

## EXERCISES ON BINARY QUADRATIC FORMS

JEFFREY STOPPLE

These are mostly computational exercises to help you understand the theorems in Chapter One of [Cox] ‘Primes of the form  $x^2 + ny^2$ ’. Section numbers like §1B below refer to the corresponding sections in Chapter One.

**Notation.** The acronym BFI stands for ‘brute force and . . . ignorance’, i.e. direct computation. We sometimes write a binary quadratic form

$$F(x, y) = ax^2 + bxy + cy^2 \quad \text{as} \quad \{a, b, c\}$$

suppressing the variables for convenience. The discriminant  $d = b^2 - 4ac$  is assumed to be  $< 0$  in these notes.

**Technology.** The arithmetic can be tedious to do by hand, and a calculator uses ‘floating point’ numbers, rounded off approximations to real numbers. The calculator will give wrong answers to integer arithmetic when the integers are moderately large. Instead, use a package like *Mathematica*, Maple, or PARI. These notes refer to PARI, since it is free. You can download PARI at

<http://pari.math.u-bordeaux.fr/download.html>

Be sure to get the Binary version if you have a Windows machine, Stable version if you have Linux or Mac OS X. There is also an online PARI calculator at

<http://modular.math.washington.edu/cgi-bin/calc/calc.py>

### §1B.

**Exercise 1.** ‘Reciprocity’ and ‘Descent’ in Fermat’s proof that  $p \equiv 1 \pmod{4}$  can be written  $x^2 + y^2$  (Thm 1.2).

- (1) For some primes, only the Reciprocity step is needed, no Descent. This can be true when, in searching for  $a$  such that  $p$  divides  $a^2 + 1$ , you find that  $p$  is actually equal  $a^2 + 1$  for some integer  $a$ . Find a  $a$  so that  $p = a^2 + 1$  for  $p = 2, 5, 17, 37, 101$ .
- (2) For some primes, a single Descent step is necessary. For  $p = 13, 29$ ,

---

stopple@math.ucsb.edu.

- (a) Find an  $a$  so that  $p$  divides  $N = a^2 + 1$  (Reciprocity). Factor  $N$ .
- (b) With  $q$  the smaller prime factor of  $N$ , use the representation  $q = x^2 + y^2$  you found above to write  $p = N/q$  as  $c^2 + d^2$ . The proof of Thm 1.2 tells you how.
- (3) For some primes, more than one Descent step is necessary. Carry out the steps for  $p = 293$ . The Reciprocity step may be tedious to do by hand, but is trivial with the PARI command

```
for(a=1,146,print(a" "(a^2+1)/293))
```

Remember, the point of this exercise is to understand the proof of Thm 1.2, not merely to find the representation as a sum of two squares, which can sometimes be done by inspection.  $\square$

**Exercise 2.** ‘Reciprocity’ and ‘Descent’ in Euler’s proof that  $p \equiv 1, 3 \pmod{8}$  can be written  $x^2 + 2y^2$ .

- (1) Find an  $a$  so that  $p = a^2 + 2$  for  $p = 3, 11, 83$ . (This is the case where you need no Descent steps.)
- (2) Find an  $a$  so that  $p = 17$  divides  $a^2 + 2$ . Carry out one Descent step to write  $17 = c^2 + 2d^2$ . The solution to exercise 1.3a in [Cox] tells you how.
- (3) Find an  $a$  so that  $p = 233$  divides  $a^2 + 2$ . Carry out two Descent steps to write  $233 = c^2 + 2d^2$ .

Remember, the point of this exercise is to understand the proof, not merely to find the representation as a square plus twice a square, which can sometimes be done by inspection.  $\square$

### §1C.

**Exercise 3.** Euler’s Conjecture 1.9 on Quadratic Reciprocity.

- (1) For  $q = 11, 4q = 44$ . Find an odd prime  $p$  in each of the classes

$$\pm 1, \pm 9, \pm 25, \pm 49, \pm 81 \pmod{44}.$$

Note that  $\pm 25 = \mp 19$ ,  $\pm 49 = \pm 5$ , and  $\pm 81 = \mp 7 \pmod{44}$ . The first few odd primes are

3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59,

61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127 . . .

- (2) For each prime  $p$  you found above, verify that

$$\left(\frac{11}{p}\right) = 1,$$

and that

$$\left(\frac{11}{p'}\right) = -1$$

for the other primes  $p'$  not in square classes mod 44. You may compute each Legendre symbol with a single 'flip' using Quadratic Reciprocity and lookup in a table modulo 11 if you like.

□

**Exercise 4.** There is more than one form with discriminant  $-84$ .

- (1) Do exercise 1.15 in [Cox], which says to use Quadratic Reciprocity to determine which classes  $[p]$  in

$$(\mathbb{Z}/84)^*$$

have  $\chi([p]) = 1$ .

