

# Solution Set 5

Math 123  
March 11, 2002

1. Artin §11.10 #1

Recall that  $A$  and  $A'$  are similar if and only if their ideal classes are the same, i.e.  $\langle A \rangle = \langle A' \rangle$ . Let  $C$  be a representative of  $\langle \bar{A} \rangle$ , so  $\langle A \rangle \langle C \rangle = \langle (1) \rangle$ . Then  $\langle A \rangle = \langle A' \rangle \iff \langle A \rangle \langle C \rangle = \langle A' \rangle \langle C \rangle = \langle (1) \rangle \iff AC$  and  $A'C$  are principal.

---

---

2. Artin §11.10 #4(c,e)

c)  $d = -14$

This ideal class group is calculated in Artin on pages 431–432; there it is shown that it is the cyclic group of order four, generated by an ideal  $Q$  such that  $Q\bar{Q} = (3)$ . Setting  $Q = (3, 1 + \delta)$  where  $\delta = \sqrt{-14}$ , we have

$$Q\bar{Q} = (9, 15, 3(1 + \delta), 3(1 - \delta)) = (3)$$

since  $\gcd(9, 15) = 3$ . Also, from Artin we know that  $Q^2$  is similar to  $P = (2, \delta)$ , and since  $Q^4$  is principal,  $Q^3$  is similar to  $\bar{Q}$ . These four ideal class representatives are drawn in Figure 2.1.

e)  $d = -17$

Since  $-17 \equiv 3 \pmod{4}$ , our bound  $[\mu]$  is 5. We know from problem 11.9 #7 on a previous homework that (2) ramifies into  $P^2$ , and that (3) and (5) do not ramify. Since  $f(x) = x^2 + 17$  is reducible in  $\mathbf{F}_3$ ,  $(3) = Q\bar{Q}$  splits, and since  $f(x)$  is irreducible in  $\mathbf{F}_5$ , (5) remains inert, so we can ignore it.

The rest of the analysis is similar to the  $d = -14$  case, given in Artin. With  $\delta = \sqrt{-17}$ , we have  $(1 + \delta)(1 - \delta) = 18 = 2 \cdot 3 \cdot 3$ , which gives an equation in ideals

$$(1 + \delta)(1 - \delta) = P^2 Q^2 \bar{Q}^2.$$

Now, the norm of  $N(1 + \delta)$  is the same as  $N(1 - \delta)$ , so the prime factorization of  $(1 + \delta)$  can contain  $P$  only once. Since 3 does not divide  $1 + \delta$  (i.e.  $\frac{1}{3}(1 + \delta)$  is not in our ring), we cannot have both  $Q$  and  $\bar{Q}$  as prime factors of  $(1 + \delta)$ ,<sup>1</sup> so choosing  $Q$  and  $\bar{Q}$  appropriately, we can conclude that

$$(1 + \delta) = PQ^2 \implies \langle Q \rangle^2 = \langle P \rangle^{-1} = \langle P \rangle.$$

Thus the ideal class group  $\mathcal{C}$  is generated by  $Q$ . One can quickly conclude that  $P$  is not principal because if  $P = (a + b\delta)$  then  $N(a + b\delta) = a^2 + 17b^2 = 2$ , which has no solution

---

<sup>1</sup>Most people neglected this step!

