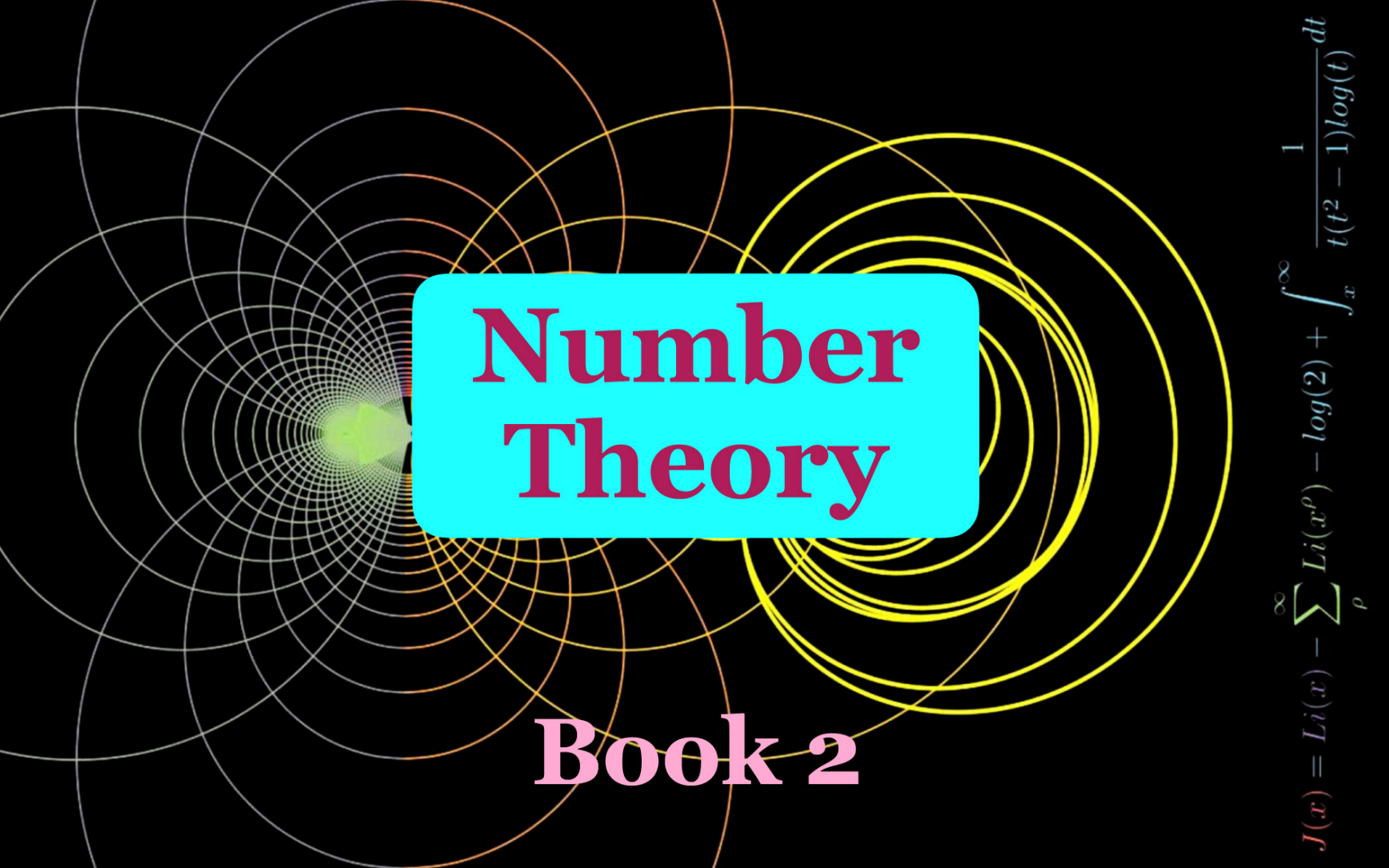

Number
Theory
Book 2
$J(x) = Li(x) - \sum_{\rho}^{\infty} Li(x^{\rho}) - \log(2) + \int_{x}^{\infty} \frac{1}{t(t^2-1)\log(t)} dt$

If R is any ring with identity then $R^\times = \{\text{units in } R\} = \{\text{invertible elements in } R\} = \{u \in R : uv = vu = 1 \text{ for some } v \in R\}$.
The units in the ring of $n \times n$ matrices over R form a mult. gp. $GL_n(R)$.
The units $R^\times$ the unit group of R.

