SECOND LECTURE FOR THE RESEARCH SCHOOL CIMPA 2015: "CLASS GROUPS VIA QUADRATIC FORMS"

DANIEL C. MAYER

1. Quadratic forms

Definition 1.1. A homogeneous bivariate polynomial

$$f(X,Y) = aX^2 + bXY + cY^2 \in \mathbb{Z}[X,Y]$$

of degree 2 is called a *binary quadratic form* with integer coefficients, briefly a *form* with symbol $f = (a,b,c)$. The *discriminant* of f is given by

$$d = \Delta(f) = b^2 - 4ac$$

and the so-called *roots* of f by

$$\rho = \frac{-b+\sqrt{d}}{2a} \quad \text{and} \quad \bar{\rho} = \frac{-b-\sqrt{d}}{2a}.$$

A form $f = (a,b,c)$ is called *positive definite* if $d < 0$ and $a > 0$, and it is called *indefinite* if $d > 0$ but d is not a complete square.

Remark 1.1. In the sequel, we exclude *negative definite* forms with $d < 0$ and $a < 0$, and also *degenerate* forms with d a square, in particular neither a nor c will be zero.
Furthermore, since

$$b^2 = d + 4ac \equiv d \mod 4,$$

the coefficient b must have the same parity (i.e. odd or even) as the discriminant d.
We are mainly interested in *primitive* forms having coprime coefficients with $\gcd(a,b,c) = 1$, since otherwise

$$d = b^2 - 4ac = (nb_0)^2 - 4(na_0)(nc_0) = n^2(b_0^2 - 4a_0c_0) = n^2 d_0 \quad \text{with} \quad n > 1$$

is not a *fundamental* discriminant.

Definition 1.2. A positive definite form $f = (a,b,c)$ is called *reduced* if

$$\text{either} \quad -a \le b \le a < c \quad \text{or} \quad 0 \le b \le a = c.$$

Date: April 19, 2015.
2000 *Mathematics Subject Classification.* Primary 11Y40, 11Y65, 14H52, 14K22, 11R37, 11R29, 11R11; Secondary 11Y11, 11Y05.
Key words and phrases. algebraic number theory computations, continued fractions, elliptic curves, complex multiplication, primality, factorization, quadratic fields.

Denote by $h(d)$ the *number of reduced positive definite forms* with fixed discriminant $d < 0$.

Remark 1.2. If f is positive definite and reduced, then $|d| = 4ac - b^2 \geq 4a^2 - a^2 = 3a^2$ and thus

$$\sqrt{\frac{|d|}{3}} \geq a.$$

Definition 1.3. The *roots* of a form $f = (a, b, c)$ with discrimiant $d = b^2 - 4ac \neq 0$ are defined as the complex or real zeros of $f(X, 1) = aX^2 + bX + c$, that is

$$\rho = \frac{-b + \sqrt{d}}{2a} \quad \text{and} \quad \bar{\rho} = \frac{-b - \sqrt{d}}{2a}.$$

Remark 1.3. The root ρ of a reduced positive definite form belongs to the fundamental region

$$\mathbb{F} = \{z \in \mathbb{H} \mid -\frac{1}{2} \leq \mathrm{Re}(z) < \frac{1}{2} \text{ and } |z| \begin{cases} \geq 1 & \text{if } \mathrm{Re}(z) \leq 0, \\ > 1 & \text{if } \mathrm{Re}(z) > 0 \end{cases} \}$$

of the operation of the special linear group $\mathrm{SL}(2, \mathbb{Z})$ on the upper half plane

$$\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) \geq 0\}.$$

Definition 1.4. Two forms $f = (a, b, c)$ and $F = (A, B, C)$ are called *equivalent*, if there exists a unimodular linear transform $x = \alpha X + \beta Y$, $y = \gamma X + \delta Y$ such that $F(X, Y) = f(\alpha X + \beta Y, \gamma X + \delta Y)$. The coefficients of F are then given by

$$A = a\alpha^2 + b\alpha\gamma + c\gamma^2 = f(\alpha, \gamma),$$

$$B = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta,$$

$$C = a\beta^2 + b\beta\delta + c\delta^2 = f(\beta, \delta).$$

Definition 1.5. An indefinite form $f = (a, b, c)$ is called *reduced* if

$$0 < \sqrt{d} - b < 2|a| < \sqrt{d} + b.$$

Denote by $n(d)$ the *number of reduced indefinite forms* with fixed discriminant $d > 0$.

