Class Groups - Outline of course

Ideal class groups in special case of imaginary quadratic fields. All results true in greater generality.

- Sketch proof of the Dirichlet class number formula, and some bounds and estimates for the class number.
- Two recent applications motivated by computational number theory and cryptography.

Reading:

- H. P. F. Swinnerton-Dyer, A brief guide to algebraic number theory.
- D. Cox, Primes of the form $x^2 + ny^2$.
- H. Cohen, A Course in Computational Algebraic Number Theory

Basic definitions for reference

- Let R be a commutative ring with a multiplicative identity 1, e.g., $R = \mathbb{Z}$.
- Let R be an *integral domain* (i.e., $ab = 0$ for $a, b \in R$ if and only if $a = 0$ or $b = 0$).
- An *ideal* is a non-empty subset $I \subseteq R$ such that I is a group under addition and

  $$\sum_{i=1}^{m} a_i r_i \quad \in \quad I$$

  for any $m \in \mathbb{N}$, $a_i \in I$ and $r_i \in R$ for $1 \leq i \leq m$.
- A standard example of an ideal in $\mathbb{Z}$ is $n\mathbb{Z}$.
- The *zero ideal* is $\{0\}$.
- An ideal I is called *proper* if I is non-zero and $I \neq R$.

Basic definitions for reference

- The ideal generated by $a_1, \ldots, a_n \in R$ is the set $(a_1, \ldots, a_n) = \{\sum_{i=1}^n a_i r_i : r_i \in R\}$. Such an ideal is called *finitely generated*.
- An ideal I is called *principal* if $I = (a)$ for some $a \in R$.
- A proper ideal I in a ring R is *prime* if, for any $a, b \in R$, $ab \in I$ implies $a \in I$ or $b \in I$.
- The *product* of two ideals I and J is

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in I, b_i \in J \right\}.$$

Imaginary quadratic fields

- Let $d \geq 1$ be a square-free integer such that $d \equiv 1 \pmod 4$, and consider $F = \mathbb{Q}(\sqrt{-d})$ and $R = \mathbb{Z}[\sqrt{-d}]$.
- Exercise: R is an integral domain.
- R is the ring of algebraic integers of F.
- The discriminant of F is $D_F = -4d$.
- The *norm* of $u + v\sqrt{-d}$ is $\mathrm{N}(u + v\sqrt{-d}) = u^2 + dv^2$.
- Example: Let $d = 5$ then

$$I = (2, 1+\sqrt{-5}) = \{2\alpha + (1+\sqrt{-5})\beta : \alpha, \beta \in \mathbb{Z}[\sqrt{-5}]\}$$

is an ideal.

Exercise

Let I be an R-ideal.

1. $I \cap \mathbb{Z}$ is an ideal, and so is generated by some integer $a \geq 0$.
2. $I = (0)$ if and only if $a = 0$.
3. $I = (1)$ if and only if $a = 1$.
4. If a is non-zero and $u + v\sqrt{-d} \in I$ then $a \mid \mathrm{N}(u + v\sqrt{-d})$.
5. $I \supseteq (a)$.
6. I a prime ideal implies a is prime.
7. If there is some integer $u > 1$ such that $I \subseteq (u)$, then $I = (u)I'$ for some ideal I' in R.

Ideals in imaginary quadratic fields

If I is a non-zero ideal in R such that $I \not\subseteq (u)$ for any integer $u > 1$ then there are integers a, b such that $I = (a, b + \sqrt{-d})$.
Further, $a \mid (b^2 + d)$.

Exercise: Let I be a prime ideal (hence non-zero and not R). Then either

- $I = (p, \sqrt{-d})$ and $p \mid d$,
- $I = (p)$ and $(\frac{-d}{p}) = -1$,
- $I = (p, \pm b + \sqrt{-d})$ for some integer b such that $b^2 \equiv -d \pmod{p}$.

History of ideals in number fields

- Originates in work of Gauss and Lagrange on quadratic forms and number theoretical problems.
- Also developed in attempt to prove Fermat's last theorem.
- Kummer studied obstruction to unique factorisation in cyclotomic rings and proved unique factorisation of "ideal numbers".
- Dedekind developed the modern concept of ideals.
- As with all good things, class groups found new connections with other areas and took on a life of their own.

Ideal classes

- Let I, J be ideals in R. We define the equivalence relation $I \sim J$ if there exist $\alpha, \beta \in R$ such that $(\alpha)I = (\beta)J$.
- Exercise: $\sim$ is well-defined under multiplication: If $I \sim I'$ and $J \sim J'$ then $IJ \sim I'J'$.
- Consider an ideal $I = (a, b + \sqrt{-d})$ with $\gcd(a, b) = 1$. Define $I^{-1} = (a, -b + \sqrt{-d})$. Then $II^{-1} \sim (1)$.
- The *ideal class group* $\mathrm{Cl}(R)$ is the set of equivalance classes of non-zero ideals with the group operation of multiplication of ideals.

Ideal class group

- Unique factorisation of ideals into prime implies the ideal class group is generated by prime ideals.
- **Lemma:** Let $d \geq 1$ be a square-free integer such that $d \equiv 1 \pmod 4$, and consider $F = \mathbb{Q}(\sqrt{-d})$ and $R = \mathbb{Z}[\sqrt{-d}]$.

  Let r be the number of (odd) prime divisors of d. Then $\mathrm{Cl}(R)[2] = \{x \in \mathrm{Cl}(R) : x^2 = (1)\}$ has order 2^r.
- Proof omitted, but we will see an example later.

Binary quadratic forms

- A *primitive binary quadratic form* is $f(x, y) = ax^2 + bxy + cy^2$, where $a, b, c \in \mathbb{Z}$ satisfy $\gcd(a, b, c) = 1$.
- The *discriminant* of the form is $b^2 - 4ac$.
- We will be concerned with *positive definite* forms, meaning $f(x, y) \geq 0$ for all $x, y \in \mathbb{Z}$, and $f(x, y) = 0$ implies $x = y = 0$.
- A form $f(x, y)$ *represents* an integer m if there are $x, y \in \mathbb{Z}$ such that $f(x, y) = m$.