- (2) The binary quadratic forms

$$x^2 + 21y^2, \quad 3x^2 + 7y^2, \quad 2x^2 + 2xy + 11y^2, \quad 5x^2 + 4xy + 5y^2$$

all have discriminant  $-84$ . For odd primes  $p$  different from 3, 7, try to determine congruences modulo 84 which tell you which forms represent which primes. The PARI code below may be of use:

```
{forprime(p=1, 500, if(kronecker(-84, p)==1,
print(p" "Mod(p, 84)" "qfbred(qfbprimeform(-84, p))))})}
```

□

**Exercise 5.** This is a continuation of exercise 4.

- (1) Show by BFI that the classes  $\{1, 25, 37\}$  form a subgroup  $H$  of the multiplicative group  $(\mathbb{Z}/84)^*$ .
- (2) Show that  $H$  is a subgroup of  $\ker(\chi_{-84})$ . That is, show that  $\chi_{-84}(h) = 1$  for each  $h$  in  $H$ .
- (3) Show that  $H$  is the subgroup of squares in  $(\mathbb{Z}/84)^*$ . Hint: Any square modulo  $84 = 12 \cdot 7$  is a square in  $(\mathbb{Z}/12)^*$  and also a square in  $(\mathbb{Z}/7)^*$ . What are the squares in these groups? Reduce the elements of  $H$  modulo 12 and 7 and compare.
- (4) What are the elements in the cosets

$$[5] \cdot H, \quad [11] \cdot H, \quad [19] \cdot H,$$

and how do they relate to the classes modulo 84 represented by the forms

$$3x^2 + 7y^2, \quad 2x^2 + 2xy + 11y^2, \quad 5x^2 + 4xy + 5y^2?$$

□

§2A. exercise 2.3 in [Cox], which says equivalent forms have the same discriminant, is a tedious direct calculation. Instead, we use the fact that in matrix language

$$F(x, y) = ax^2 + bxy + cy^2 = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

and  $F' \sim F$  via a matrix  $M$ , if

$$F'(x, y) = F((x, y)M).$$

Thus

$$\begin{aligned} F'(x, y) &= \begin{bmatrix} x & y \end{bmatrix} M \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} {}^{tr}(\begin{bmatrix} x & y \end{bmatrix} M) \\ &= \begin{bmatrix} x & y \end{bmatrix} M \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} {}^{tr}M \begin{bmatrix} x \\ y \end{bmatrix} \end{aligned}$$

where  ${}^{tr}M$  denotes the transposed matrix.

**Exercise 6.** Show that equivalent forms have the same discriminant  $d$ . Hint: how does the discriminant of  $F$  relate to the determinant of the matrix above?  $\square$

Multiplication shows that

$$4a(ax^2 + bxy + cy^2) = (2ax + by)^2 + (4ac - b^2)y^2.$$

If  $d = b^2 - 4ac < 0$ , the expression on the right is always positive. This means that  $ax^2 + bxy + cy^2$  always has the same sign as the constant  $a$ . In other words, a form with negative discriminant represents only positive numbers or only negative numbers. There is obviously a close connection between the cases; the range of values of  $\{a, b, c\}$  is the negative of the range of values of  $\{-a, -b, -c\}$ . For this reason, we will now consider only forms which represent positive integers. Such forms are called POSITIVE DEFINITE; they have  $a > 0$ . Since  $\{a, b, c\}$  is equivalent to  $\{c, -b, a\}$  by  $(x, y) \rightarrow (-y, x)$ , this latter form also represents only positive integers, and so its first coefficient  $c$  is also positive.

A key fact in the theory is that for a fixed  $d$ , the number of equivalence classes of forms with discriminant  $d$  is finite. We define  $h$  the CLASS NUMBER to be the number of equivalence classes. We provide below alternate simpler proofs of Theorems 2.8 and 2.13 in [Cox]. (This material is stolen from [Stopp], who stole it from [Oesterlé].)

**Theorem.** For each  $d < 0$  the class number  $h$  is finite. In fact, every form is equivalent to a form  $\{a, b, c\}$  with

$$|b| \leq a \leq c.$$

This is (part of) Theorem 2.8 in [Cox].

*Proof.* The proof of the theorem consists of showing that, if the inequality fails to hold, we can find an equivalent form which reduces the sum of the first and last coefficients. This process can be repeated only a finite number of times since there are only finitely many positive integers less than  $a + c$ .

So, let  $\text{sgn}(b) = \pm 1$  be the sign of  $b$ , then  $\text{sgn}(b)b = |b|$ . If  $a < |b|$ , the matrix

$$\begin{bmatrix} 1 & 0 \\ -\text{sgn}(b) & 1 \end{bmatrix} \text{ changes } (x, y) \text{ to } (x - \text{sgn}(b)y, y).$$

The corresponding form is

$$\begin{aligned} a(x - \text{sgn}(b)y)^2 + b(x - \text{sgn}(b)y)y + cy^2 = \\ ax^2 + (b - 2\text{sgn}(b)a)xy + (a + c - |b|)y^2. \end{aligned}$$

We have that  $a + (a + c - |b|) < a + c$ , because  $a < |b|$ .

**Exercise 7.** Show that, in the case  $c < |b|$ , the matrix

$$\begin{bmatrix} 1 & -\text{sgn}(b) \\ 0 & 1 \end{bmatrix}$$

similarly reduces the sum of the first and last coefficients.  $\square$

Eventually, both  $a$  and  $c$  are  $\geq |b|$ , and the matrix  $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$  interchanges  $a$  and  $c$  if necessary. This proves the inequality claimed above.

Next we show that there are only finitely many such triples with discriminant  $d$ . The inequalities for  $a$ ,  $|b|$ , and  $c$  imply that

$$3a^2 = 4a^2 - a^2 \leq 4ac - b^2 = -d = |d|.$$

This means  $a \leq \sqrt{|d|/3}$  and  $|b| \leq a \leq \sqrt{|d|/3}$ . Also,  $b^2 - 4ac = d$  implies  $b^2 \equiv d \pmod{4}$ , and thus  $b \equiv d \pmod{2}$ . In other words  $b$  is odd if and only if  $d$  is. There are only finitely many choices for  $a$  and  $b$ , and  $c$  is then completely determined by the discriminant equation;  $c = (b^2 - d)/(4a)$ .