If R is a commutative ring with identity then $R^\times$ is abelian.

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

eg. $\mathbb{Z}^\times = \{\pm 1\}$. $|\mathcal{O}^\times| \geq 2$ since $\pm 1 \in \mathcal{O}^\times$.

In a real quadratic field, $\mathcal{O}^\times = \{\pm 1\} \times \langle \alpha \rangle$ (commutative)

$\{\pm 1\}$: torsion part: the elements of finite order in $\mathcal{O}$ (roots of unity in $\mathcal{O}$)

$\langle \alpha \rangle = \{\alpha^k : k \in \mathbb{Z}\}$: infinite cyclic group with generator α

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

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

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

$\mathcal{O}^\times = \{\pm 1, \pm 1 \pm \sqrt{2}, \pm 3 \pm 2\sqrt{2}, \cdots\}$

$\langle \alpha \rangle = \langle 1+\sqrt{2} \rangle$ = positive elements in $\mathcal{O}^\times$.

Solutions of $x^2 - 2y^2 = \pm 1$ are $\{(\pm 1, 0), (\pm 1, \pm 1), (\pm 3, \pm 2), \cdots\}$.

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

$\{\pm 1\} \times \langle 1-\sqrt{2} \rangle = \{\pm 1\} \times \langle 1+\sqrt{2} \rangle = \mathcal{O}^\times$

$\langle 1-\sqrt{2} \rangle$: not canonical; $\langle 1+\sqrt{2} \rangle$: canonical

---

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

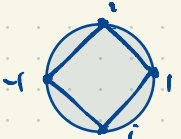
$\mathcal{O}^\times$ is finite since the equation $x^2 - dy^2 = \pm 1$ has only finitely many solutions

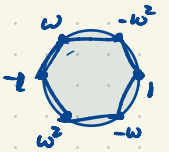
If $K = \mathbb{Q}[\sqrt{-5}]$ then $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$, $\mathcal{O}^\times = \{\pm 1\}$.

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

$\mathbb{Q}[\sqrt{-1}] = \mathbb{Q}[i]$ $\mathcal{O} = \mathbb{Z}[i]$ $\mathcal{O}^\times = \{\pm 1, \pm i\}$

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





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

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

($\{\text{roots of unity in } \mathcal{O}\}$: torsion part of $\mathcal{O}^\times$; finite cyclic group of even order)

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

written additively.

r_1+r_2-1 = 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. $K = \mathbb{Q}[\alpha]$ 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 pairs), $n = r_1 + 2r_2$.

e.g. $\mathbb{Q}[\sqrt{2},\sqrt{3}] = \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} : a,b,c,d \in \mathbb{Q}\}$ 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. $|\mathrm{Aut}\, K| \le n$. 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 $r_1=2$, $r_2=0$, $n = r_1+2r_2 = 2$, rank $r_1+r_2-1 = 2+0-1 = 1$.

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

Another example with Dirichlet's Unit Theorem

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

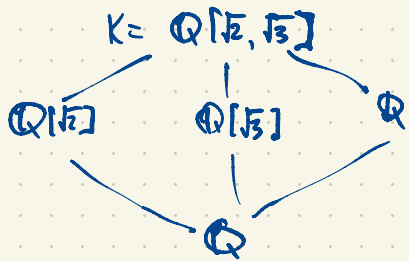
Every embedding $K \hookrightarrow \mathbb{C}$ is real ($K \hookrightarrow \mathbb{R}$) i.e. $r_1 = 4$, $r_2 = 0$, $n = r_1 + 2r_2 = 4+0 = 4$.

Dirichlet's unit theorem: $\mathcal{O}^\times \cong \{\pm 1\} \times \mathbb{Z}^3$ ← the only roots of $\mathbb{R}$ are ± 1

i.e. $\mathcal{O}^\times = \{\pm \alpha^i \beta^j \gamma^k : i,j,k \in \mathbb{Z}\}$

$r_1 + r_2 - 1 = 4+0-1 = 3$ gives the rank.