Binary quadratic form associated to an ideal

Reference: Theorem 7.7, Section 7.B of Cox.

- Let $d > 1$ be a square-free integer such that $d \equiv 1 \pmod 4$.
- Consider an ideal $I = (a, b + \sqrt{-d})$ in $R = \mathbb{Z}[\sqrt{-d}]$ and let $c = (b^2 + d)/a$.
- Associate to I the binary quadratic form $ax^2 + 2bxy + cy^2$ of discriminant $(2b)^2 - 4ac = -4d$.
- The ideal $(1) = \mathbb{Z}[\sqrt{-d}]$ corresponds to the form $x^2 + dy^2$ (i.e., $(a, b, c) = (1, 0, d)$).
- The ideal $I = (2, 1 + \sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$ corresponds to the form $2x^2 + 2xy + 3y^2$.

Exercise

- Define the norm of an ideal I to be $\mathrm{N}(I) = [R : I]$.
- If $I = (a, b + \sqrt{-d})$ then show that
$$f(x, y) = \mathrm{N}(ax + (b + \sqrt{-d})y)/\mathrm{N}(I) = ax^2 + 2bxy + cy^2$$
where $c = (b^2 + d)/a$.
- $f(x, y) = \frac{1}{2}(x, y)A(x, y)^T$ where
$$A = \begin{pmatrix} 2a & 2b \\ 2b & 2c \end{pmatrix}.$$

Reduction of ideals

- Let $I = (a, b + \sqrt{-d})$ with $a \geq 1$ and $c = (b^2 + d)/a$. Associate to I the tuple (a, b, c).
- $I = (a, (b \pm a) + \sqrt{-d})$ has associated tuple $(a, b \pm a, c + a \pm 2b)$.
- $$I\left(\frac{-b + \sqrt{-d}}{a}\right) = (c, -b + \sqrt{-d})$$
  has associated tuple $(c, -b, a)$.
- Applying these rules can reduce any tuple (a, b, c) to satisfy $|b| \leq a/2$ and $a \leq c$.

Reduction

In terms of the matrix

$$A = \begin{pmatrix} 2a & 2b \\ 2b & 2c \end{pmatrix}$$

these two reduction rules correspond to

$$\begin{pmatrix} 1 & 0 \\ \pm 1 & 1 \end{pmatrix} A \begin{pmatrix} 1 & 0 \\ \pm 1 & 1 \end{pmatrix}^T = \begin{pmatrix} 2a & 2(b \pm a) \\ 2(b \pm a) & 2(c + a \pm 2b) \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} A \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^T = \begin{pmatrix} 2c & -2b \\ -2b & 2a \end{pmatrix}.$$

Reduced ideal/form

- Ideal/form is *reduced* if $|b| \leq \frac{1}{2}a$ and $a \leq c$. i.e., $|2b| \leq a \leq c$.
- Exercise: Form reduced means a is the smallest non-zero integer represented by the form.
- Equivalent tuples correspond to forms that represent the same set of integers.
- **Lemma:** Ideal reduced implies $a \leq \sqrt{4d/3}$.

Reduced ideal/form

- Ideal/form is *reduced* if $|b| \leq \frac{1}{2}a$ and $a \leq c$.
  i.e., $|2b| \leq a \leq c$.
- Exercise: Form reduced means a is the smallest non-zero integer represented by the form.
- Equivalent tuples correspond to forms that represent the same set of integers.
- **Lemma:** Ideal reduced implies $a \leq \sqrt{4d/3}$.
- Proof: We have $b^2 \leq (a/2)^2$ and
  $a^2 \leq ac = b^2 + d \leq (a/2)^2 + d$, and so $a \leq \sqrt{4d/3}$.
- **Theorem:** The ideal class group is finite.
- Its order is called the *class number*, denoted $h(-d)$.

Reduced principal ideals

Exercise: Let $I = (a, b + \sqrt{-d})$ be a reduced ideal. Suppose $I = (u + v\sqrt{-d})$ is a principal ideal.

1. Show that $a = u^2 + v^2 d$.
2. Show that $u^2 + v^2 d \leq b^2 + d \leq 4d/3$ and so $|v| \leq 1$.
3. Show that $v \neq 0$, and so $u + v\sqrt{-d} = b + \sqrt{-d}$
4. Show that the tupe corresponding to I is $(a, b, 1)$.
5. Hence show that an ideal I reduces to (1) if and only if I is principal.

Example: Compute $h(-65)$

Let $d = 5 \cdot 13 \equiv 1 \pmod 4$. $\mathbb{Z}[\sqrt{-d}]$ has discriminant $-4d = -260$.

We have $|2b| \le a \le \sqrt{260/3} < \sqrt{87} < 10$ and so $|b| \le 4$.

We are going to try each b in turn, and solve $ac = b^2 + d$ subject to $|2b| \le a \le c$:

Example: Compute $h(-65)$

Let $d = 5 \cdot 13 \equiv 1 \pmod 4$. $\mathbb{Z}[\sqrt{-d}]$ has discriminant $-4d = -260$.

We have $|2b| \leq a \leq \sqrt{260/3} < \sqrt{87} < 10$ and so $|b| \leq 4$.

We are going to try each b in turn, and solve $ac = b^2 + d$ subject to $|2b| \leq a \leq c$:

- $b = 0$: $ac = 65$. Tuples $(a, b, c) = (1, 0, 65), (5, 0, 13)$. Order 1 and 2.

Example: Compute $h(-65)$

Let $d = 5 \cdot 13 \equiv 1 \pmod 4$. $\mathbb{Z}[\sqrt{-d}]$ has discriminant $-4d = -260$.