The theorem not only proves the class number is finite, but gives an upper bound. Here is an example with  $d = -35$ . We have  $\sqrt{|d|/3} = 3.41565\dots$ , so  $|b| \leq 3$  and  $1 \leq a \leq 3$ . Also,  $b$  must be odd as  $d$  is, so  $b$  is restricted to  $-3, -1, 1, 3$ . With  $b = \pm 1$ ,  $b^2 - d$  is 36. We only

get a form when  $c = (b^2 - d)/(4a)$  is an integer. The choice  $a = 1$  gives rise to the forms  $\{1, \pm 1, 9\}$ . The choice  $a = 2$  gives  $c = 36/8$ ; not an integer. The choice  $a = 3$  gives rise to the forms  $\{3, \pm 1, 3\}$ . Meanwhile if  $b = \pm 3$  then  $a \geq |b|$  must be 3, and  $c = 44/12$  is not an integer. The class number is less than or equal to 4.

**Exercise 8.** Carry out this same analysis with discriminant  $-23$  to get a bound on the class number.  $\square$

In fact the proof above gives even more. It actually gives an algorithm for finding a representative of a class which satisfies the inequalities. For example, the form  $\{33, -47, 17\}$  has discriminant  $-35$ , but  $47 > 33$  so the theorem says to replace  $(x, y)$  by  $(x + y, y)$ , which gives  $\{33, 19, 3\}$ . We chose the sign '+' because  $b$  was negative. Now  $19 > 3$ , so the theorem says to change  $(x, y)$  to  $(x, y - x)$  which gives  $\{17, 13, 3\}$ . Again  $13 > 3$  so the same variable change produces  $\{7, 7, 3\}$  and then  $\{3, 1, 3\}$ , which can be reduced no further since the inequality  $1 \leq 3 \leq 3$  is satisfied. Notice that the sum of the first and last entry decreases at each step:

$$33 + 17 > 33 + 3 > 17 + 3 > 7 + 3 > 3 + 3.$$

**Exercise 9.** Carry out this algorithm with the form

$$F(x, y) = 12x^2 + 11xy + 3y^2$$

which has discriminant  $-23$ . Also, at each step of the reduction, compute the sum of the first and last coefficients to see that it really does decrease at each step. Do the same for

$$G(x, y) = 39x^2 + 43xy + 12y^2 \quad \text{and}$$

$$H(x, y) = 93x^2 + 109xy + 32y^2,$$

which also both have discriminant  $-23$ .  $\square$

We now have a bound on the class number, but we want to know it exactly. The question is, can two forms with the same discriminant satisfying the inequality of the theorem be equivalent to each other? To answer this, we will need the following lemma.

**Lemma (Fundamental Inequalities).** Suppose the quadratic form

$$F(x, y) = ax^2 + bxy + cy^2$$

satisfies  $|b| \leq a \leq c$ . Then  $a$  is the minimum of  $F$ , that is, for all  $(x, y) \neq (0, 0)$ ,

$$F(x, y) \geq a.$$

Furthermore,  $ac$  is the minimum of products of values of  $F$ . In other words for all pairs of lattice points  $(x, y)$  and  $(u, v)$  with  $(x, y)$  and  $(u, v)$  not colinear,

$$F(x, y)F(u, v) \geq ac.$$

*Proof.* It is easy to see that  $F$  actually does represent  $a$ , since  $a = F(1, 0)$ . Similarly  $F(1, 0)F(0, 1) = ac$ . If  $x \neq 0$ ,

$$(1) \quad F(x, 0) = ax^2 \geq a.$$

Similarly if  $y \neq 0$

$$(2) \quad F(0, y) = cy^2 \geq c,$$

and  $c \geq a$ . In the general case neither  $x$  nor  $y$  is 0. We see that

$$\begin{aligned} F(x, y) &= ax^2 + bxy + cy^2 \\ &\geq ax^2 - |b||x||y| + cy^2 \\ &\geq ax^2 - |b||x||y| + cy^2 - a(x - y)^2 \\ &= (2a - |b|)|x||y| + (c - a)y^2 \\ (3) \quad &\geq (2a - |b|) + (c - a) = a + c - |b| \geq c \end{aligned}$$

since  $a \geq |b|$ . This proves that  $a$  is the minimum value. Suppose we have two lattice points which are not colinear. They can not both lie on the horizontal axis. Thus one of the inequalities (2) or (3) must hold, and the product  $F(x, y)F(u, v) \geq ac$ .

Now we are ready to tell whether forms satisfying the usual inequalities are equivalent. Almost always they are distinct; the only ambiguity is that  $\{a, b, c\} \sim \{a, -b, c\}$  if  $b = 0$  (which is trivial), if  $|b| = a$  or if  $a = c$ . We will state this more precisely.

**Theorem.** *Every form with discriminant  $d$  is equivalent to exactly one form satisfying the inequalities*

$$(4) \quad |b| \leq a \leq c \quad \text{and} \quad b \geq 0 \quad \text{if either } |b| = a, \text{ or if } a = c.$$

This is (the rest of) Theorem 2.8 and also Theorem 2.13 in [Cox].