Remark 1.4. An indefinite form f is reduced if and only if

$$0 < b < \sqrt{d} \quad \text{and} \quad \left|2|a| - \sqrt{d}\right| < b.$$

Theorem 1.1. *Each equivalence class of positive definite forms contains a unique reduced form.*

Algorithm 1.1. (Counting reduced positive definite forms)
Input: a negative fundamental discriminant $d < 0$.
Memory: a list L of forms $f = (a, b, c)$.
Initialization:
$L \leftarrow []$
$h \leftarrow 0$
$a \leftarrow 1$
Recursion:

```
while (a ≤ sqrt(|d|/3)) {
    if (0 = d mod 4) b ← 0
    else b ← 1
    while (b ≤ a) {
        c ← |d| + b^2
        if (0 = c mod 4a) {
            c ← c div 4a
            if (c ≥ a) {
                h ← h + 1
                append f = (a, b, c) to L
            } if
            if ((b > 0) and (b < a) and (c > a) {
                h ← h + 1
                append f = (a, −b, c) to L
            } if
        } if
        b ← b + 2
    } while b
    a ← a + 1
} while a
```

Termination: $a > \sqrt{\frac{|d|}{3}}$.
Output:
a list L of all reduced positive definite forms $f = (a, b, c)$ with discriminant $d = b^2 - 4ac < 0$, and the number $h = h(d)$ of all equivalence classes of positive definite forms with discriminant d under the action of $\mathrm{SL}(2, \mathbb{Z})$.
Complexity: $O(d)$ steps.

Algorithm 1.2. (Counting reduced indefinite forms)
Input: a positive fundamental discriminant $d > 0$.
Memory: a list L of forms $f = (a, b, c)$.
Initialization:
$L \leftarrow []$
$n \leftarrow 0$
`if` $(0 = d \mod 4)$ $b \leftarrow 2$
`else` $b \leftarrow 1$
Recursion:
`while` $(b \leq \sqrt{d})$ {
    $a \leftarrow \lfloor \frac{\sqrt{d}-b}{2} \rfloor + 1$
    `while` $(a < \frac{\sqrt{d}+b}{2})$ {
        `if` $(0 = (b^2 - d) \mod 4a)$ {
            $c \leftarrow (b^2 - d)$ div $4a$
            $n \leftarrow n + 2$
            append $f = (a, b, c)$ to L
            append $f = (-a, b, -c)$ to L
        } if
        $a \leftarrow a + 1$
    } while a
    $b \leftarrow b + 2$
} while b
Termination: $b > \sqrt{d}$.
Output:
a list L of all reduced indefinite forms $f = (a, b, c)$ with discriminant $d = b^2 - 4ac > 0$, and the number $n = n(d)$ of all reduced indefinite forms with discriminant d.
Complexity: $O(d)$ steps.

Example 1.1. We determine all reduced positive definite forms $f = (a, b, c)$ for some small discriminants $-15 \le d \le -3$.

(1) $d = -3$: $a \le \sqrt{\frac{|d|}{3}} = \sqrt{\frac{3}{3}} = 1 \Longrightarrow a = 1$,
d odd $\Longrightarrow b \le a = 1$ odd $\Longrightarrow b = 1$,
$|d| + b^2 = 3 + 1 = 4$ divisible by $4a = 4 \Longrightarrow c = \frac{4}{4} = 1$,
$f = (1, 1, 1)$ with root $\xi = \frac{-b+\sqrt{d}}{2a} = \frac{-1+\sqrt{-3}}{2} = \zeta_3$, $|\xi| = 1$, $\mathrm{Re}(\xi) = -\frac{1}{2}$.

(2) $d = -4$: $a \le \sqrt{\frac{|d|}{3}} = \sqrt{\frac{4}{3}} \approx 1.155 \Longrightarrow a = 1$,
d even $\Longrightarrow b \le a = 1$ even $\Longrightarrow b = 0$,
$|d| + b^2 = 4$ divisible by $4a = 4 \Longrightarrow c = \frac{4}{4} = 1$,
$f = (1, 0, 1)$ with root $\xi = \frac{-b+\sqrt{d}}{2a} = \frac{\sqrt{-4}}{2} = \sqrt{-1} = \zeta_4$, $|\xi| = 1$, $\mathrm{Re}(\xi) = 0$.

(3) $d = -7$: $a \le \sqrt{\frac{|d|}{3}} = \sqrt{\frac{7}{3}} \approx 1.528 \Longrightarrow a = 1$,
d odd $\Longrightarrow b \le a = 1$ odd $\Longrightarrow b = 1$,
$|d| + b^2 = 7 + 1 = 8$ divisible by $4a = 4 \Longrightarrow c = \frac{8}{4} = 2$,
$f = (1, 1, 2)$ with root $\xi = \frac{-b+\sqrt{d}}{2a} = \frac{-1+\sqrt{-7}}{2}$, $|\xi| = \sqrt{2}$, $\mathrm{Re}(\xi) = -\frac{1}{2}$.