We have $|2b| \le a \le \sqrt{260/3} < \sqrt{87} < 10$ and so $|b| \le 4$.

We are going to try each b in turn, and solve $ac = b^2 + d$ subject to $|2b| \le a \le c$:

- $b = 0$: $ac = 65$. Tuples $(a, b, c) = (1, 0, 65), (5, 0, 13)$. Order 1 and 2.
- $b = 1$: $ac = 66$. Tuple $(a, b, c) = (2, 1, 33) \sim (2, -1, 33)$ order 2. Tuples $(3, \pm 1, 22), (6, \pm 1, 11)$.

Example: Compute $h(-65)$

Let $d = 5 \cdot 13 \equiv 1 \pmod 4$. $\mathbb{Z}[\sqrt{-d}]$ has discriminant $-4d = -260$.

We have $|2b| \le a \le \sqrt{260/3} < \sqrt{87} < 10$ and so $|b| \le 4$.

We are going to try each b in turn, and solve $ac = b^2 + d$ subject to $|2b| \le a \le c$:

- $b = 0$: $ac = 65$. Tuples $(a, b, c) = (1, 0, 65), (5, 0, 13)$. Order 1 and 2.
- $b = 1$: $ac = 66$. Tuple $(a, b, c) = (2, 1, 33) \sim (2, -1, 33)$ order 2. Tuples $(3, \pm 1, 22), (6, \pm 1, 11)$.
- $b = 2$: $ac = 69$. Try $(a, c) = (3, 23)$, but $|2b| \not\le a$

Example: $h(-65)$

- $b = 3$: $ac = 74$. No solution with $|2b| \leq a \leq c$.

Example: $h(-65)$

- $b = 3$: $ac = 74$. No solution with $|2b| \leq a \leq c$.
- $b = 4$: $ac = 81$. Note $(a, b, c) = (9, 4, 9) \equiv (9, -4, 9)$, so ideal class has order 2.

Example: $h(-65)$

- $b = 3$: $ac = 74$. No solution with $|2b| \leq a \leq c$.
- $b = 4$: $ac = 81$. Note $(a, b, c) = (9, 4, 9) \equiv (9, -4, 9)$, so ideal class has order 2.

Hence the class number of $d = -65$ is 8.
Class group has 4 elements of order dividing 2, so is $C_2 \times C_4$.

Exercises

- $h(-1) = 1$
- $h(-5) = 2$
- $h(-21) = 4$

Computing the class number

- We have an algorithm to compute the class number, which tests $\sqrt{d/3}$ choices for b, factors $b^2 + d$ and counts the ideals.
- This is an exponential-time algorithm in terms of the input size.
- There are better algorithms that exploit the group structure (e.g., baby-step-giant-step or Pollard rho) and factorisation of ideals (e.g., index calculus, Hafner-McCurley).

Class number one

- **Theorem:** (Heegner/Baker/Stark) Let F be an imaginary quadratic field of discriminant D_F. Then $h(D_F) = 1$ if and only if

  $$D_F \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}.$$

  See Section 12.E of Cox.
- **Rabinowicz Theorem**: Let $A \in \mathbb{N}$. All values $n^2 + n + A$ are prime, for $0 \leq n \leq A - 2$, if and only if $h(1 - 4A) = 1$.
  See: `https://dms.umontreal.ca/~andrew/Courses/Chapter4.pdf`

Back of envelope calculation of average class number

Back of envelope calculation of average class number

- Ideal classes correspond to tuples (a, b, c) with $1 \leq a \leq \sqrt{4d/3}$, $|b| \leq a/2$, $a \leq c$, and $b^2 + d = ac$.
- So $\sum_{d=1}^{N} h(-d)$ is the number of all such tuples for $d \leq N$.
- To estimate the sum consider all $|b| \leq \sqrt{N/3}$, $|2b| \leq a \leq \sqrt{4N/3}$, and all $a \leq c \leq (N + b^2)/a$.
- Rough count gives $> cN^{3/2}$ for some constant c.
- So $h(-d)$ should on average be at least $\sqrt{d}$.

Dirichlet class number formula

Let w be the number of units in $\mathbb{Z}[\sqrt{-d}]$, so $w = 2$ when $d > 1$.
Then

$$\frac{2\pi h(-d)}{w\sqrt{d}} = \sum_{n=1}^{\infty} (\tfrac{-4d}{n})\tfrac{1}{n}.$$

For the proof I will follow Chapter 6 of Harold Davenport, Multiplicative Number Theory, Springer GTM 74.

Legendre symbol

Let $p > 2$ be prime and $a \in \mathbb{Z}$.
Define $(\frac{a}{p})$ as:

- 0 if $p \mid a$,
- 1 if there exists a solution to $x^2 \equiv a \pmod{p}$,
- -1 otherwise.

This is *multiplicative*: $a = \prod_i p_i^{e_i}$ implies

$$(\tfrac{a}{p}) = \prod_i (\tfrac{p_i}{p})^{e_i}.$$

Kronecker symbol

Let $n \geq 1$ and $a \in \mathbb{Z}$.
Let $n = \prod_i p_i^{e_i}$.
Define $\left(\frac{a}{n}\right)$ as

$$\left(\frac{a}{n}\right) = \prod_i \left(\frac{a}{p_i}\right)^{e_i}$$

where

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & \text{if } 2 \mid a, \\ 1 & \text{if } a \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } a \equiv \pm 3 \pmod{8}. \end{cases}$$

Dirichlet L-series

- Let $\chi : \mathbb{Z} \to \mathbb{C}$ be a non-constant periodic character such as $\chi(n) = (\frac{-4d}{n})$.
- Define the Dirichlet L-series

$$L(\chi, s) = \sum_{n=1}^{\infty} \chi(n) \frac{1}{n^s}.$$

- Exercise: $\sum_{n=1}^{|4d|} \chi(n) = 0$.
- Since the sums $\sum_{n=1}^{M} \chi(n)$ are bounded, Dirichlet's test shows that the L-series converges for $s > 0$.

