 \text{ or } \pm 1$$

Proof of Euler's Criterion: Use Fermat's Little Theorem.

$$\text{For all } a \in \mathbb{Z}, p \text{ prime, } a^p \equiv a \pmod{p}$$

Now if p is an odd prime:

$$a^{p-1} \equiv 1 \pmod{p} \text{ if } a \not\equiv 0 \pmod{p}$$

Every element of \mathbb{F}_p is a root of $x^p - x \in \mathbb{F}_p[x]$

$$x^p - x = x(x^{p-1} - 1) = x(x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1)$$

How to compute $\left(\frac{q}{p}\right)$? (given $q \in \mathbb{Z}$, p prime)

If a, p are hundreds of digits long: Use Euler's criterion on a computer.

If you're working by hand using numbers that are up to about four digits: use the Law of Quadratic Reciprocity.

$$\left(\frac{p}{q}\right) = \pm \left(\frac{q}{p}\right) \quad \text{for any odd primes } p \neq q$$

↑
+1 if at least one of p, q is $\equiv 1 \pmod{4}$
-1 if $p \equiv q \equiv 3 \pmod{4}$.

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8} \end{cases}$$

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv -1 \pmod{4} \end{cases} \quad \left. \vphantom{\left(\frac{-1}{p}\right)} \right\} \text{Proof: Euler Criterion } (-1)^{\frac{p-1}{2}} \equiv \left(\frac{-1}{p}\right)$$

More concisely: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$ Law of Quadratic Reciprocity

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

Example Compute $\left(\frac{60}{7703}\right) = \left(\frac{2}{7703}\right)\left(\frac{3}{7703}\right)\left(\frac{5}{7703}\right) = -\left(\frac{7703}{3}\right) \cdot \left(\frac{7703}{5}\right) = -\left(\frac{2}{3}\right) \cdot \left(\frac{3}{5}\right) = -(-1) \cdot (-1) = -1$

So 60 is a nonsquare mod 7703.

$$\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1$$

Proof of Law of Quadratic Reciprocity

We use the quadratic Gauss sum for p an odd prime:

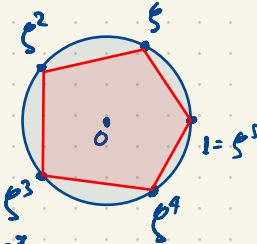
$\xi = e^{2\pi i/p}$ primitive p^{th} root of unity. ($\xi^p = 1 \neq \xi$, $\xi^{p^1} + \xi^{p^2} + \dots + \xi^2 + \xi + 1 = 0$)

$$S = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \xi^k = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \xi^k$$

quadratic Gauss sum ξ^2 root of $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \dots + x^2 + x + 1)$

min. poly of ξ over \mathbb{Q} (cyclotomic poly.)

Ex. $p=5$, $S = \xi - \xi^2 - \xi^3 + \xi^4$, $\xi = e^{2\pi i/5}$



$$\begin{aligned} S^2 &= (\xi - \xi^2 - \xi^3 + \xi^4)^2 = \xi^2 + \xi^4 + \xi^6 + \xi^8 \\ &= -2\xi^3 - 2\xi^4 + 2\xi^5 + 2\xi^5 - 2\xi^6 - 2\xi^7 \\ &= \underline{\xi^2} + \underline{\xi^4} + \underline{\xi} + \underline{\xi^3} - \underline{2\xi^3} - \underline{2\xi^4} + \underline{2} + \underline{2} - \underline{2\xi} - \underline{2\xi^2} \\ &= 4 - \xi - \xi^2 - \xi^3 - \xi^4 \\ &= 5 - \underbrace{(1 + \xi + \xi^2 + \xi^3 + \xi^4)} = 5 \end{aligned}$$

Lemma If S is the quadratic Gauss sum (defined above) then $S^2 = \pm p = \begin{cases} p & \text{if } p \equiv 1 \pmod{4} \\ -p & \text{if } p \equiv 3 \pmod{4} \end{cases}$

ie. $S^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p$

By the way, this implies that $S = \begin{cases} \pm\sqrt{p} & \text{if } p \equiv 1 \pmod{4} \\ \pm i\sqrt{p} & \text{if } p \equiv 3 \pmod{4} \end{cases}$

In fact both of these " \pm " signs turn out to be "+". But this takes a little more work and it's not needed to prove quadratic reciprocity.