*Proof.* First observe that if  $b = 0$ , then  $\{a, b, c\} \sim \{a, -b, c\}$  is trivial. If  $a = c$ , then changing  $(x, y)$  to  $(-y, x)$  shows that  $\{a, b, c\} \sim \{c, -b, a\} = \{a, -b, c\}$ . Finally if  $|b| = a$  then we saw in the proof of the last theorem that changing  $(x, y)$  to  $(x - \text{sgn}(b)y, y)$  makes

$$\{a, b, c\} \sim \{a, b - 2\text{sgn}(b)a, a + c - |b|\} = \{a, -b, c\}.$$

Together with the previous theorem this already shows every form is equivalent to at least one form satisfying the inequalities.

We need to show ‘at most one’; that is, that the forms satisfying the inequalities are in distinct classes. Suppose now that  $F = \{a, b, c\}$  and  $F' = \{a', b', c'\}$  are equivalent, and both satisfy the inequalities (4). Since they are equivalent, they represent the same integers, and so have the same minimum. The lemma says the minimum of  $F$  is  $a$  and the minimum of  $F'$  is  $a'$ , so  $a' = a$ . Similarly the minimum for products of pairs are equal, and so  $a'c' = ac$  and thus  $c' = c$ . By the fact that  $b^2 - 4ac = b'^2 - 4a'c'$  we get that  $b' = \pm b$ . If  $b' = b$ , we are done. (Why?) If  $b' = -b$ , one of the two is negative. Without loss of generality it is  $b$ . Then the inequalities imply that

$$0 < |b| < a < c.$$

In this case the proof of (3) shows we have strict inequalities, that is

$$(5) \quad F(x, y) > c > a \quad \text{if neither } x \text{ nor } y \text{ is } 0.$$

Since  $F$  and  $F'$  are equivalent, there is a change of variables

$$F'(x, y) = F(rx + ty, sx + uy).$$

Then  $a = F'(1, 0) = F(r, s)$ . By (5), we deduce that  $s = 0$  and  $r = \pm 1$ . Similarly  $c = F'(0, 1) = F(t, u)$  gives  $t = 0$  and  $u = \pm 1$ . In order to get determinant 1, the matrix is either  $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$  or  $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ , which means that  $F'$  actually was equal to  $F$  all along, not just equivalent.

A form which satisfies the inequalities (4) is called REDUCED. The theorem says every equivalence class contains exactly one reduced form. In our example with discriminant  $-35$  above, we see the reduced forms are precisely  $\{1, 1, 9\}$  and  $\{3, 1, 3\}$ , and thus the class number is 2.

The theorem actually leads to an algorithm to enumerate all the reduced forms, and thus compute the class number. We observed above that for a reduced form  $\{a, b, c\}$  of discriminant  $d$ , we have  $|b| \leq \sqrt{|d|/3}$  and  $b \equiv d \pmod{2}$ . The first step of the algorithm is to list all possible  $b$  values. Next we notice that  $4ac = b^2 - d$  implies that the only possible  $a$  choices are divisors of  $(b^2 - d)/4$ . Furthermore we need only consider divisors  $a$  with  $|b| \leq a$ . Since the  $c$  value will be  $(b^2 - d)/(4a)$  we will have  $a \leq c$  exactly when  $a \leq \sqrt{(b^2 + d)/4} \leq c$ . The second step is to list all possible  $a$  and  $c$  values for each  $b$ . For each triple  $a, b, c$  we count one or two forms according to whether or not  $\{a, b, c\} \sim \{a, -b, c\}$  by the second part of (4).

**Exercise 10.** Compute the reduced forms for the discriminants  $-627$  and  $-1411$ .  $\square$

**Exercise 11.** This exercise determines which reduced form of discriminant  $-23$  represents 13. See Lemma 2.5 in [Cox].

(1) Verify that

$$\left(\frac{-23}{13}\right) = 1.$$

(2) Solve the congruences (by BFI, or whatever)

$$b^2 \equiv -23 \pmod{13}, \quad b \equiv -23 \pmod{2}.$$

(3) Now you have  $b^2 \equiv -23 \pmod{4 \cdot 13}$ , so you can write

$$-23 = b^2 - 4 \cdot 13 \cdot l$$

for some  $l$ .

(4) So the form  $\{13, b, l\}$  represents 13, and has discriminant  $-23$ . Carry out the reduction algorithm to see which *reduced* form it is equivalent to. This form also represents 13.  $\square$

§2C. Equation (2.19) in [Cox] says

$$\begin{aligned} p \equiv 1, 3, 7, 9 \pmod{20} &\Leftrightarrow \left(\frac{-5}{p}\right) = 1 \\ &\Leftrightarrow p = x^2 + 5y^2 \text{ or } 2x^2 + 2xy + 3y^2. \end{aligned}$$

**Exercise 12.** Write

$$\left(\frac{-20}{p}\right) = \left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{5}{p}\right),$$

and use (1.16) in [Cox] and Quadratic Reciprocity to determine congruences on  $p$  modulo 4 and 5 which make both terms positive, (respectively, both negative.) Next, use these to determine congruences modulo 20 which make both terms positive, (respectively, both negative.) We will see below this determines which of the two forms of discriminant  $-20$  represent  $p$ .  $\square$