More about binary quadratic forms

- Let $f(x,y) = ax^2 + (2b)xy + cy^2$ with $D = (2b)^2 - 4ac$.
- Note: $4af(x,y) = (2ax + 2by)^2 - Dy^2$.
- Lemma 2.5 of Cox: Let $D = 0, 1 \pmod 4$ be an integer and m be an odd integer relatively prime to D. Then m is properly represented by a primitive form of discriminant D if and only if D is a quadratic residue modulo m.
- Proof sketch: Let b be such that $D \equiv b^2 \pmod m$. m odd implies b has same parity as D. So can ensure $D \equiv b^2 \pmod{4m}$. So $D = b^2 - 4mc$ for some c and $mx^2 + bxy + cy^2$ is a form of discriminant D that represents m.

Sketch proof of Dirichlet class number formula

- Fix $d > 0$ and set $F = \mathbb{Q}(\sqrt{-d})$ and $R = \mathbb{Z}[\sqrt{-d}]$.
- Let $f_1, \ldots, f_h$ be quadratic forms corresponding to the $h = h(-d)$ ideal classes.
- For $n \in \mathbb{N}$ define $R(n, f_i)$ to be the number of distinct representations of n by f_i.

  So

  $$R(n, f_i) = \#\{(x, y) : x, y \in \mathbb{Z}_{\geq 0}, f_i(x, y) = n\}.$$

  ("distinct" means counting solutions like $(\pm x)^2$ once.)
- Define $R(n)$ to be

  $$R(n) = \sum_{i=1}^{h} R(n, f_i).$$

Sketch proof of Dirichlet class number formula

- **Lemma:** $R(n)$ is multiplicative.
- Proof: $R(n)$ is number of factorisations of (n) as $I\overline{I}$.

Sketch proof of Dirichlet class number formula

- **Lemma:** $R(n)$ is multiplicative.
- Proof: $R(n)$ is number of factorisations of (n) as $I\bar{I}$.
- **Lemma:** Let p be an odd prime. If $(\frac{D_F}{p}) = 1$ then $R(p) = 2$ and $R(p^k) = k + 1$.
  If $(\frac{D_F}{p}) = -1$ then $R(p) = 0$ and $R(p^2) = 1$.
- Proof: If $(\frac{D_F}{p}) = 1$ then by Lemma 2.5 of Cox above there are two forms that represent p. These correspond to the two non-equivalent ideals I_1 and I_2 such that $(p) = I_1 I_2$.
  Now for ideals of norm p^2 there are three choices: I_1^2, $(p) = I_1 I_2$, and I_2^2. So $R(p^2) = 3$, etc.

Sketch proof of Dirichlet class number formula

- In summary, $R(p^k) = \sum_{j=0}^{k} (\frac{D_F}{p^j})$.
- **Corollary:**

$$R(n) = \sum_{m|n} (\frac{D_F}{m}).$$

Sketch proof of Dirichlet class number formula

- The method of proof is to study $\frac{1}{N}\sum_{n=1}^{N} R(n)$ and take a limit as $N \to \infty$.
- Using the previous formulae we get

$$\frac{1}{N}\sum_{n=1}^{N} R(n) = \frac{1}{N}\sum_{n=1}^{N}\sum_{m \mid n}\left(\frac{D_F}{m}\right)$$

$$= \frac{1}{N}\sum_{m=1}^{N}\left\lfloor \frac{N}{m}\right\rfloor\left(\frac{D_F}{m}\right) \approx \sum_{m=1}^{N}\left(\frac{D_F}{m}\right)\frac{1}{m}.$$

(Meaning of $\approx$ is that there is an error term $+O(\sqrt{N})$.)

- This converges to $L((\frac{D_F}{\cdot}), 1)$ as $N \to \infty$.

Sketch proof of Dirichlet class number formula

- On the other hand $\sum_{n=1}^{N} R(n, f_i)$ for $f_i(x, y) = ax^2 + 2bxy + cy^2$ is counting the number of solutions $(x, y) \in \mathbb{Z}^2$ such that $f_i(x, y) \leq N$.
- It is the number of integer points in an ellipse of area $2\pi N/\sqrt{|D_F|}$.
- This counts all solutions (not "distinct representations") so we get a factor w coming from the units in the ring.
- There are h different forms, so

$$w \sum_{n=1}^{N} R(n) \approx 2\pi h N/\sqrt{|D_F|}.$$

- This completes the proof.

Dirichlet class number formula

Let w be the number of units in $\mathbb{Z}[\sqrt{-d}]$, so $w = 2$ when $d > 1$.

Then

$$\frac{2\pi h(-d)}{w\sqrt{d}} = \sum_{n=1}^{\infty} (\tfrac{-4d}{n})\tfrac{1}{n}.$$

General statement of Dirichlet class number formula

Let K be a number field of degree $n = r_1 + 2r_2$.

Let R_K be the regulator, and w_K the number of units of finite order in $\mathcal{O}_K$.

Let D_K and h_K be the discriminant and class number.

Define the Dedekind zeta function

$$\zeta_K(s) = \sum_{(0) \neq I \subseteq \mathcal{O}_K} \mathrm{N}(I)^{-s}.$$

Then

$$\lim_{s \to 1} (s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} R_K h_K}{w_K \sqrt{|D_K|}}.$$

Lower bounds on class number

(From Ajit Bhand, M Ram Murt, Class Numbers of Quadratic Fields.)

- Hecke showed that a variant of Riemann hypothesis for Dirichlet L-series implies there is some constant c such that $h(-d) > c\sqrt{d}/\log(d)$.
- Deuring/Mordell/Heilbronn: falsity of variants of Riemann hypothesis imply $h(-d)$ tends to infinity.