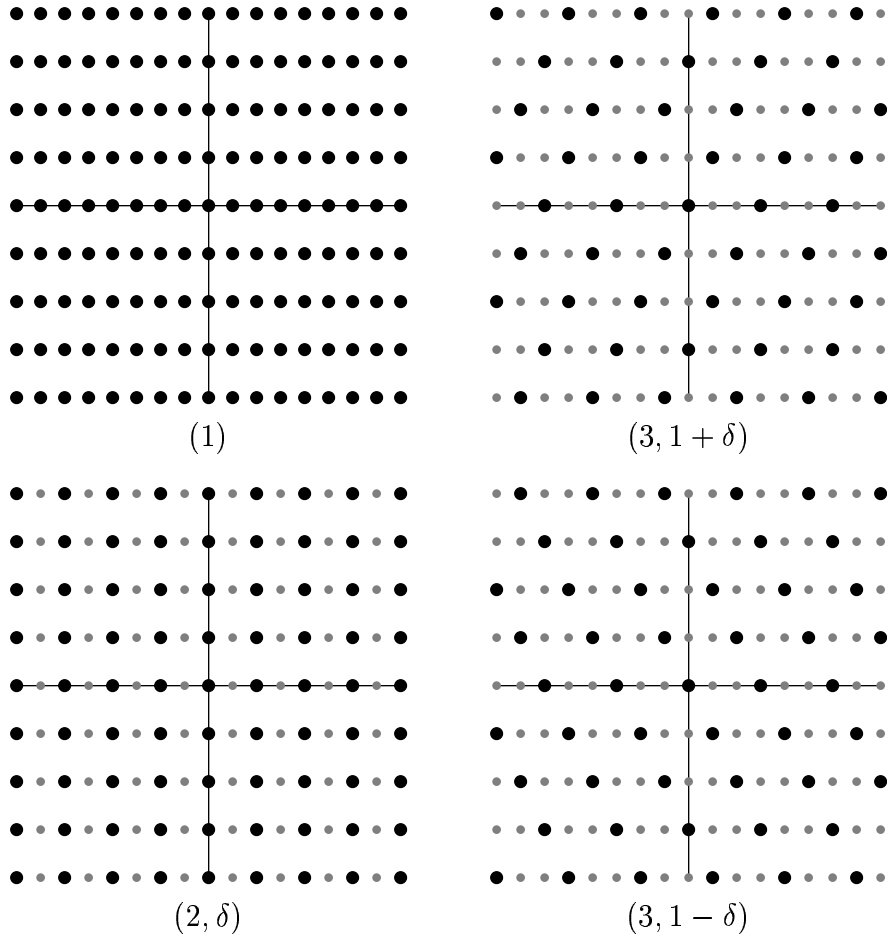


Figure 2.1: The possible shapes of the ideals in  $\mathbf{Z}[\sqrt{-14}]$  (not to scale).

in the integers.<sup>2</sup> Thus  $Q$  is also not principal, so since  $P^2$  is principal, the order of  $Q$  is 4 and we again find that  $\mathcal{C} \cong \mathbf{Z}/4$ , generated by  $\langle Q \rangle$ .

All that remains is to calculate the ideals. We see that with  $P = (2, 1 + \delta)$  we have

$$P\overline{P} = (4, 18, 2(1 + \delta), 2(1 - \delta)) = (2)$$

since  $\gcd(4, 18) = 2$ ; similarly, with  $Q = (3, 2 + \delta)$  we have

$$Q\overline{Q} = (9, 21, 3(2 + \delta), 3(2 - \delta)) = (3)$$

since  $\gcd(9, 21) = 3$ . Again,  $Q^2$  is similar to  $P$  and  $Q^3$  is similar to  $Q$ ; the four ideal shapes are given in Figure 2.2.

---

<sup>2</sup>Most people also neglected this easy step.