**Exercise 13.** Write

$$\left(\frac{-56}{p}\right) = \left(\frac{8}{p}\right) \cdot \left(\frac{-7}{p}\right) = \left(\frac{2}{p}\right) \cdot \left(\frac{-7}{p}\right),$$

and use (1.16) in [Cox] and Quadratic Reciprocity to determine congruence on  $p$  modulo 8 and 7 which make both terms positive, (respectively, both negative.) Next, use these to determine congruences modulo 56 which make both terms positive, (respectively, both negative.) We will see below this determines which of the four forms of discriminant  $-56$  represent  $p$ .  $\square$

On p. 33 of [Cox], he says “When  $D = -20$ , one easily computes that

$$\begin{aligned}x^2 + 5y^2 &\text{ represents } 1, 9 \text{ in } (\mathbb{Z}/20\mathbb{Z})^* \\2x^2 + 2xy + 3y^2 &\text{ represents } 3, 7 \text{ in } (\mathbb{Z}/20\mathbb{Z})^{**}\end{aligned}$$

For the first equation reduce modulo 4 to see that an odd prime  $p$  represented by the form must be 1 modulo 4. Now reduce modulo 5 to see it must be 1 or 4 modulo 5. The former is 1 modulo 20; the latter is 9 modulo 20.

For the second equation if  $y$  is even then  $x$  is odd since  $p$  is. Now  $2y$  and  $y^2$  are 0 modulo 4 and  $p \equiv 2x^2 \equiv 2$  modulo 4, contradiction. So  $y$  must be odd and  $3y^2$  is 3 modulo 4. Whether  $x$  is odd or even,  $2x^2 + 2xy$  is 0 modulo 4, so in all cases  $2x^2 + 2xy + 3y^2$  is 3 modulo 4. Meanwhile,

$$2x^2 + 2xy + 3y^2 \equiv 3(2x + y)^2 \pmod{5}.$$

If  $p$  is not 5 then  $(2x + y)^2$  is a nonzero square modulo 5, so is 1 or 4. Then 3 times that is either 3 or 2 modulo 5. Combined with the mod 4 result, the former is 3 modulo 20 and the latter is 7 modulo 20.

Cox continues “. . . while for  $D = -56$  one has

$$\begin{aligned}x^2 + 14y^2, 2x^2 + 7y^2 &\text{ represent } 1, 9, 15, 23, 25, 39 \text{ in } (\mathbb{Z}/56\mathbb{Z})^* \\3x^2 \pm 2xy + 5y^2 &\text{ represent } 3, 5, 13, 19, 27, 45 \text{ in } (\mathbb{Z}/56\mathbb{Z})^{**}\end{aligned}$$

(If your book has 29 instead of 39, it is a typo.)

**Exercise 14.** To see this,

- (1) Reduce  $x^2 + 14y^2$  and  $2x^2 + 7y^2$  modulo 7 to see the former is a square modulo 7, i.e. in the set  $\{1, 2, 4\}$ , while the latter is twice a square:  $\{2, 4, 1\}$ .
- (2) Verify that  $x^2 + 14y^2 \equiv x^2 + 6y^2$  modulo 8. If the form represents a  $p$  relatively prime to 56, then  $x$  is odd (why?) Show  $p$  is 1 or 7 modulo 8 depending on  $y$  modulo 2.
- (3) Meanwhile  $2x^2 + 7y^2 \equiv -(6x^2 + y^2)$  modulo 8. What are the possibilities for  $x$  and  $y$  modulo 2? Show  $p$  is 7 or 1 modulo 8.
- (4) Verify the six possibilities (three choices modulo 7 and two modulo 8) give exactly the six modulo 56 Cox claims. For example, if  $p \equiv 39$  modulo 56 then  $p \equiv 4$  modulo 7 and  $\equiv 7$  modulo 8.
- (5) Verify

$$3x^2 \pm 2xy + 5y^2 \equiv 3(x \pm 5y)^2 \pmod{7}.$$

What are the nonzero squares modulo 7? What is the set of 3 times a square, modulo 7? (Observe this is the same whether you choose + or -.)

(6) Verify

$$3x^2 \pm 2xy + 5y^2 \equiv 3((x \pm 3y)^2 + 6y^2) \pmod{8}.$$

Show this is 3 times (1 or 7) modulo 8, i.e. 3 or 5 modulo 8.

(7) What classes modulo 56 are (3, 5, or 6 modulo 7) and (3 or 5 modulo 8)?  $\square$

**Exercise 15.** This exercise does for discriminant  $-15$  what was done above for discriminants  $-20$  and  $-56$ .

(1) Find all reduced forms of discriminant  $-15$ , using the reduction algorithm. (There are only two.)

(2) By writing

$$\chi_{-15}([p]) = \left( \frac{-15}{p} \right) = \left( \frac{-3}{p} \right) \left( \frac{5}{p} \right),$$

determine conditions on  $p$  modulo 3 and modulo 5 such that  $\chi_{-15}([p]) = 1$ .

(3) Determine the congruence classes  $[p]$  modulo 15 such that  $\chi_{-15}([p]) = 1$ . By Theorem 2.16 in [Cox], an odd  $p \neq 3, 5$  is in one of these classes if and only if  $p$  is represented by one of the two forms you found above.