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



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

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

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

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

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

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

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

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

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

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

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

First of all, $\mathcal{O} = \{\text{alg. int. in } K\} \supseteq \{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} : a,b,c,d \in \mathbb{Z}\}$. Since $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ are alg. int.

Actually $\mathcal{O} = (1, \sqrt{2}, \sqrt{3}, \sqrt{6}, \frac{\sqrt{2}+\sqrt{6}}{2}) = (1, \sqrt{2}, \sqrt{3}, \frac{\sqrt{2}+\sqrt{6}}{2})$

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

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

$\beta = \sqrt{2}+\sqrt{3}$ 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.

$f: \mathbb{C} \to \mathbb{C}$ 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)

$e^{\frac{1}{z}}$ has an essential singularity at 0 ("worse" than a pole)

f has a simple pole at z_0 if $f(z) = \frac{a_{-1}}{z-z_0} + a_0 + a_1(z-z_0) + a_2(z-z_0)^2 + \cdots$ $0 < |z-z_0| < r$ in Ω

a_{-1} = Residue of f at z_0.

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

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

Class number formula
$$\underbrace{\lim_{s \to 1} (s-1)\zeta_K(s)}_{\text{residue of } \zeta_K(s) \text{ at its simple pole}} = \frac{2^{r_1}(2\pi)^{r_2} \operatorname{Reg}_K h_K}{w_K \sqrt{|\operatorname{disc} K|}}$$

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 $K \supset \mathbb{Q}$ has the form $K = \mathbb{Q}[\alpha] \cong \mathbb{Q}[x]/(m(x))$ $m(x)$ = min. poly. of α 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 $\cdots$ $K \hookrightarrow \mathbb{C}$

eg. $\alpha = \sqrt{2} + \sqrt{3}$ is a generator
$K = \mathbb{Q}[\alpha] = \mathbb{Q}[x]/(x^4 - 10x^2 + 1)$
$r_1 = 4$ real roots $\pm\sqrt{2} \pm \sqrt{3}$
$2r_2 = 0$ non-real roots.

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

Remarks about computation:

$\zeta_K(2) \approx 1.855557$

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

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

The Riemann zeta function $\zeta(s) = \frac{1}{s-1} + O(1)$ as $s \to 1$ 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 $h_K \to \infty$ as $d \to -\infty$

We know much less about the real quadratic fields.

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

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

- $x^2 + x + 41$ has prime values for $x = 0, 1, 2, 3, \cdots, 39$
- 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.
- $\operatorname{disc}(x^2 + x + 41) = 1 - 4 \cdot 41 = -163$.

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

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

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

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

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

Where do Dirichlet L-functions come from?

Dirichlet characters are functions $\chi: \mathbb{Z} \to \mathbb{C}$ 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 $\mathbb{Z}/n\mathbb{Z}$ ie. $\chi(a) = \chi(b)$ whenever $a \equiv b \bmod n$.

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

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

The Dirichlet L-function corresponding to χ is

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

$$= \frac{\xi_K(s)}{\zeta(s)}$$

Euler factorization

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

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

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

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

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

$$\xi_K(s) = \prod_{\mathfrak{g}} \frac{1}{1 - \frac{1}{N(\mathfrak{g})^s}}$$

For $p = 2$, $(2) = \mathfrak{g}_2^2$, $\mathfrak{g}_2 = (2, 1+\sqrt{-5})$, $N(\mathfrak{g}_2) = 2$,

Same at $p = 5$.