Upper bounds on class number

- Suffices to upper bound $\sum_{n=1}^{\infty} (\frac{-4d}{n}) \frac{1}{n}$.
- Exercise: Let $S(x) = \sum_{n=1}^{x} (\frac{D}{n})$. Then $|S(x)| \le |D|/2$.
  (There exist sharper bounds.)
- Abel's summation formula then allows to prove

$$\left| \sum_{n=|D|}^{\infty} (\frac{-4d}{n}) \frac{1}{n} \right| < \frac{1}{2}.$$

Upper bounds on class number

- Finally,

$$\sum_{n=1}^{|D|} \left(\tfrac{-4d}{n}\right)\tfrac{1}{n} \le \sum_{n=1}^{|D|} \tfrac{1}{n} \approx \log(|D|).$$

Hence we get the upper bound (taking $w = 2$)

$$h(-d) \le \tfrac{1}{\pi}\sqrt{4d}\log(4d).$$

Which groups occur as class groups?

- Recent survey "Missing class groups and class number statistics for imaginary quadratic fields" by S. Holmin, N. Jones, P. Kurlberg, C. McLeman and K. Petersen.
- Watkins (2003) used the ideas of Goldfeld and Gross-Zagier to give an unconditional resolution of Gauss' class number problem for imaginary quadratic class numbers $h \leq 100$ and found that none of the groups $C_3^3, C_3^4, C_9 \times C_3^2$ occur.
- $F(h) =$ number of fundamental discriminants $d < 0$ of class number h.

  Soundararajan has conjectured

  $c_1 h / \log(h) < F(h) < c_2 h \log(h)$.

Application to cryptography: Groups of unknown order

- Anyone can choose a large prime $p \equiv 1 \pmod 4$ and efficiently compute in $\mathrm{Cl}(\mathbb{Z}[\sqrt{-p}])$.
- It seems to be hard to compute the class number, which is the group order.
- This has various applications that I probably won't go into, such as accumulators, delay functions, certain digital signature schemes, etc.

Computational assumptions

- *Gen*(λ) outputs a "random group of unknown order" in time polynomial in λ that requires $O(\lambda)$ bits to write down.
- **Low order assumption:** There is no efficient algorithm (running in time polynomial in λ) that takes as input the description of a group G output by *Gen*(λ), and outputs a pair (g, d) where the order of g is d and $1 < d < 2^\lambda$.
- **Adaptive root assumption:** There is no efficient algorithm that takes as input the description of a group G from *Gen*, outputs a group element g, receives a random "challenge" prime $1 < \ell < 2^\lambda$, and then outputs $h = g^{1/\ell}$ (i.e., $h^\ell = g$).

Annoying fact about class groups

- As we have seen, an ideal $I = (a, b + \sqrt{-d})$ is represented as a pair of integers (a, b) with $|2b| \leq a \leq \sqrt{4d/3}$.
- So it takes about $\log_2(d)$ bits to represent an ideal.
- But the group size is approx $\sqrt{d}$.
- Ideally we would have a representation of ideal classes that uses $\frac{1}{2}\log_2(d)$ bits
- Elliptic curves have same property, but there is an efficient way to compress group elements.

Compression of class group representations

- Simple idea that doesn't work: Just represent using a, then compute b such that $b^2 \equiv -d \pmod{a}$.
- New solution (Dobson-Galbraith-Smith, 2021): Using continued fractions compute $s, t \in \mathbb{Z}$ such that $|s|, |t| \leq \sqrt{a}$ and $bt \equiv s \pmod{a}$.
- Send (a, t), which takes $\frac{3}{4}\log_2(d)$ bits.
- Receiver knows $s^2 \equiv (bt)^2 \equiv -dt^2 \pmod{a}$, but $0 \leq s^2 \leq a$ so s can be computed and hence b.
- There are a few special cases to deal with. See paper.

Elliptic curves are class groups

- Let $y^2 = f(x)$ be the equation for an elliptic curve E over a field K (e.g., $f(x) = x^3 + Ax + B$).
- Consider the ring $R = K[x,y]/(y^2 - f(x)) \cong K[x][\sqrt{f(x)}]$, which is a Dedekind domain.
- We can consider the ideal class group of R.
- A point $P = (a,b)$ on E corresponds to the ideal $(x-a, y-b) = (x-a, -b+\sqrt{f(x)})$.
- I will now explain that the elliptic curve addition formulae are multiplication and reduction of ideals.
- This gives an "easy" proof of associativity of the group operation.

Elliptic curves are class groups

- Let $P = (a, b)$ and $Q = (c, d)$.
- $(x - a, y - b)(x - a, y + b) = (x - a)$ expresses $(a, b) + (a, -b) = \mathcal{O}$.
- The product $(x - a, y - b)(x - c, y - d)$ is an ideal representing $P + Q$. But it is not reduced.
- First, write it in the form $I = (a(x), b(x) + y)$.
- Recall the ideal reduction rule:

$$I\left(\frac{-b + \sqrt{-d}}{a}\right) = (c, -b + \sqrt{-d}).$$

- The exact same idea reduces the ideal I to an ideal of the form $(x - u, y - v)$, where $(u, v) = P + Q$ for the elliptic curve group law.

Lecture 3

- Introduction to isogenies of elliptic curves.
- Description of action of ideal class group on a certain set, with detailed proofs for my students (that are easier to understand than reading Waterhouse).
- Brief description of the CSIDH isogeny based cryptosystem.
- Overview of the theory of complex multiplication, and sketch explanation of one result needed for the ideal class group action.