Proof of the lemma:

$$S^2 = \left[\sum_{k=0}^{p-1} \binom{k}{p} s^k \right] \left[\sum_{l=0}^{p-1} \binom{l}{p} s^l \right]$$

$$= \sum_{k=0}^{p-1} \sum_{l=0}^{p-1} \binom{k+l}{p} s^{k+l}$$

Substitute $l = km$ for each k , $0 \leq m \leq p-1$

$$= \sum_{k=0}^{p-1} \sum_{m=0}^{p-1} \binom{k+m}{p} s^{k+km}$$

$$\binom{k+m}{p} = \binom{k}{p} \binom{m}{p} = \binom{m}{p}$$

$$= \sum_{k=0}^{p-1} \sum_{m=0}^{p-1} \binom{m}{p} s^{(m+1)k}$$

$$= \sum_{m=0}^{p-1} \binom{m}{p} \sum_{k=1}^{p-1} s^{(m+1)k}$$

When $m = p-1$, the inner sum is $\sum_{k=1}^{p-1} \binom{p-1}{p} = (p-1) \binom{-1}{p}$

$$= \binom{p-1}{p} \binom{-1}{p} - \left[\binom{0}{p} + \binom{1}{p} + \binom{2}{p} + \dots + \binom{p-2}{p} \right]$$

When $0 \leq m \leq p-2$, the inner sum is $s + s^2 + \dots + s^{p-1} = -1$
 $m+1$ nonzero integer mod p

ie. $1 + s + s^2 + \dots + s^{p-1} = 0$

for $m = p-1$ for $0 \leq m \leq p-2$

$$\sum_{k=0}^{p-1} \binom{k}{p} = \binom{0}{p} + \binom{1}{p} + \binom{2}{p} + \dots + \binom{p-1}{p} = 0$$

one term is 0
 $\frac{p-1}{2}$ terms equal +1 (for k square)
 $\frac{p-1}{2}$ terms equal -1 (for k nonsq)

$$= \binom{p-1}{p} \binom{-1}{p} - \left[-\binom{-1}{p} \right] = \binom{-1}{p} p \quad \square$$

If q is prime then $(x+y)^2 \equiv x^2 + y^2 \pmod{q}$. in $\mathbb{F}_q[x, y]$, $(x+y)^2 = x^2 + y^2$

Use Binomial Theorem $(x+y)^2 = x^2 + 2xy + y^2$

Complete the proof of Quadratic Reciprocity: use $q \equiv 0 \pmod{q}$.

$S = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \epsilon^k$ where $\epsilon = e^{2\pi i/p}$ $p \neq q$ odd primes

$S^2 = \left(\frac{-1}{p}\right) p$ Take $\frac{q-1}{2}$ power of both sides

$(S^2)^{\frac{q-1}{2}} = \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} p^{\frac{q-1}{2}}$

$S^{2^{\frac{q-1}{2}}} = (-1)^{\frac{q-1}{2} \cdot \frac{q-1}{2}} p^{\frac{q-1}{2}}$

$S^2 = (-1)^{\frac{(p-1)(q-1)}{4}} p^{\frac{q-1}{2}} S$

$\left(\frac{q}{p}\right) S \equiv (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right) S \pmod{q}$

$\left(\frac{q}{p}\right) S^2 \equiv (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right) S^2 \pmod{q}$

$\left(\frac{q}{p}\right) \equiv (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right) \pmod{q}$

$\pm 1 \equiv \pm 1 \pmod{q}$

$\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right)$

$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$

since q is an odd prime.

$\left(\frac{p}{q}\right) \equiv p^{\frac{q-1}{2}} \pmod{q}$ (Euler's Criterion)

Multiply both sides by S

$S^2 \equiv \left(\sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \epsilon^k\right)^2 \equiv \sum_{k=0}^{p-1} \left(\frac{k}{p}\right)^2 \epsilon^{kq}$

by above ("Freshman's Dream")

$= \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) \epsilon^{kq} = \sum_{k=0}^{p-1} \left(\frac{kq}{p}\right) \epsilon^{kq}$

$l = kq$

$= \sum_{l=0}^{p-1} \left(\frac{lq}{p}\right) \epsilon^{l} = \sum_{l=0}^{p-1} \left(\frac{l}{p}\right) \left(\frac{q}{p}\right) \epsilon^l = \left(\frac{q}{p}\right) \sum_{l=0}^{p-1} \left(\frac{l}{p}\right) \epsilon^l$

Multiply both sides by S

$S^2 = \pm p \not\equiv 0 \pmod{q}$

$\{\text{alg. int.}\} \cap \mathbb{Q} = \mathbb{Z}$

Modular forms & elliptic curves N. Koblitz

We'll start with elementary treatment of elliptic curves.