For $p = 3$, $(3) = \mathfrak{g}_3\bar{\mathfrak{g}}_3$, $\mathfrak{g}_3 = (3, 1+\sqrt{-5})$, $N(\mathfrak{g}_3) = 3$

Same for $p \equiv 1, 3, 7, 9 \bmod 20$ (p splits)

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

Same for $p \equiv 11, 13, 17, 19 \bmod 20$ (p remains prime)

$\frac{\xi_\chi(s)}{\zeta(s)}$ has Euler factors at 2: $\frac{1/(1-\frac{1}{2^s})}{1/(1-\frac{1}{2^s})} = 1 = \frac{1}{1-\frac{0}{2^s}}$

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

$\frac{\xi_\chi(s)}{\xi_K(s)}$ ⋯⋯ 11: $\frac{1/(1-\frac{1}{121^s})}{1/(1-\frac{1}{11^s})} = \frac{1}{1+\frac{1}{11^s}}$

Why do we care about Dirichlet L-functions?
These are essential for proving:

Dirichlet's Theorem: Every arithmetic progression $a, a+k, a+2k, a+3k, a+4k, \ldots$ ($a,k \in \mathbb{Z}$, $k>0$, $\gcd(a,k)=1$) contains infinitely many primes i.e. there are infinitely many primes $\equiv k \bmod a$.

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

Let χ be a Dirichlet character mod 5: $\chi(a)$ only depends on $a \bmod 5$.

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

$\chi(1) = 1$.

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

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

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

$\chi(1) = 1$

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 (if $\gcd(k,n)>1$) or a root of unity (if $\gcd(k,n)=1$)

We'll discuss the special case of Dirichlet's Theorem for $n=4$:
There are infinitely many primes $\equiv 1 \bmod 4$ and
primes $\equiv 3 \bmod 4$.

Warm-up: There are infinitely many primes.

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

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

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

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

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

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

$\zeta(x) \to \infty$ as $x \to 1^+$.

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

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

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

$\ln \zeta(x) = \sum_p \ln\left(\frac{1}{1-\frac{1}{p^x}}\right)$ $\quad u = \frac{1}{p^x} \in (0,1)$

$= \sum_p \sum_{k=1}^{\infty} \frac{1}{k p^{kx}} = \underbrace{\sum_p \frac{1}{p^x}}_{\text{large}} + \underbrace{\sum_p \sum_{k=2}^{\infty} \frac{1}{k p^{kx}}}_{\text{small}}$

Helpful in HW1 #6:

If $N(\alpha) = -1$ then $N(\alpha^2) = 1$

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

$x^2 + 1 = 101y^2$

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

$N(\underbrace{10 + \sqrt{101}}_{\alpha}) = -1$

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

$= 201 + 20\sqrt{101}$

$(x, y) = (201, 20)$ is a solution of $x^2 - 101y^2 = 1$

For all $x>1$ (uniformly)

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

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

$u^2+u^3+u^4+\cdots = \frac{u^2}{1-u}$ for $|u|<1$

$u = \frac{1}{p^x}$

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

$\frac{1}{p^x-1} \le \frac{2}{p^x}$

$p^x \le 2(p^x-1)$

$p^x \le 2p^x - 2$

$2 \le p^x$ $\quad p \ge 2$, $x \ge 1$

So $\sum_p \frac{1}{p^x} = \ln \zeta(x) - (\text{small terms})$ for all $x>1$.

($\text{small terms} \in [0, \frac{\pi^2}{6}]$)

As $x \to 1^+$, $\ln \zeta(x) \to \infty$ but ("small terms") $\not\to \infty$ so $\sum_p \frac{1}{p^x} \to \infty$.

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
- Furstenberg

Dirichlet's proof builds on Euler's proof

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

If $\chi: \mathbb{Z} \to \mathbb{C}$ is a Dirichlet character mod 4 then $\chi(k) = 1$ when ever $k \equiv 1 \bmod 4$

$\chi(k) = 0$ - - - $\gcd(k,4) > 1$ (k even)

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

$\chi(3)^2 = \chi(9) = \chi(1) = 1$

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:

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

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

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

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

$$\| \quad \left(1 - \frac{1}{2^x}\right)\zeta(x)$$

$$\downarrow \quad \downarrow$$

$$\frac{1}{2} \quad \infty$$

$$L_1(x) = L_{\chi_1}(x) = \sum_{n=1}^{\infty} \frac{\chi_1(n)}{n^x} = 1 - \frac{1}{3^x} + \frac{1}{5^x} - \frac{1}{7^x} + \frac{1}{9^x} - \frac{1}{11^x} + \cdots \quad \text{for } x > 1.$$

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

we only care that this converges.