Isogeny

- Let E_1, E_2 be elliptic curves. Point at infinity always denoted $\mathcal{O}$.
- An isogeny is a non-constant map $\phi : E_1 \to E_2$ that is both a morphism in the sense of geometry and a group homomorphism.
- An isogeny $\phi : E_1 \to E_2$ has finite kernel $G \subseteq E_1(\overline{\mathbb{F}}_p)$.
- Example (elliptic curves over $\mathbb{C}$): The map $z \mapsto z$ on $\mathbb{C}$ induces

$$\mathbb{C}/\langle 1, \tau \rangle \to \mathbb{C}/\langle 1, \tfrac{1}{2}\tau \rangle$$

Kernel is $\{0, \frac{1}{2}\tau\}$.

Example of an isogeny

- Let $E_1 : y^2 = x^3 + x$ and $E_2 : Y^2 = X^3 - 4X$.
- The point $(0, 0)$ on E_1 has order 2.
- There is an isogeny $\phi : E_1 \to E_2$ with kernel generated by $(0, 0)$, given by the rational function

$$\phi(x, y) = \left(\frac{x^2 + 1}{x} \,,\; y \frac{x^2 - 1}{x^2} \right).$$

- $\phi(\mathcal{O}) = \phi((0, 0)) = \mathcal{O}$.

Multiplication by $[n]$ map

- Example:

$$[n] : E_1 \rightarrow E_1$$

  maps P to $[n](P) = P + P + \cdots + P$ (n times).
- Kernel is $E_1[n]$.
- Note $[0](P) = \mathcal{O}$ is the point at infinity.

Endomorphism ring

- Let E be an elliptic curve over $\mathbb{F}_p$.
- Define
  $\mathrm{End}(E) = \{\text{isogenies } \phi : E \to E \text{ over } \overline{\mathbb{F}}_p\} \cup \{[0]\}$.
- This is a ring, under pointwise addition and composition.
- Additive identity is $[0]$ and multiplicative identity is $[1]$.
- We will work with $\mathrm{End}_{\mathbb{F}_p}(E)$.

Frobenius Map on Elliptic Curves

- Let E be an elliptic curve over $\mathbb{F}_p$.
- Define the Frobenius map $\pi : E \to E$ by $\pi(x, y) = (x^p, y^p)$.
- Note that $\ker(\pi) = \{\mathcal{O}\}$.
- **Fact:** The Frobenius satisfies a degree 2 characteristic polynomial $\pi^2 - t\pi + p = 0$.
- Further $t^2 - 4p < 0$.
- So $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E)$ is an imaginary quadratic ring. To be precise $(a + b\pi)(P) = [a]P + [b]\pi(P)$.

Frobenius Map on Supersingular Elliptic Curves

- A supersingular curve $E/\mathbb{F}_p$ has $p+1$ points. Equivalently $E[p] = \{\mathcal{O}\}$.
- Example: When $p \equiv 2 \pmod{3}$ then $y^2 = x^3 + 1$ is supersingular.
- If E over $\mathbb{F}_p$ is supersingular then $t = 0$ and $\pi^2 = [-p]$.
- If $\gcd(a, p) = 1$ then $(a + b\pi)$ has kernel of size $a^2 + pb^2$.
- Technically there is a notion of *degree* of an isogeny, and $\#\ker(\phi) = \deg(\phi)$ when ϕ is *separable*.

Isogenies from kernels

- Given a finite subgroup $G \subseteq E_1(\overline{\mathbb{F}}_p)$ there exists an elliptic curve E_2 and a (separable) isogeny $\phi : E_1 \to E_2$ with $\ker(\phi) = G$.
- the curve E_2 and the isogeny ϕ are unique up to isomorphism.
- The pair (E_2, ϕ) can be computed using Vélu's formulae.

Action of ideal on supersingular elliptic curves

- Let E over $\mathbb{F}_p$ be supersingular, so $\mathbb{Z}[\sqrt{-p}] \cong \mathbb{Z}[\pi] \subseteq \mathrm{End}(E)$. (Assume $p \equiv 1 \pmod 4$ to be consistent with the previous lectures.)
- Let $I \subseteq \mathbb{Z}[\sqrt{-p}]$ be a non-zero ideal.
- Define

$$\begin{aligned} E[I] &= \cap_{\phi \in I} \ker(\phi) \\ &= \{P \in E(\overline{F}_p) : \phi(P) = \mathcal{O}\ \forall \phi \in I\}. \end{aligned}$$

- Exercise: If $I = (\alpha_1, \alpha_2)$ then $E[I] = \ker(\alpha_1) \cap \ker(\alpha_2)$.

Action of ideal on supersingular elliptic curves

- Recall $E[I] = \cap_{\phi \in I} \ker(\phi)$ where $I \subseteq \mathbb{Z}[\sqrt{-p}]$.
- Define $\phi_I : E \to E_I$ to be the isogeny with kernel $E[I]$.
- Since ϕ_I is an isogeny we have $[m] \circ \phi_I = \phi_I \circ [m]$.
- Exercise: Show that if G is a finite subgroup of E then $I(G) = \{a + b\sqrt{-d} : (a + b\sqrt{-d})(G) = \{\mathcal{O}\}\}$ is an ideal in $\mathbb{Z}[\sqrt{-p}]$.

  Waterhouse defines I to be a kernel ideal if $I(E[I]) = I$.

Action of a principal ideal on supersingular elliptic curves

- Let E over $\mathbb{F}_p$ be supersingular, so $\mathbb{Z}[\sqrt{-p}] \cong \mathbb{Z}[\pi] \cong \mathrm{End}_{\mathbb{F}_p}(E)$.
- Let $I = (\alpha) \subseteq \mathbb{Z}[\sqrt{-p}]$ be a non-zero principal ideal.
- Then $E[I] = \ker(\alpha)$ and so $\phi_I : E \to E_I$ is the isogeny with kernel $\ker(\alpha)$.
- Hence $\phi_I = \alpha$ maps E to E.
- In other words, principal ideals map the curve to itself.
- Note that, when α is separable, $\# \ker(\alpha) = \mathrm{N}(\alpha) = \mathrm{N}(I)$. This is called the *degree* of the isogeny.