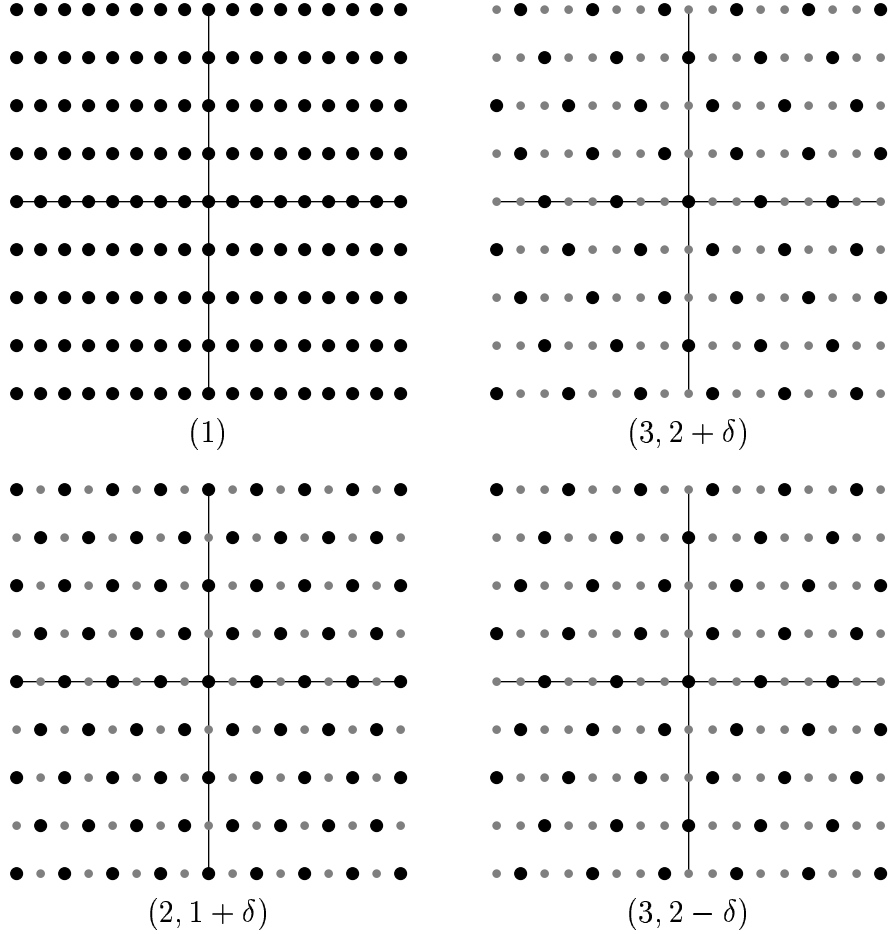


Figure 2.2: The possible shapes of the ideals in  $\mathbf{Z}[\sqrt{-17}]$  (not to scale).

**3.** Artin §11.11 #1

With  $\delta = \sqrt{2}$  and  $R = \mathbf{Z}[\delta]$ , we can define a norm  $\sigma(a + b\delta) = |a^2 - 2b^2|$  on  $\mathbf{Q}[\delta]$  which becomes a size function on  $R$ ; note that for  $\alpha, \beta \in \mathbf{Q}[\delta]$  we have  $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ .

Let  $x, y \in R$  with  $y \neq 0$ . Define  $q' = \frac{x}{y}$ ; suppose  $q' = q'_1 + q'_2\delta$  with  $q'_1, q'_2 \in \mathbf{Q}$ . Define  $q_i$  to be the closest integer to  $q'_i$  (for  $i = 1, 2$ ), and let  $q = q_1 + q_2\delta$ . Let  $r' = q' - q = r'_1 + r'_2\delta$ , so

$$\sigma(r') = |r_1'^2 - 2r_2'^2| \leq r_1'^2 + 2r_2'^2 \leq \frac{3}{4}$$

since  $r'_1, r'_2 \leq \frac{1}{2}$ . Now, we can write

$$q = \frac{x}{y} - r' \implies x = qy + r$$

with  $r = yr'$ . Now,  $\sigma(r) = \sigma(y)\sigma(r') < \sigma(y)$  since  $\sigma(r') < 1$ , and  $r \in R$  since  $x, qy \in R$ . Thus  $R$  is a Euclidian domain.

4. Artin §11.11 #3

First we prove a general fact (which is provided here mainly for reference and because I was interested; it is not technically part of the problem). Let  $\delta = \sqrt{d}$  for  $d > 0$  squarefree, let  $R$  be the ring of algebraic integers in  $\mathbf{Q}[\delta]$ , and for  $\alpha = a + b\delta \in R$  define  $\bar{\alpha} = a - b\delta$ . Note that  $R \subset \mathbf{R}$ .