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

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

$$\tan^{-1} x = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \cdots \qquad (|x| \le 1)$$

$$L_0(x) + L_1(x) = 2\left(1 + \frac{1}{5^x} + \frac{1}{9^x} + \frac{1}{13^x} + \frac{1}{17^x} + \cdots\right) = 2\sum_{n \equiv 1 \bmod 4} \frac{1}{n^x} \qquad (x > 1)$$

$$L_0(x) - L_1(x) = 2\left(\frac{1}{3^x} + \frac{1}{7^x} + \frac{1}{11^x} + \frac{1}{15^x} + \cdots\right) = 2\sum_{n \equiv 3 \bmod 4} \frac{1}{n^x} \qquad (x > 1)$$

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

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

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

$\frac{\chi_1(p)}{p^x}$: $-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}-\frac{1}{11}+\frac{1}{13}+\frac{1}{17}-\frac{1}{19}-\frac{1}{23}+\frac{1}{29}-\frac{1}{31}+\cdots$ not alternating series

$\sum_p \sum_k |(*)| \leq \frac{\pi^2}{6}$

For all $x>1$:

$$\ln L_0(x) + \ln L_1(x) = 2 \sum_{p \equiv 1 \bmod 4} \frac{1}{p^x} + (\text{unif. bdd terms for all } x>1)$$
$$= 2\left(\frac{1}{5^x} + \frac{1}{13^x} + \frac{1}{17^x} + \frac{1}{29^x} + \cdots\right) + \cdots$$

$$\ln L_0(x) - \ln L_1(x) = 2 \sum_{p \equiv 3 \bmod 4} \frac{1}{p^x} + (\text{unif. bdd terms for all } x>1)$$
$$= 2\left(\frac{1}{3^x} + \frac{1}{7^x} + \frac{1}{11^x} + \frac{1}{19^x} + \frac{1}{23^x} + \cdots\right)$$

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

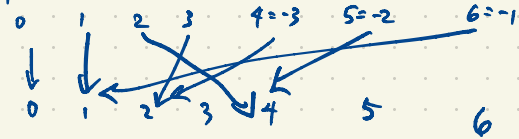
Reciprocity Laws, starting with quadratic reciprocity

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

Excluding 0, half of the elements of $\mathbb{F}_p - \{0\}$ are squares; half are nonsquares ie. $\frac{p-1}{2} = |\text{nonzero squares}| = |\text{nonsquares}|$

The map $\mathbb{F}_p \to \mathbb{F}_p$, $x \mapsto x^2$ 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

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

(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.

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

$\equiv 0$ or ± 1

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

For all $a \in \mathbb{Z}$, p prime, $a^p \equiv a \bmod p$.

$a^{p-1} \equiv 1 \bmod p$ if $a \not\equiv 0 \bmod p$.

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

Now if p is an odd prime:

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

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

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

$\uparrow$ $+1$ if at least one of p, q is $\equiv 1 \bmod 4$

-1 if $p \equiv q \equiv 3 \bmod 4$.

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

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

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

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

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

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

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

So 60 is a nonsquare mod 7703.

Proof of Law of Quadratic Reciprocity

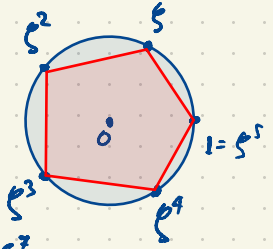
We use the quadratic Gauss sum for p an odd prime:

$\zeta = e^{2\pi i/p}$ primitive p^{th} root of unity $\quad (\zeta^p = 1 \neq \zeta,\ \zeta^{p-1} + \zeta^{p-2} + \cdots + \zeta^2 + \zeta + 1 = 0)$

ζ root of $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1)$

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

$$S = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right)\zeta^k = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right)\zeta^k \qquad \text{quadratic Gauss sum}$$



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

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

Lemma If S is the quadratic Gauss sum (defined above) then $S^2 = \pm p = \left(\frac{-1}{p}\right)p$ if $p \equiv 1 \bmod 4$, $\ldots 3 \ldots$