Exercise: $\pi \circ \phi_I = \phi_I \circ \pi$

- Suppose $\phi : E_1 \to E_2$ where E_1 and E_2 are defined over $\mathbb{F}_p$.
- Write $\phi(P) = (\phi_x(P), \phi_y(P))$.
- In general it is not true that

$$(\phi_x(P)^p, \phi_y(P)^p) = (\phi_x(x_P^p, y_P^p), \phi_y(x_P^p, y_P^p)).$$

- However, $I \subseteq \mathbb{Z}[\pi]$ and so (exercise) $P \in E[I]$ implies $\pi(P) \in E[I]$.
- Since $E[I]$ is Galois-invariant it follows that ϕ_I is Galois-invariant.

Consequences

Let $\phi_I : E \to E_I$.

From $\pi \circ \phi_I = \phi_I \circ \pi$ we deduce:

- $(a + b\pi) \circ \phi_I = \phi_I \circ (a + b\pi)$.
- $\mathbb{Z}[\pi] \subseteq \mathrm{End}_{\mathbb{F}_p}(E_I)$.
  (This is really just saying: E_I is defined over $\mathbb{F}_p$.)

Products of ideals

- **Lemma:** Let E over $\mathbb{F}_p$ be supersingular with $\mathbb{Z}[\sqrt{-p}] \cong \mathbb{Z}[\pi] \cong \mathrm{End}_{\mathbb{F}_p}(E)$.
  Let $I, J \subseteq \mathbb{Z}[\sqrt{-p}]$ be non-zero ideals.
  Then $\phi_{IJ} = \phi_J \circ \phi_I$.

Products of ideals

- **Lemma:** Let E over $\mathbb{F}_p$ be supersingular with $\mathbb{Z}[\sqrt{-p}] \cong \mathbb{Z}[\pi] \cong \mathrm{End}_{\mathbb{F}_p}(E)$.
  Let $I, J \subseteq \mathbb{Z}[\sqrt{-p}]$ be non-zero ideals.
  Then $\phi_{IJ} = \phi_J \circ \phi_I$.
- Proof: Let $I = (\alpha_1, \alpha_2)$ and $J = (\beta_1, \beta_2)$. Then $IJ = (\alpha_i \beta_j : 1 \leq i, j \leq 2)$.
- Let $P \in \ker(\phi_J \circ \phi_I)$.
- Then $\phi_I(P) \in \ker(\phi_J)$ so $\beta_j(\phi_I(P)) = \mathcal{O}$ for all j.
- Then $\phi_I(\beta_j(P)) = \mathcal{O}$ for all j.
- So $\alpha_i(\beta_j(P)) = \mathcal{O}$ for all i, j.
- Hence $P \in \ker(\phi_{IJ})$.

Rest of proof

- The argument is reversible. Let $P \in \ker(\phi_{IJ})$.
- Then $\alpha_i(\beta_j(P)) = \mathcal{O}$ for all i, j.
- So $\phi_I(\beta_j(P)) = \mathcal{O}$ for all j.
- So $\beta_j(\phi_I(P)) = \mathcal{O}$ for all j.
- So $P \in \ker(\phi_J \circ \phi_I)$.
- Since $\ker(\phi_{IJ}) = \ker(\phi_J \circ \phi_I)$ it follows that $\phi_{IJ} = \phi_J \circ \phi_I$ up to composition with an isomorphism.

Action of a equivalent ideals on supersingular elliptic curves

- Let E over $\mathbb{F}_p$ be supersingular, so $\mathbb{Z}[\sqrt{-p}] \cong \mathbb{Z}[\pi] \cong \mathrm{End}_{\mathbb{F}_p}(E)$.
- Let $I, J \subseteq \mathbb{Z}[\sqrt{-p}]$ be non-zero ideals.
- Suppose $I \sim J$.
- Then there are non-zero $\alpha, \beta \in \mathbb{Z}[\sqrt{-p}]$ with $(\alpha)I = (\beta)J$.
- So

$$E \xrightarrow{\phi_I} E_I \xrightarrow{\alpha} E_I$$

and

$$E \xrightarrow{\phi_J} E_J \xrightarrow{\beta} E_J$$

are the same isogeny.

Degree of isogeny corresponding to an ideal

- Already noted that when $I = (\alpha)$ is principal and α is separable, then $\# \ker(\alpha) = \mathrm{N}(I)$.
- This is true in greater generality: When ϕ_I is separable then $\# \ker(\phi_I) = \mathrm{N}(I)$.
- Quick and dirty way to see this is to let $I = (a, b + \sqrt{-p})$ and note that $I\bar{I} = (a)$ where $\bar{I} = (a, -b + \sqrt{-p})$.
  It is clear that $\deg(\phi_I) = \deg(\phi_{\bar{I}})$.
  And $\mathrm{N}(I\bar{I}) = \mathrm{N}(I)^2$.

Action of ideal class group on supersingular elliptic curves

- Non-equal ideals I, J such that $I \sim J$ give $\phi_I : E \to E_1$ and $\phi_J : E \to E_1$. These are **different** ideals, but to the same curve.
- Hence $\mathrm{Cl}(\mathbb{Z}[\pi])$ acts on the set of supersingular elliptic curves

$$\{E/\mathbb{F}_p : \mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\pi]\}$$

  up to isomorphism.
- An ideal I maps E to $I * E := E_I$, being the image curve of ϕ_I.
- (There is also quaternion stuff, but I am just talking about abelian group action.)

Abelian group action

- This abelian group action is implicit in the theory of complex multiplication.
- It was stated in a computational context by Kohel (1996), and proposed for cryptography by Couveignes (1997, unpublished).
- The idea was rediscovered by Rostovtsev-Stolbunov (2006) and Stolbunov (2010) who specifically mentioned it may resist attack by quantum computers.