CLAIM 4.1.  $U_0$  is an infinite cyclic group, generated by the unit  $\alpha$  such that  $\alpha < 1$  and for all  $\beta \in U_0$ ,  $\beta < \alpha$  or  $\beta > 1$ , i.e.  $\alpha$  is the largest element that is less than 1.

PROOF.

We call this  $\alpha$  the *fundamental unit*.

Let  $\epsilon : R \hookrightarrow \mathbf{R}^2$  be the embedding of  $R$  into the  $(u, v)$ -plane. We note that  $\epsilon(\alpha\beta) = (\alpha\beta, \overline{\alpha\beta}) = (\alpha\beta, \bar{\alpha}\bar{\beta})$ , so multiplication in  $R$  is coordinate-wise multiplication in  $\mathbf{R}^2$ . Thus if  $\alpha, \beta$  are in the first quadrant, i.e.  $\alpha, \bar{\alpha}, \beta, \bar{\beta} > 0$ , then  $\alpha\beta$  is too, so  $U_0$  is closed under multiplication and taking inverses.

Now let  $\alpha \in U_0$  be the fundamental unit, and let  $\beta \in U_0$  be any element. Suppose that  $\beta \notin \langle \alpha \rangle$ ; suppose further that  $\beta < 1$  (otherwise  $\beta^{-1} < 1$  and  $\beta^{-1} \notin \langle \alpha \rangle$  still). Let  $n > 0$  be the integer such that  $\alpha^n > \beta > \alpha^{n+1}$ , and let  $\gamma = \beta/\alpha^n$ . So  $\gamma < 1$  and  $\gamma > \alpha^{n+1}/\alpha^n = \alpha$ , which contradicts the fact that  $\alpha$  was the fundamental unit. Thus  $U_0 = \langle \alpha \rangle$ ; note that  $U_0$  is infinite since  $\alpha^{n+1} < \alpha^n$  for each  $n$ . □

a)  $d = 3$

By looking at Figure 5.1, one can easily convince oneself that  $2 - \delta$  is the fundamental unit.

b)  $d = 5$

By drawing a picture similar to Figure 5.1, one can see that  $(3 - \delta)/2$  is the fundamental unit.

5. Artin §11.11 #5

The picture is given in Figure 5.1.

6. Artin §11.12 #4

Throughout this problem, the ambient ring is  $\mathbf{Z}$ . We know that  $(a, b)$  is principal, generated by the greatest common divisor  $d = \gcd(a, b)$ , and that  $ax + by = c$  has a solution if and only if  $c \in (a, b) = (d)$ . Thus there is a solution if and only if  $\gcd(a, b) | c$ .

Now, if  $ax + by = c$  then for any  $z, w$  with  $az = bw$  we have  $a(x + z) + b(y - w) = c$  as well; this is the general form for the solutions since given any other solution  $ax' + by' = c$ ,