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

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

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:

$$S^2 = \left[\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\zeta^k\right]\left[\sum_{l=0}^{p-1}\left(\frac{l}{p}\right)\zeta^l\right]$$

$$= \sum_{k=1}^{p-1}\sum_{l=0}^{p-1}\left(\frac{kl}{p}\right)\zeta^{k+l}$$

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

$$= \sum_{k=1}^{p-1}\sum_{m=0}^{p-1}\left(\frac{k^2m}{p}\right)\zeta^{k+km}$$

$$\left(\frac{k^2m}{p}\right) = \left(\frac{k^2}{p}\right)\left(\frac{m}{p}\right) = \left(\frac{m}{p}\right)$$

$$= \sum_{k=1}^{p-1}\sum_{m=0}^{p-1}\left(\frac{m}{p}\right)\zeta^{(m+1)k}$$

$$= \sum_{m=0}^{p-1}\left(\frac{m}{p}\right)\sum_{k=1}^{p-1}\zeta^{(m+1)k}$$

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

When $0 \le m \le p-2$, the inner sum is $\zeta + \zeta^2 + \cdots + \zeta^{p-1} = -1$
($m+1$ nonzero integer mod p)

ie. $1 + \zeta + \zeta^2 + \cdots + \zeta^{p-1} = 0$

$$= \underbrace{(p-1)\left(\frac{-1}{p}\right)}_{\text{for } m=p-1} - \underbrace{\left[\left(\frac{0}{p}\right) + \left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \cdots + \left(\frac{p-2}{p}\right)\right]}_{\text{for } 0 \le m \le p-2}$$

$$\sum_{k=0}^{p-1}\left(\frac{k}{p}\right) = \left(\frac{0}{p}\right) + \left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \cdots + \left(\frac{p-1}{p}\right) = 0$$

one term is 0

$\frac{p-1}{2}$ terms equal $+1$ (for k nonzero squares)

$\frac{p-1}{2}$ terms equal -1 (for k nonsq)

$$= (p-1)\left(\frac{-1}{p}\right) - \left[\left(\frac{1}{p}\right)\right] = \left(\frac{-1}{p}\right)p. \qquad \square$$

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

Use Binomial Theorem $(x+y)^q = x^q + qx^{q-1}y + \frac{q(q-1)}{2}x^{q-2}y^2 + \cdots + qxy^{q-1} + y^q$

Complete the proof of Quadratic Reciprocity: use $q \equiv 0 \mod q$.

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

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

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

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

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

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

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

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

± 1 ± 1 ± 1

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

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

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

Multiply both sides by S

$S^q \equiv \left(\sum_{k=0}^{p-1}\left(\frac{k}{p}\right)\zeta^k\right)^q \equiv \sum_{k=0}^{p-1}\left(\frac{k}{p}\right)^q\zeta^{kq}$ by above ("Freshman's Dream")

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

$= \sum_{\ell=0}^{p-1}\left(\frac{\ell q}{p}\right)\zeta^{\ell} = \sum_{\ell=0}^{p-1}\left(\frac{\ell}{p}\right)\left(\frac{q}{p}\right)\zeta^{\ell} = \left(\frac{q}{p}\right)\underbrace{\sum_{\ell=0}^{p-1}\left(\frac{\ell}{p}\right)\zeta^{\ell}}_{S}$

Multiply both sides by S

$S^2 = \pm p \not\equiv 0 \mod q$

since q is an odd prime.

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

Modular forms & elliptic curves N. Koblitz

We'll start with elementary treatment of elliptic curves.

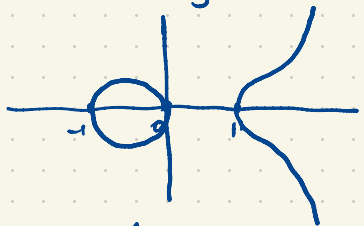
Let F be a field. The solutions $(x,y) \in F^2$ of $y^2 = f(x) = ax^3+bx^2+cx+d$ $(a,b,c,d \in F)$ where $\gcd(f(x), f'(x)) = 1$ form an elliptic curve.

First caveat: Elliptic curves can be expressed in a more general form but after "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.