  "Besides being interesting from the theoretical point of view, the proposed cryptographic schemes might also have an advantage against quantum computer attacks."

CSIDH (Castryck, Lange, Martindale, Panny, Renes 2018)

- Main point of CSIDH is the choice of prime.
- Let $p = 4\ell_1 \cdots \ell_n - 1$ where ℓ_i are small primes. (The CSIDH paper suggests taking the first 73 odd primes and then $\ell_{74} = 587$.)
- Let X be the set of isomorphism classes of **supersingular** elliptic curves E with j-invariant in $\mathbb{F}_p$. Each such curve has $\mathbb{Z}[\sqrt{-p}]$ in its endomorphism ring.
- The primes ℓ_i all split in $\mathbb{Z}[\sqrt{-p}]$.
- To compute $I * E$ one writes I as a product of powers of the 74 split primes.

Generalised Diffie-Hellman

$N(I) = \prod_{i=1}^{n} \ell_i^{e_i}$

$$\begin{tikzcd}
 & I * E \arrow[dr] & \\
E \arrow[ur] \arrow[dr] & & IJ * E \\
 & J * E \arrow[ur] &
\end{tikzcd}$$

$N(J) = \prod_{i=1}^{n} \ell_i^{f_i}$

Complex multiplication

- Complex multiplication is an important theory. I am not going to do justice to it in this lecture.
- Usually credited to Kronecker, who was studying abelian extensions of imaginary quadratic fields.
- Consider an elliptic curve E as $\mathbb{C}/\langle 1, \tau \rangle$ with $Im(\tau) > 0$.
- What is $\mathrm{End}(E)$?
- We know $\mathbb{Z} \subseteq \mathrm{End}(E)$.
- Anything else should correspond to $z \mapsto \alpha z$ such that $\alpha 1 \in \langle 1, \tau \rangle$ and $\alpha \tau \in \langle 1, \tau \rangle$.

Complex multiplication

- Suppose $\alpha 1 \in \langle 1, \tau \rangle$ and $\alpha\tau \in \langle 1, \tau \rangle$.
- We have $\alpha = a + b\tau$ for some $a, b \in \mathbb{Z}$, and
$$\alpha\tau = (a + b\tau)\tau = c + d\tau$$
for some $c, d \in \mathbb{Z}$.
- Then τ satisfies the quadratic
$$b\tau^2 + (a - d)\tau - c = 0$$
and α satisfies
$$\alpha^2 - (a + d)\alpha + (ad - bc) = 0.$$
- It follows that τ lies in an imaginary quadratic field and that α is an algebraic integer.
- The map $z \mapsto \alpha z$ is called a *complex multiplication*.

Complex multiplication

- Any element τ with $Im(\tau) > 0$ in any imaginary quadratic field gives rise to an elliptic curve $\mathbb{C}/\langle 1, \tau \rangle$ with complex multiplication.
- Suppose $\mathbb{C}/\langle 1, \tau \rangle$ has endomorphism ring containing $\mathbb{Z}[\alpha]$ where $\alpha \in \mathbb{Z}[\sqrt{-d}]$.
- Then $r\langle 1, \tau \rangle \subseteq \langle 1, \tau \rangle$ for all $r \in R = \mathbb{Z}[\sqrt{-d}]$.
- In other words, the lattice $\langle 1, \tau \rangle$ is a fractional ideal for the ring R.
- Every isomorphism class of elliptic curves over $\mathbb{C}$ with complex multiplication corresponds to an ideal class in an imaginary quadratic field.

Complex multiplication

- Fix an imaginary quadratic ring $\mathbb{Z}[\sqrt{-d}]$ of class number h.
- Let $I_1, \ldots, I_d$ be ideals representing the ideal classes.
- Then $\mathbb{C}/I_1, \ldots, \mathbb{C}/I_h$ are non-isomorphic elliptic curves, all with endomorphism ring $\mathbb{Z}[\sqrt{-d}]$.
- If J is an ideal and $I_n J^{-1} \sim I_m$, then

$$\mathbb{C}/I_n \longleftarrow \mathbb{C}/I_n J^{-1} \cong \mathbb{C}/I_m$$

is an isogeny of degree $\mathrm{N}(J)$.
(You really have to think about fractional ideals here.)

Complex multiplication

- Fix an imaginary quadratic ring $R = \mathbb{Z}[\sqrt{-d}]$ of class number h.
- Let $I_1, \dots, I_d$ be ideals representing the ideal classes.
- It follows that the ideal class group $\mathrm{Cl}(\mathbb{Z}[\sqrt{-d}])$ acts transitively on the set of elliptic curves $\mathbb{C}/I_1, \dots, \mathbb{C}/I_h$.

Field of definition, reduction, lifting, etc

- Elliptic curves with complex multiplication are defined over a number field (the Hilbert Class Field), and hence can be reduced modulo p.
- Let h be the class number of $\mathbb{Z}[\sqrt{-p}]$ (where $p \equiv 1 \pmod 4$).
- Then there are h isomorphism classes of elliptic curves over the Hilbert class field, all having endomorphism ring $\mathbb{Z}[\sqrt{-p}]$.
- Reducing modulo p gives h supersingular elliptic curves over $\mathbb{F}_p$.

Field of definition, reduction, lifting, etc

- Conversely (Deuring's lifting theorem), there are not more than h elliptic curves over $\mathbb{F}_p$ with endomorphism ring $\mathbb{Z}[\sqrt{-p}]$.
- Hence there are precisely h isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$ with $\mathrm{End}_{\mathbb{F}_p} = \mathbb{Z}[\sqrt{-p}]$.
- It follows that the action of ideal classes on supersingular elliptic curves is a group of size h acting transitively on a set of size h.