(4) Determine which forms represent which congruence classes modulo 15. Because the discriminant is odd, the 'completing the square' trick works slightly differently: you should look not just at  $p$  modulo 15, but  $4p$  modulo 15 in the case of the principal form, and  $8p$  modulo 15 in the other case. Now reduce modulo 3 and modulo 5.  $\square$

**Exercise 16.** This exercise is similar to exercise 11, but builds on the example (2.21) in [Cox].

(1) Verify that the prime  $p = 71$  is congruent to 15 modulo 56. Therefore, by (2.21) it is represented by either  $x^2 + 14y^2$  or by  $2x^2 + 7y^2$ . But which?

(2) Solve the congruences (by BFI, or PARI)

$$b^2 \equiv -56 \pmod{71}, \quad b \equiv -56 \pmod{2}.$$

(3) Now you have  $b^2 \equiv -56 \pmod{4 \cdot 71}$ , so you can write

$$-56 = b^2 - 4 \cdot 71 \cdot l$$

for some  $l$ .

- (4) So the form  $\{71, b, l\}$  represents 71, and has discriminant  $-56$ . Carry out the reduction algorithm to see which *reduced* form it is equivalent to. This form also represents 71.
- (5) Show by BFI that the other form does not represent 71. Hint:  $0 < y < 3$ , and  $0 < x < \sqrt{71 - 14y^2}$ .  $\square$

**Exercise 17.** The proof of Lemma 2.24 shows that for discriminants  $d \equiv 1 \pmod{4}$ , the subgroup  $H$  of values of the principal form in  $(\mathbb{Z}/d)^*$  is actually the subgroup of squares. This is useful for actually computing  $H$ . Show that if  $d = -4n$ , with  $n \equiv 1 \pmod{4}$ , this statement is still true. Hint: Look at  $x^2 + ny^2$  modulo  $n$  and modulo 4, considering whether  $x$  and  $y$  are odd or even.  $\square$

A FUNDAMENTAL DISCRIMINANT  $d$  is one which is not of the form  $Df^2$  with  $D$  also a discriminant. Equivalently,  $d$  is squarefree if  $d \equiv 1 \pmod{4}$ , and if  $d \equiv 0 \pmod{4}$  then  $n = d/4$  is squarefree with  $n \equiv 2$  or  $3 \pmod{4}$ .

The previous exercise shows for fundamental discriminants  $d$ , that  $H$  is the subgroup of squares as long as  $d$  is not 0 modulo 8.

**Exercise 18.** Now that we have Theorem 2.26 in [Cox], we can prove a strong theorem like Fermat's any time there is a single class in each genus.

- (1) Use the algorithm to list all of the reduced forms of discriminant  $-195$ . (You should see four of them.)
- (2) Since the discriminant is odd, the principal genus is the subgroup  $H$  of squares in  $(\mathbb{Z}/195)^*$ . Determine the elements of this subgroup by BFI, or PARI, or use the fact that  $195 = 3 \cdot 5 \cdot 13$ , and  $a$  is a square if and only if it is congruent to a square modulo each prime factor. (You should see that  $\#H = 12$ .)
- (3) For each form you found in (1) other than the principal form, determine a value it represents which is relatively prime to 195. (You should be able to do this by inspection.) Now determine the corresponding coset of  $H$ .
- (4) Since each form gives a *different* coset, there must only be one class in each genus! State a theorem like (2.22) in [Cox] for the four forms you found in (1).
- (5) Use the congruence conditions to determine which forms (if any) represent the following primes:

$$\{229, 233, 239, 241, 251, 257, 263, 269, 271, 277\}$$

$\square$

**Exercise 19.** OK, maybe the numbers were too large in the previous exercise to get a feel for what's going on.

- (1) Use the algorithm to list all of the reduced forms of discriminant  $-39$ . (You should see four of them.)
- (2) Since the discriminant is odd, the principal genus is the subgroup  $H$  of squares in  $(\mathbb{Z}/39)^*$ . Determine the elements of this subgroup by BFI, or PARI, or use the fact that  $39 = 3 \cdot 13$ , and  $a$  is a square if and only if it is congruent to a square modulo each prime factor. (You should see that  $\#H = 6$ .)
- (3) For each form you found in (1) other than the principal form, determine a value it represents which is relatively prime to 39. (You should be able to do this by inspection.) Now determine the corresponding coset of  $H$ .
- (4) You should see that the four forms correspond to only *two* cosets; there are two classes in each genus! State a theorem similar to (2.21) in [Cox]  $\square$

**Exercise 20.** This is a continuation of exercise 5, where you showed that the kernel of the Kronecker symbol,  $\ker(\chi_{-84})$  is the union of

$$H = \{1, 25, 37\},$$

along with the cosets  $[5] \cdot H$ ,  $[11] \cdot H$ , and  $[19] \cdot H$ . Now we know that by Theorem 2.26 in [Cox],

$$\begin{aligned} p = x^2 + 21y^2 &\Leftrightarrow [p] \in H \\ p = 3x^2 + 7y^2 &\Leftrightarrow [p] \in [19]H \\ p = 2x^2 + 2xy + 11y^2 &\Leftrightarrow [p] \in [11]H \\ p = 5x^2 + 4xy + 5y^2 &\Leftrightarrow [p] \in [5]H \end{aligned}$$

This exercise investigates what the factorizations of the discriminant into a product of discriminants tells us. We can factor  $-84$  into discriminants three ways: as

$$-3 \cdot 28, \quad \text{or} \quad -4 \cdot 21 \quad \text{or} \quad -7 \cdot 12.$$

