ALGEBRAIC NUMBER THEORY

HOMEWORK 3

(1) Show that if $m = 2p$ for some prime $p \equiv 5 \bmod 8$, then the equation $x^2 - 2py^2 = -1$ has a solution in integers.

It is of course not sufficient to check that this equation has solutions modulo 8 or something. We proceed as for $m = p \equiv 1 \bmod 4$.

We start with a minimal positive solution (t, u) of the Pell equation $t^2 - 2pu^2 = +1$. Clearly t is odd, and working modulo 4 we immediately see that u must be even. Now $2pu^2 = t^2 - 1 = (t-1)(t+1)$. The gcd of the factors on the right divides the difference $(t+1) - (t-1) = 2$, and the gcd is even since t is odd. Thus $\gcd(t-1, t+1) = 2$, and we are in one of the following cases:

$$\begin{aligned} t - 1 &= 4pr^2 & \qquad t + 1 &= 2s^2, \\ t - 1 &= 2pr^2 & \qquad t + 1 &= 4s^2, \\ t - 1 &= 4r^2 & \qquad t + 1 &= 2ps^2, \\ t - 1 &= 2r^2 & \qquad t + 1 &= 4ps^2. \end{aligned}$$

Taking the difference of these equations and cancelling 2 gives

$$\begin{aligned} s^2 - 2pr^2 &= +1, \\ 2s^2 - pr^2 &= +1, \\ ps^2 - 2r^2 &= +1, \\ 2ps^2 - r^2 &= +1. \end{aligned}$$

The second and the third equation are impossible: reduction modulo p shows $(\frac{2}{p}) = +1$, but this contradicts $p \equiv 5 \bmod 8$ (you can also check that, in the second equation, s must be even and r odd, which gives you $p \equiv 1 \bmod 8$ without using the second supplementary law). The first equation contradicts the minimality of (t, u): from $2rs = u$ we deduce that $|r| < |u|$. Since one out of these equations must hold (we started with an existing solution of the Pell equation), the last equation must be solvable.

(2) Show that if $m = 2p$ for some prime $p \equiv 5 \bmod 8$, then the ring of integers $\mathcal{O}_K$ in $\mathbb{Q}(\sqrt{m}\,)$ does not have unique factorization.

Clearly $\mathfrak{p} = (2, \sqrt{m}\,)$ is a prime ideal with norm 2 since $\mathfrak{p}^2 = (2)$. We claim that $\mathfrak{p}$ is not principal.

In fact, if say $\mathfrak{p} = (a + b\sqrt{m}\,)$, then $a^2 - mb^2 = \pm 2$. Reducing this equation modulo p shows that $(\frac{\pm 2}{p}) = +1$. On the other hand, $(\frac{-1}{p}) = +1$ since $p \equiv 1 \bmod 4$ and $(\frac{2}{p}) = -1$ since $p \equiv 5 \bmod 8$: this is a contradiction.

Now it is clear that $2 \cdot p = \sqrt{2p} \cdot \sqrt{2p}$ is an example of nonunique factorization. We just have shown that 2 is irreducible; if p were reducible, there would exist an element π of norm $\pm p$, and then $\sqrt{2p}/\pi$ would be an element of norm 2: contradiction.

(3) Compute the fundamental unit of $\mathbb{Q}(\sqrt{67}\,)$ using elements of small norm. You can find elements with small norm using `pari`:

```
for(a=1,15,print(a,"   ",factor(a^2-67)))
```

The following elements have norms divisible only by primes ≤ 7:

α	$N\alpha$
$2+\sqrt{67}$	$-3^2 \cdot 7$
$5+\sqrt{67}$	$-2 \cdot 3 \cdot 7$
$7+\sqrt{67}$	$-2 \cdot 3^2$
$8+\sqrt{67}$	3
$9+\sqrt{67}$	$2 \cdot 7$
$11+\sqrt{7}$	$2 \cdot 3^3$

A little bit of experience will show you that the elements $a+\sqrt{67}$ for $a=7$ and $a=8$ will actually suffice. Thus let us write down all prime ideals of norms 2 and 3. Since $67 \equiv 3 \bmod 4$, the prime 2 is ramified, and the unique prime ideal of norm 2 is $\mathfrak{2} = (2, 1+\sqrt{67}\,)$. Next $(\frac{67}{3}) = +1$, hence $\mathfrak{3}_1 = (3, 1+\sqrt{67}\,)$ and $\mathfrak{3}_2 = (3, 1-\sqrt{67}\,)$ are the prime ideals of norm 3.

Now we factor the principal ideals $(a+\sqrt{m}\,)$ into prime ideals. Since $7+\sqrt{67} \equiv 1+\sqrt{67} \equiv 0 \bmod \mathfrak{3}_1$, we must have $(7+\sqrt{67}\,) = \mathfrak{2}\mathfrak{3}_1^2$. Similarly we get $8+\sqrt{67} \equiv -1+\sqrt{67} \equiv 0 \bmod \mathfrak{3}_2$, hence $(8+\sqrt{67}\,) = \mathfrak{3}_2$ and therefore $(8-\sqrt{67}\,) = \mathfrak{3}_1$.

This shows that $\beta = \frac{7+\sqrt{67}}{(8-\sqrt{67}\,)^2}$ generates the prime ideal $\mathfrak{2}$. From $\mathfrak{2}^2 = (2)$ we then see that $\varepsilon = \beta^2/2$ must be a unit > 0, and since clearly $\varepsilon \neq 1$ (it is twice a square) it is nontrivial. In fact we get

$$\varepsilon = \frac{(7+\sqrt{67}\,)^2}{2(8-\sqrt{67}\,)^4} = 48842 + 5967\sqrt{67}.$$

It remains to check that ε is fundamental. In any case, $\varepsilon = \eta^m$ for some $m \in \mathbb{N}$, where η is the fundamental unit. Since $\eta \geq 1+\sqrt{67}$, we find

$$m = \frac{\log \varepsilon}{\log \eta} \leq \frac{\log \varepsilon}{\log(1+\sqrt{67}\,)} < 5.17.$$

If $\varepsilon = \eta^2$, then $\eta \approx 306.0784$ and $\eta' = 1/\sqrt{\varepsilon} \approx 0.00326$. Clearly $\eta + \eta'$ is not an integer, hence $\eta = \sqrt{\varepsilon}$ is not an element of $\mathcal{O}_K$. Similar calculations show that ε is not a third or fifth power. Thus ε is fundamental.

(4) Determine whether the prime ideals above 3 in $K = \mathbb{Q}(\sqrt{229}\,)$ are principal or not.

1. Find a unit. We do this by solving the Pell equation $t^2 - 229u^2 = \pm 4$ and find the fundamental unit $\varepsilon = \frac{1}{2}(15+\sqrt{229}\,)$.

2. Assume that there exists some $a+b\sqrt{229} \in \mathcal{O}_K$ with norm $a^2-229b^2 = \pm 3$. Then we have shown that there is a solution with $|b| < \frac{\sqrt{3}}{2\sqrt{229}}(\sqrt{\varepsilon}+1)$. A little calculation shows that $|b| < 0.4$, hence we must have $b = 0$ (**Warning:** you cannot draw this conclusion from $|b| < 1$ since we might have $b = \frac{1}{2}$). But clearly there can be no solution with $b = 0$.

Conclusion: the prime ideals $(3, \omega)$ and $(3, \omega')$ in $\mathbb{Q}(\sqrt{229}\,)$ are not principal.