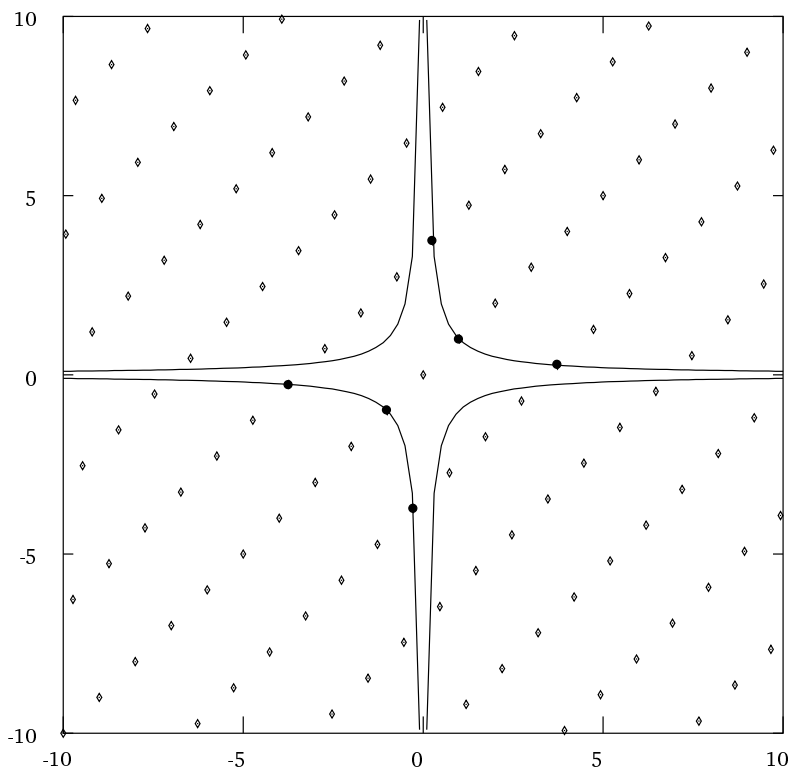


Figure 5.1: The ring  $\mathbf{Z}[\sqrt{3}]$ , embedded into the  $(u, v)$  plane, with units in large dots.

we can subtract the two solutions to obtain  $a(x - x') + b(y - y') = 0$ , which is to say that  $a(x - x') = b(y' - y)$ . Now, the smallest absolute value of  $az = bw$  is  $\text{lcm}(a, b)$ , and since  $\text{lcm}(a, b)$  divides any number  $d$  such that  $a|d$  and  $b|d$ , we must have that all solutions are of the form  $a(x + nz) + b(y - nw)$  where  $n \in \mathbf{Z}$  is any integer,  $z = \text{lcm}(a, b)/a$ , and  $w = \text{lcm}(a, b)/b$ .

7. Artin §11.12 #5

We rewrite the equation  $x^2 + 2y^2 = p$  as  $(x + \delta)(x - \delta) = (p)$ , where  $\delta = \sqrt{-2}$ . Thus we see that, since  $R = \mathbf{Z}[\delta]$  is a PID, there is an inter solution if and only if  $p$  splits in  $R$ , which is true if and only if  $x^2 + 2$  is reducible in  $\mathbf{F}_p$ , which is the case if and only if  $x^2 = -2$  has a solution mod  $p$ .

That was the algebra part of the problem; the rest is a number theory question. Assume that  $p \neq 2$  (if  $p = 2$  then clearly  $x^2 + 2$  is reducible). Since the equation  $x^2 = 1$  has exactly two solutions in  $\mathbf{F}_p$ , the kernel of the homomorphism  $x \mapsto x^2 : \mathbf{F}_p^* \rightarrow \mathbf{F}_p^*$  is  $\{\pm 1\}$ , so the image is half of the elements of  $\mathbf{F}_p^*$ , i.e. if  $(\mathbf{F}_p^*)^2 = \{x^2 \mid x \in \mathbf{F}_p^*\}$ , then  $|(\mathbf{F}_p^*)^2| = (p - 1)/2$ . Since  $\mathbf{F}_p^*$  is abelian,  $(\mathbf{F}_p^*)^2$  is normal, so  $\mathbf{F}_p^*/(\mathbf{F}_p^*)^2$  is group isomorphic to  $\{\pm 1\}$ , so the product of two quadratic nonresidues (elements of  $\mathbf{F}_p^* - (\mathbf{F}_p^*)^2$ ) is a quadratic residue mod  $p$ . Thus  $-2$  is a square mod  $p$  if and only if either 2 and  $-1$  are squares mod  $p$  or both are

---

not squares mod  $p$ . Well, we know that  $-1$  is a square mod  $p$  if and only if  $p \equiv 1 \pmod{4}$ , and the special case of quadratic reciprocity tells us that  $2$  is a square mod  $p$  if and only if  $p \equiv 1$  or  $7 \pmod{8}$ .

To summarize, then,  $x^2 + 2y^2 = p$  has a solution when either  $p = 2$  or  $p \equiv 1$  or  $3 \pmod{8}$ .

---

---

*Joe Rabinoff*