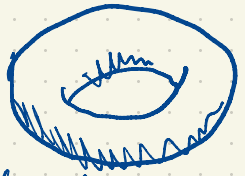
General fact: The points of any elliptic curve form an abelian group.

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

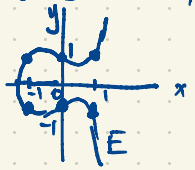


torus

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



Symmetric about x-axis:

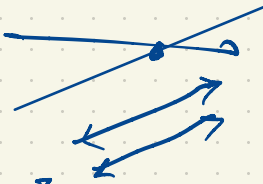
$(x,y) \in E \iff (x,-y) \in E$.

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

$(0, \pm 1)$, $(\pm 1, \pm 1) \in E$

$(5, \pm 11)$, $(3, \pm 5) \in E$ $\quad 11^2 = 121$; $5^3 - 5 + 1 = 121$

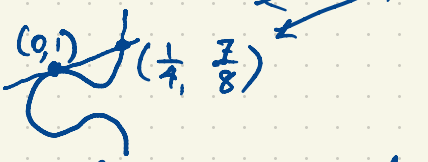
Any other rational points on E?



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



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

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

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

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

$0 = x^3 - 4x^2 + 3x = x(x-1)(x-3)$ gives $(3,-5) \in E$

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

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

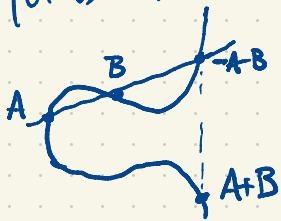
$2y' = -1$

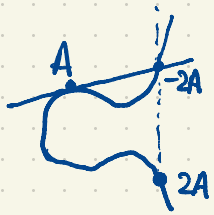
Solve $\begin{cases} y = 1 - \frac{x}{2} \\ y^2 = x^3 - x + 1 \end{cases}$ $\quad (1 - \frac{x}{2})^2 = x^3 - x + 1$

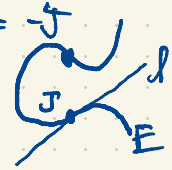
$1 - x + \frac{x^2}{4} = x^3 - x + 1$

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

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







l 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

$J=\left(\frac{1}{13}, \quad\right)$ not a rational point.

$$y^2 = x^3 - x + 1 = \frac{1}{3\sqrt{3}} - \frac{1}{13} + 1$$
$$= 1 - \frac{2}{3\sqrt{3}}$$
$$= \frac{3\sqrt{3}-2}{3\sqrt{3}}$$
$$(1-\sqrt{3})^2 = 4 - 2\sqrt{3}$$

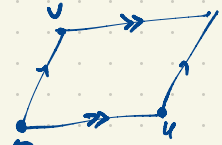
The identity element O is the unique point of E at infinity

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 $E(\mathbb{Q})$

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

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 Weierstass elliptic functions $\wp, \wp'$



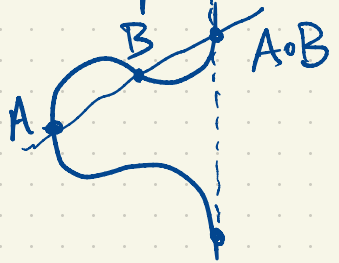
$L = \mathbb{Z}u + \mathbb{Z}v \subset \mathbb{R}^2$

$\mathbb{R}^2/L = T^2 = \text{torus}$

$\cong E(\mathbb{R})$

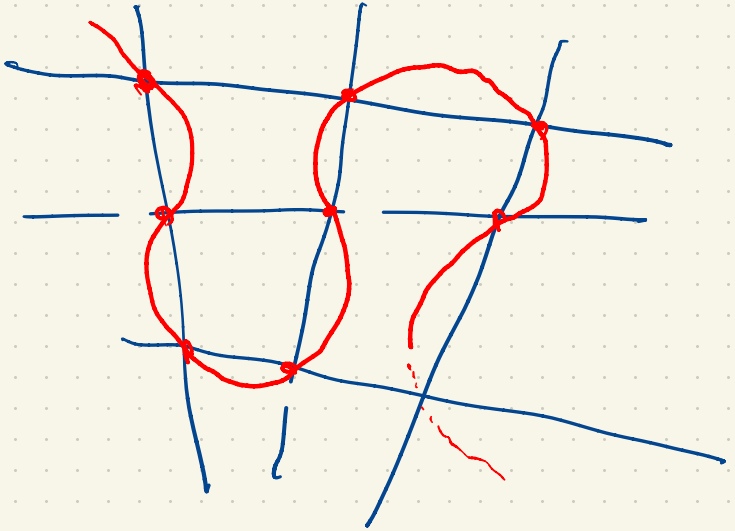
- More insight:

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		
2	2	± 1
3	0	0
4	1	± 1

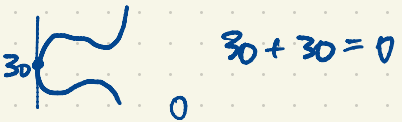
no solutions

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

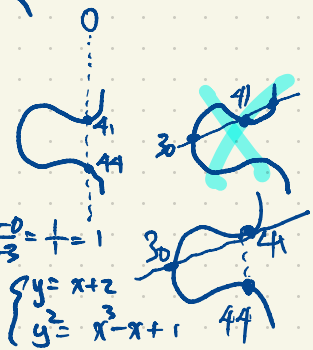
"01" "04" "11, 14, 41, 44" "30"

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

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



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



Eg. $41 + 44 = O$

$41 + 30 = 44$

slope of secant joining 41, 30: $\frac{1-0}{4-3} = \frac{1}{1} = 1$

Secant line: $y = x + 2$

$$\begin{array}{r} x+1 \\ x^2-2x+2 \overline{)\, x^3 - x^2 + 2} \\ x^3 - 2x^2 + 2x \\ \hline x^2 - 2x + 2 \\ x^2 - 2x + 2 \\ \hline 0 \end{array}$$

$\begin{cases} y = x+2 \\ y^2 = x^3 - x + 1 \end{cases}$

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

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

$0 = x^3 - x^2 + 2$

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

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

Also over $\mathbb{F}_5$ consider the elliptic curve $y^2 = x^3 + x + 1$

x	x^3+x+1	y
0	1	± 1
1	3	
2	1	± 1
3	1	± 1
4	4	± 2

The elliptic curve has nine points so $E(\mathbb{F}_5)$ is a group of order 9

$E(\mathbb{F}_5) = \{O, 01, 04, 21, 24, 31, 34, 42, 43\}$

Cyclic of order 9? (C_9) or elementary abelian? ($C_3 \times C_3$)

How many points are on an elliptic curve over a finite field $\mathbb{F}_q$, $q = p^k$, p prime, $k \geq 1$?

$E: y^2 = f(x) = x^3 + ax^2 + bx + c$

The number of points on $E(\mathbb{F}_p)$ is $|E(\mathbb{F}_p)| = p + 1 + \sum_{x=0}^{p-1} \left(\frac{f(x)}{p}\right)$

identify O = point at infinity

Expect $|E(\mathbb{F}_p)| \approx p+1 \pm c\sqrt{p}$

Actually: $|E(\mathbb{F}_q)| \in [q - 2\sqrt{q}, q + 2\sqrt{q}]$

$||E(\mathbb{F}_q)| - (q+1)| \leq 2\sqrt{q}$ Hasse-Weil Bound

$= 1 + \sum_{x=0}^{p-1} \left[\left(\frac{f(x)}{p}\right) + 1\right]$

no. of square roots of $f(x)$ in $\mathbb{F}_p$.

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

p	$\lvert E(\mathbb{F}_p)\rvert$	HW bounds
5	8	[2, 10]
7	12	[3, 13]
11	10	[6, 18]
13	19	[7, 21]
17	14	[10, 26]
19	22	[17, 28]
29	37	[20, 40]
31	35	[21, 43]
37	36	[26, 50]
23	23	but $E(\mathbb{F}_{23})$ is not elliptic curve; it has genus 0.

Elliptic curves are curves of genus $g = 1$.

HW bound: For an irreducible curve X of degree d and genus g, the number of points over $\mathbb{F}_q$ is in the interval $[q+1 - 2g\sqrt{q},\ q+1+2g\sqrt{q}]$

$$|X(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}$$