Let F be a field. The solutions of $y^2 = f(x) = ax^3 + bx^2 + cx + d$ ($a, b, c, d \in F$)
 $(x, y) \in F^2$ where $\gcd(f(x), f'(x)) = 1$

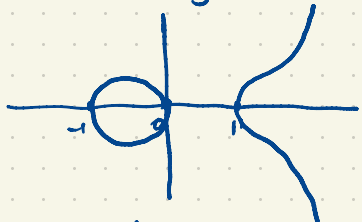
form an elliptic curve.

First caveat: Elliptic curves can be expressed in a more general form but often "change of coordinates" they take on a more standard form Weierstrass Normal Form suggested by our formula.

Second caveat: There is a "point at infinity" on the curve missing from our description.

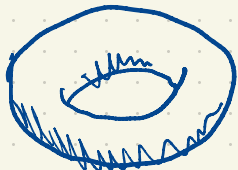
General fact: The points of any elliptic curve form an abelian group.

Eg. $F = \mathbb{R}$, curve $y^2 = x^3 - x$ is an elliptic curve



Topologically this curve is $S^1 \sqcup S^1$

The same equation over \mathbb{C} gives a more complete picture



torus

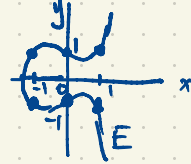
Importance of elliptic curves in number theory

- proof of FLT
- cryptography: most important public key cryptosystems
Diffie-Hellman, RSA, ECC = Elliptic Curve Cryptosystem
- primality testing, pseudorandom number generation
- integer factorization

Concrete example

$$E: y^2 = x^3 - x + 1$$

$f(x) = x^3 - x + 1$ has three distinct complex roots, one of which is real (not rational).



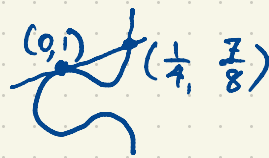
Symmetric about x-axis:
 $(x, y) \in E \iff (x, -y) \in E$.

$(0, \pm 1), (\pm 1, \pm 1) \in E$ Any other rational points on E?
 $(5, \pm 11), (3, \pm 5) \in E$ $11^2 = 121; 5^3 - 5 + 1 = 121$

There are infinitely many rational points on E because:



Solve $\begin{cases} y = mx + b \\ y^2 = x^3 - x + 1 \end{cases}$
 $(mx + b)^2 = x^3 - x + 1$ for x



Eg. $(0, 1), (1, -1) \in E$ lie on secant line $y = 1 - 2x$

Generically, a curve of degree m intersects a curve of degree n in mn points.

$$(1 - 2x)^2 = x^3 - x + 1$$
$$1 - 4x + 4x^2 = x^3 - x + 1$$

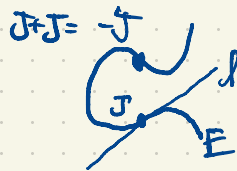
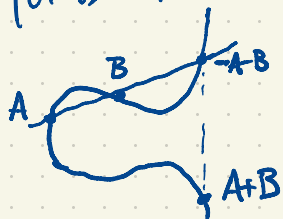
Eg. $(0, 1), (0, 1) \in E$ lie on tangent line $y = -\frac{1}{2}x + 1$ $0 = x^3 - 4x^2 + 3x = x(x-1)(x-3)$ gives $(3, -5) \in E$

$2yy' = 3x^2 - 1$ at $(0, 1), y' = -\frac{1}{2}$
 $2y' = -1$

Solve $\begin{cases} y = 1 - \frac{x}{2} \\ y^2 = x^3 - x + 1 \end{cases}$ $(1 - \frac{x}{2})^2 = x^3 - x + 1$
 $1 - x + \frac{x^2}{4} = x^3 - x + 1$

$$0 = x^3 - \frac{x^2}{4} = x^2(x - \frac{1}{4})$$

Group law on E : There is an abelian group operation "+" defined on the points of E defined by:



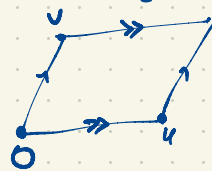
intersects E at J, J, J
 $J+J+J=0$
 But J has coordinates in $\mathbb{Q}[\sqrt{3}]$ or a degree 4 number field

$$J = \left(\frac{1}{\sqrt{3}}, \right)$$

not a rational point.

$$\begin{aligned} y^2 = x^3 - x + 1 &= \frac{1}{3\sqrt{3}} - \frac{1}{\sqrt{3}} + 1 \\ &= 1 - \frac{2}{3\sqrt{3}} \\ &= \frac{3\sqrt{3}-2}{3\sqrt{3}} \end{aligned}$$

$$(1-\sqrt{3})^2 = 4 - 2\sqrt{3}$$



$$\begin{aligned} L &= \mathbb{Z}u + \mathbb{Z}v \subset \mathbb{C} \\ \mathbb{R}^2/L &= T^2 = \text{torus} \\ &\cong E(\mathbb{R}) \end{aligned}$$

The identity element 0 is the unique point of E at infinity

The real points of E form an additive abelian group $E(\mathbb{R})$ and over \mathbb{Q} we get the rational points of E which is a subgroup $E(\mathbb{Q})$

$$E: y^2 = x^3 - x + 1$$

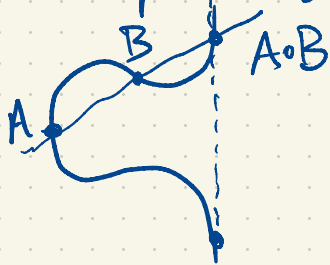
Why is the group law for addition associative?

- Check using coordinates. Ugly but elementary.
- This gives no insight.

- The curve (as a Riemann surface) is a torus. The explicit isomorphism uses Weierstrass elliptic functions \wp, \wp'

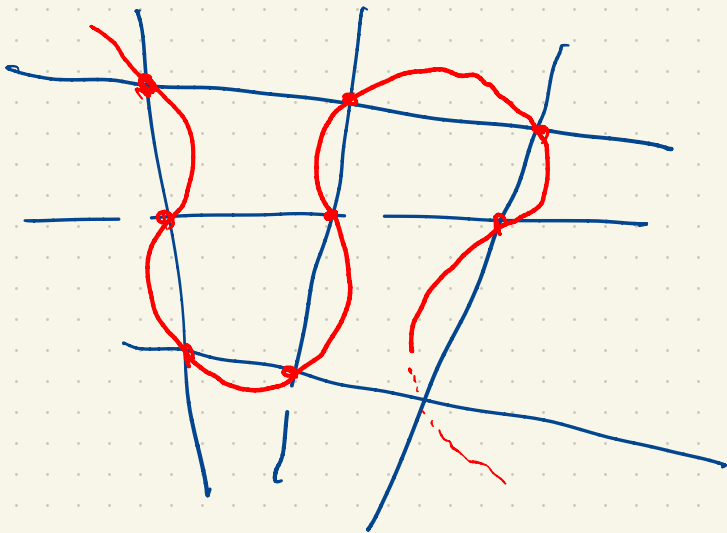
- More insight:

There is an important quasigroup (nonassociative group) coming from E



The group operation is $A+B = O \circ (A \circ B)$

The proof that $A+B$ is associative uses elementary but less technical arguments than



$E(\mathbb{F}_5) =$ points of E over $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$

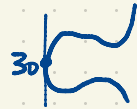
$E: y^2 = x^3 - x + 1$

x	$x^3 - x + 1$	y
0	1	± 1
1	1	± 1
2	2	no solutions
3	0	0
4	1	± 1

$E(\mathbb{F}_5) = \{0, (0,1), (0,-1), (\pm 1, \pm 1), (3,0)\}$ is an abelian group of order 8.

$(3,0) \in E(\mathbb{F}_5)$ is the unique element of order 2

So $E(\mathbb{F}_5)$ must be cyclic



$30 + 30 = 0$

+	0	01	41	14	30	11	44	04
0	0	01	41	14	30	11	44	04
01	01	41	14	30	11	44	04	0
41	41	14	30	11	44	04	0	01
14	14	30	11	44	04	0	01	41
30	30	11	44	04	0	01	41	14
11	11	44	04	0	01	41	14	30
44	44	04	0	01	41	14	30	11
04	04	0	01	41	14	30	11	44