(4) $d = -8$: $a \le \sqrt{\frac{|d|}{3}} = \sqrt{\frac{8}{3}} \approx 1.633 \Longrightarrow a = 1$,
d even $\Longrightarrow b \le a = 1$ even $\Longrightarrow b = 0$,
$|d| + b^2 = 8$ divisible by $4a = 4 \Longrightarrow c = \frac{8}{4} = 2$,
$f = (1, 0, 2)$ with root $\xi = \frac{-b+\sqrt{d}}{2a} = \frac{\sqrt{-8}}{2} = \sqrt{-2}$, $|\xi| = \sqrt{2}$, $\mathrm{Re}(\xi) = 0$.

(5) $d = -11$: $a \le \sqrt{\frac{|d|}{3}} = \sqrt{\frac{11}{3}} \approx 1.915 \Longrightarrow a = 1$,
d odd $\Longrightarrow b \le a = 1$ odd $\Longrightarrow b = 1$,
$|d| + b^2 = 11 + 1 = 12$ divisible by $4a = 4 \Longrightarrow c = \frac{12}{4} = 3$,
$f = (1, 1, 3)$ with root $\xi = \frac{-b+\sqrt{d}}{2a} = \frac{-1+\sqrt{-11}}{2}$, $|\xi| = \sqrt{3}$, $\mathrm{Re}(\xi) = -\frac{1}{2}$.

(6) $d = -15$: $a \le \sqrt{\frac{|d|}{3}} = \sqrt{\frac{15}{3}} \approx 2.236 \Longrightarrow 1 \le a \le 2$;

- $a = 1$:
  d odd $\Longrightarrow b \le a = 1$ odd $\Longrightarrow b = 1$,
  $|d| + b^2 = 15 + 1 = 16$ divisible by $4a = 4 \Longrightarrow c = \frac{16}{4} = 4$,
  $f_1 = (1, 1, 4)$ with root $\xi = \frac{-b+\sqrt{d}}{2a} = \frac{-1+\sqrt{-15}}{2}$, $|\xi| = 2$, $\mathrm{Re}(\xi) = -\frac{1}{2}$;
- $a = 2$:
  d odd $\Longrightarrow b \le a = 2$ odd $\Longrightarrow b = 1$,
  $|d| + b^2 = 15 + 1 = 16$ divisible by $4a = 8 \Longrightarrow c = \frac{16}{8} = 2$,
  $f_2 = (2, 1, 2)$ with root $\xi = \frac{-b+\sqrt{d}}{2a} = \frac{-1+\sqrt{-15}}{4}$, $|\xi| = 1$, $\mathrm{Re}(\xi) = -\frac{1}{4}$;
  here, we have $b > 0$, $b < a$, but $c = a$, and thus we are done.

This is the first example with $h(-15) = 2$.
Here, f_2 is of order 2 and thus its own inverse.

Example 1.2. We determine all reduced positive definite forms $f = (a, b, c)$ for slightly bigger discriminants $-23 \leq d \leq -19$.

(1) $d = -19$: $a \leq \sqrt{\frac{|d|}{3}} = \sqrt{\frac{19}{3}} \approx 2.517 \Longrightarrow 1 \leq a \leq 2$;

- $a = 1$:
  d odd $\Longrightarrow b \leq a = 1$ odd $\Longrightarrow b = 1$,
  $|d| + b^2 = 19 + 1 = 20$ divisible by $4a = 4 \Longrightarrow c = \frac{20}{4} = 5$,
  $f = (1, 1, 5)$ with root $\xi = \frac{-b+\sqrt{d}}{2a} = \frac{-1+\sqrt{-19}}{2}$, $|\xi| = \sqrt{5}$, $\mathrm{Re}(\xi) = -\frac{1}{2}$;
- $a = 2$:
  d odd $\Longrightarrow b \leq a = 2$ odd $\Longrightarrow b = 1$,
  $|d| + b^2 = 19 + 1 = 20$ not divisible by $4a = 8$ and we are done.