- (1) Show that

$$\begin{aligned} \left(\frac{-84}{a}\right) = 1 &\Leftrightarrow \\ \left(\frac{-3}{a}\right) = \left(\frac{28}{a}\right), \quad \left(\frac{-4}{a}\right) = \left(\frac{21}{a}\right), \quad \left(\frac{-7}{a}\right) = \left(\frac{12}{a}\right). \end{aligned}$$

- (2) On each element  $a$  of  $H$ , as well as each element  $a$  of the cosets  $[5] \cdot H$ ,  $[11] \cdot H$ , and  $[19] \cdot H$ , compute each of

$$\left(\frac{-3}{a}\right), \quad \left(\frac{-4}{a}\right), \quad \left(\frac{-7}{a}\right).$$

Your answer is a table with 3 columns and 12 rows. Instead of just BFI, try to use the multiplicative properties of the Kronecker symbol. You might also use the fact that  $H$  is the subgroup of squares in  $(\mathbb{Z}/84)^*$  to simplify the computation; anything in  $H$  is also a square modulo every divisor  $d$  of 84.  $\square$

These are examples of what we will eventually call GENUS CHARACTERS.

**§3A.** Lemma 3.2 and Lemma 3.3 in [Cox] on composition of forms can be greatly simplified.

**Exercise 21.** Suppose we have forms  $f = \{a, b, c\}$  and  $g = \{a', b', c'\}$ . By Lemma 2.25 and Lemma 2.3 we can change the variables in  $g$  so that  $(a, a') = 1$ . Thus there exist  $x$  and  $x'$  so that  $xa + x'a' = 1$ .

- (1) Verify directly that the solution  $B$  to the first two congruences in Lemma 3.2

$$B \equiv b \pmod{2a}$$

$$B \equiv b' \pmod{2a'}$$

is given by

$$B = x'a'b + xab'.$$

- (2) Verify, just as in the proof of Lemma 3.2, that the third congruence

$$B^2 \equiv d \pmod{4aa'}$$

actually follows from the first two. Hint: At some point you will need the fact that  $b^2 = d + 4ac$ , and  $b'^2 = d + 4a'c'$ .

- (3) Verify directly that for a form  $f = \{a, b, c\}$  and its opposite  $\{a, -b, c\} \sim \{c, b, a\}$ , that  $B = b$  trivially satisfies the congruences of Lemma 3.2, without the requirement that  $a$  and  $a' = c$  be relatively prime.  $\square$

**Exercise 22.** There are five reduced forms of discriminant  $-47$ , namely

$$\{1, 1, 12\}, \quad \{2, \pm 1, 6\}, \quad \{3, \pm 1, 4\}.$$

- (1) Use the composition law (3.7) to compute the square of the form  $\{2, 1, 6\}$ . (Try the substitution  $(x, y) \rightarrow (x, x + y)$  to make  $(a, a') = 1$ .) Which *reduced* form is this equivalent to?

- (2) Now compose that form with  $\{2, 1, 6\}$ . Which reduced form is it equivalent to?
- (3) Since the group has order 5, it is isomorphic to  $\mathbb{Z}/5$ . Can you give a correspondence between the five forms and the set

$$\mathbb{Z}/5 = \{0, 1, 2, 3, 4\}?$$

□

**Exercise 23.** This exercise compliments Proposition 3.11 of [Cox], covering the case when  $d \equiv 1 \pmod{4}$ . With  $r$  the number of prime factors of  $d$ , there are  $2^{r-1}$  ambiguous forms

$$\{e, e, (e - d/e)/4\} \quad \text{for } e|d, \quad 0 < e < \sqrt{|d|}.$$

- (1) Verify that  $(e - d/e)/4$  is really an integer, and that these forms all have discriminant  $d$ .
- (2) Verify that if  $e < \sqrt{|d|}/3$ , the form is reduced.
- (3) Verify that if  $\sqrt{|d|}/3 < e < \sqrt{|d|}$ , then a single step of the reduction algorithm gives the form

$$\{(e - d/e)/4, (e + d/e)/2, (e - d/e)/4\},$$

and that this form is now reduced.

- (4) Any ambiguous form  $\{a, b, c\}$  has  $a = b$  or  $a = c$ . (The case  $b = 0$  is omitted since  $d$  is odd.) Show that every such form arises from one of the divisors  $e$  of  $d$  as above. Hint: The discriminant  $b^2 - 4ac = d$ . □

§3B. The next four exercises will compute an example illustrating the results in §3B of Chapter 1 in [Cox].

**Exercise 24.** If you don't have PARI to help with the computations, or if you are new at group theory, be sure to ask for lots of help.

- (1) List all the reduced forms with discriminant  $-260$ . (You should see eight of them.)
- (2) How many forms are ambiguous, i.e. have order 2? There are three abelian groups of order 8, namely

$$\mathbb{Z}/8, \quad \mathbb{Z}/4 \times \mathbb{Z}/2, \quad \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2.$$

Which of these groups has the same number of element of order 2 as you just found?

- (3) What is the subgroup  $H$  of squares in  $(\mathbb{Z}/260)^*$ ? You may either use the fact that the squares are simultaneously squares modulo 20 and modulo 13, or use the PARI code

```
{for(a=1, 260, if(gcd(a, 260)==1,
  print(a" "Mod(a^2, 260))))}
```

(4) Group the forms into their genera. You can do this in either of two ways:

(a) For each form you found in (1), determine a value it represents which is relatively prime to 260, and determine the corresponding coset of  $H$ . Or,

(b) Use the PARI code

```
{forprime(p=1, 500,
  if(kronecker(-260, p)==1,
    print(p" "Mod(p, 260)" "
      qfbred(qfbprimeform(-260, p))))}
```

which computes which form of discriminant  $-260$  represents each of the primes below 500. Once you have a specific prime in mind, you can compute the corresponding coset of  $H$  with the PARI code

```
{for(a=1, 260, if(gcd(a, 260)==1,
  print(Mod(p*a^2, 260))))}
```

where the character  $p$  is replaced with an actual number.

(You should see four genera, each with two forms.)  $\square$

**Exercise 25.** (Continuation of exercise 24)

- (1) Work out the multiplication table for the cosets of  $H$ . (It is a four by four table with 16 entries.)
- (2) Work out the multiplication table for the genera. (It is a four by four table with 16 entries.)
- (3) Work out the multiplication table for  $\mathbb{Z}/2 \times \mathbb{Z}/2$ , and compare to your previous two answers.  $\square$

**Exercise 26.** (Continuation of exercise 24)

- (1) The discriminant  $-260$  factors as  $-4 \cdot 5 \cdot 13$ . Compute each of the three genus characters

$$\left(\frac{-4}{a}\right), \quad \left(\frac{5}{a}\right), \quad \left(\frac{13}{a}\right).$$

on each of the four cosets of  $H$ .

- (2) We know that

$$\left(\frac{-260}{a}\right) = 1 \Leftrightarrow$$

$$\left(\frac{-4}{a}\right) = \left(\frac{65}{a}\right), \quad \left(\frac{5}{a}\right) = \left(\frac{-52}{a}\right), \quad \left(\frac{13}{a}\right) = \left(\frac{-20}{a}\right).$$

For each factorization of  $-260 = D_1 D_2$  as above, and each form  $\{a, b, c\}$ , write  $a = a_1 a_2$  with  $\gcd(a, D_1) = a_1$  and  $a_2 =$

$a/a_1$ . Compute

$$\left(\frac{D_1}{a_2}\right) \left(\frac{D_2}{a_1}\right),$$

and see that it is the same value as the genus character.

Thus the values of the genus characters can be computed directly from the forms, and so Lagrange's definition of genus 'Two forms are in the same genus if they represent the same congruence classes in  $(\mathbb{Z}/d)^*$ ' is the same as Gauss' definition of genus 'Two forms are in the same genus if all the genus characters agree.'  $\square$

**Exercise 27.** (Continuation of exercise 24)

- (1) Use PARI to compute the square of every reduced form you found above; the code `Qfb(a, b, c)^2` suffices, where  $a$ ,  $b$ , and  $c$  are the relevant coefficients.
- (2) Observe that the square of every form is in the principal genus.
- (3) Observe that every form in the principal genus is the square of some form.

Thus the principal genus is the subgroup of squares  $\mathcal{C}(-260)^2$  of the class group  $\mathcal{C}(-260)$ .  $\square$

Recall the definition of fundamental discriminant above. A PRIMARY DISCRIMINANT is a fundamental discriminant which is divisible by only one prime. The primary discriminants are

$$-4, 8, -8, \text{ and } \pm p,$$

for every odd prime  $p$ , where the sign  $\pm$  is chosen so that  $\pm p \equiv 1 \pmod{4}$ . Every fundamental discriminant has a unique factorization into primary discriminants. (See previous exercises for examples.)

**Exercise 28.** This exercise concerns the definition of assigned characters in [Cox], which can be greatly simplified.

- (1) For odd primes  $p$  dividing  $d$ , the character

$$\chi(a) = \left(\frac{a}{p}\right) \text{ is just } \left(\frac{\pm p}{a}\right),$$

where the sign  $\pm$  is chosen to make a primary discriminant, i.e.  $\pm p \equiv 1 \pmod{4}$ .

- (2) His character

$$\delta(a) = (-1)^{(a-1)/2} \text{ is just } \left(\frac{-4}{a}\right)$$

for  $a$  odd.

(3) His character

$$\epsilon(a) = (-1)^{(a^2-1)/8} \text{ is just } \left(\frac{8}{a}\right)$$

for  $a$  odd, and thus

$$\delta\epsilon(a) = \left(\frac{-8}{a}\right).$$

(4) Fundamental discriminants are either odd, or else of the form  $-4n$  with  $n \equiv 1, 2$  or  $5, 6 \pmod{8}$ . Check that the even primary discriminant factor of  $d$  is equal to

- (a)  $-4 \Leftrightarrow n \equiv 1, 5 \pmod{8}$ ,
- (b)  $8 \Leftrightarrow n \equiv 6 \pmod{8}$ , and
- (c)  $-8 \Leftrightarrow n \equiv 2 \pmod{8}$ .

Thus for fundamental discriminants, the assigned characters are merely the Kronecker symbols for the primary discriminants dividing  $d$ .  $\square$

#### REFERENCES

- [Cox] D. Cox, *Primes of the Form  $x^2 + ny^2$* , Wiley, 1989.
- [Oesterlé] J. Oesterlé, *Le problème de Gauss sur le nombre de classes*, Enseign. Math. (2) 34 (1988), no. 1-2, pp. 43-67.
- [Stopples] J. Stopples, *A Primer of Analytic Number Theory: from Pythagoras to Riemann*, Cambridge University Press, 2003.