(2) $d = -20$: $a \leq \sqrt{\frac{|d|}{3}} = \sqrt{\frac{20}{3}} \approx 2.582 \Longrightarrow 1 \leq a \leq 2$;

- $a = 1$:
  d even $\Longrightarrow b \leq a = 1$ even $\Longrightarrow b = 0$,
  $|d| + b^2 = 20$ divisible by $4a = 4 \Longrightarrow c = \frac{20}{4} = 5$,
  $f_1 = (1, 0, 5)$ with root $\xi = \frac{-b+\sqrt{d}}{2a} = \frac{\sqrt{-20}}{2} = \sqrt{-5}$, $|\xi| = \sqrt{5}$, $\mathrm{Re}(\xi) = 0$;
- $a = 2$:
  d even $\Longrightarrow b \leq a = 2$ even $\Longrightarrow 0 \leq b \leq 2$;
  (a) $b = 0$:
  $|d| + b^2 = 20$ not divisible by $4a = 8$;
  (b) $b = 2$:
  $|d| + b^2 = 20 + 4 = 24$ divisible by $4a = 8 \Longrightarrow c = \frac{24}{8} = 3$,
  $f_2 = (2, 2, 3)$ with root $\xi = \frac{-b+\sqrt{d}}{2a} = \frac{-2+\sqrt{-20}}{4}$, $|\xi| = \sqrt{\frac{3}{2}}$, $\mathrm{Re}(\xi) = -\frac{1}{2}$;
  here, we have $b > 0$, $c > a$ but $b = a$, and thus we are done.

This is the second example with $h(-20) = 2$. f_2 is of order 2 and thus its own inverse.

(3) $d = -23$: $a \leq \sqrt{\frac{|d|}{3}} = \sqrt{\frac{23}{3}} \approx 2.769 \Longrightarrow 1 \leq a \leq 2$;

- $a = 1$:
  d odd $\Longrightarrow b \leq a = 1$ odd $\Longrightarrow b = 1$,
  $|d| + b^2 = 23 + 1 = 24$ divisible by $4a = 4 \Longrightarrow c = \frac{24}{4} = 6$,
  $f_1 = (1, 1, 6)$ with root $\xi = \frac{-b+\sqrt{d}}{2a} = \frac{-1+\sqrt{-23}}{2}$, $|\xi| = \sqrt{6}$, $\mathrm{Re}(\xi) = -\frac{1}{2}$;
- $a = 2$:
  d odd $\Longrightarrow b \leq a = 2$ odd $\Longrightarrow b = 1$,
  $|d| + b^2 = 23 + 1 = 24$ divisible by $4a = 8 \Longrightarrow c = \frac{24}{8} = 3$,
  $f_2 = (2, 1, 3)$ with root $\xi = \frac{-b+\sqrt{d}}{2a} = \frac{-1+\sqrt{-23}}{4}$, $|\xi| = \frac{\sqrt{6}}{2}$, $\mathrm{Re}(\xi) = -\frac{1}{4}$;
  here, we have $b > 0$, $b < a$, $c > a$, and thus we additionally get
  $f_3 = (2, -1, 3)$ with root $\xi = \frac{-b+\sqrt{d}}{2a} = \frac{1+\sqrt{-23}}{4}$, $|\xi| = \frac{\sqrt{6}}{2}$, $\mathrm{Re}(\xi) = \frac{1}{4}$.

This is the first example with $h(-23) = 3$. Here, f_2 is of order 3 with inverse $f_3 = f_2^{-1}$.

References

[1] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[2] W. Bosma, J. J. Cannon, C. Fieker, and A. Steels (eds.), *Handbook of Magma functions* (Edition 2.21, Sydney, 2015).

[3] H. Cohen, *A course in computational algebraic number theory*, Graduate texts in mathematics **138**, Springer, 1996.

[4] H. Cohen, *Advanced topics in computational number theory*, Graduate texts in mathematics **193**, Springer, 2000.

[5] The GAP Group, *GAP – Groups, Algorithms, and Programming — a System for Computational Discrete Algebra*, Version 4.7.7, Aachen, Braunschweig, Fort Collins, St. Andrews, 2015, (`http://www.gap-system.org`).

[6] The MAGMA Group, *MAGMA Computational Algebra System*, Version 2.21-3, Sydney, 2015, (`http://magma.maths.usyd.edu.au`).

[7] Oracle, *JDK* 7u80, *Java SE*, and *NetBeans*, Version 8.0.2, Redwood City, CA, 2015, (`http://www.oracle.com`).

[8] The PARI Group, *PARI/GP*, Version 2.7.3, Bordeaux, 2015, (`http://pari.math.u-bordeaux.fr`).

[9] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Encyclopedia of mathematics and its applications, Cambridge University Press, 1990.

[10] S.S. Wagstaff, Jr., *The Joy of Factoring*, Student Mathematical Library (STML), Vol. **68**, American Mathematical Society (AMS), 2013.

Naglergasse 53, 8010 Graz, Austria
E-mail address: `algebraic.number.theory@algebra.at`
URL: `http://www.algebra.at`