Michaelmas 2012, NT III/IV, Solutions to Problem Sheet 6.

1. $d = 7$:-

   $7 \not\equiv 1 \mod 4$ so we can solve $a^2 - 7b^2 = \pm 1$ for the smallest $b > 0$.

b	$7b^2 \pm 1$		a^2
1	6	8	
2	27	29	
3	62	64	$64 = 8^2$

   So the fundamental unit is $8 + 3\sqrt{7}$.

   $d = 30$:-

   $30 \not\equiv 1 \mod 4$ so we can solve $a^2 - 30b^2 = \pm 1$ for the smallest $b > 0$.

b	$30b^2 \pm 1$		a^2
1	29	31	
2	119	121	$121 = 11^2$

   So the fundamental unit is $11 + 2\sqrt{30}$.

   $d = 53$:-

   $53 \equiv 1 \mod 4$ so we must solve $x^2 - 30y^2 = \pm 4$ for the smallest $y > 0$.

y	$53y^2 \pm 4$		x^2
1	49	57	$49 = 7^2$

   So the fundamental unit is $\dfrac{7 + \sqrt{53}}{2}$.

2. Put $K = \mathbb{Q}(\sqrt{30})$. and $u = 11 + 2\sqrt{30}$. Then $u\tilde{u} = 121 - 4 \times 30 = 1$.
   (So u is a unit — in fact the fundamental unit — of $\mathbb{Z}[\sqrt{30}]$.)

   Now $u > 11 + 2 \times 5 = 21$. So $0 < 11 - 2\sqrt{30} = 1/u < 1/21$ and $\sqrt{30} > (11 - 1/21)/2$.

   Hence $u^2 = 241 + 44\sqrt{30} > 241 + 44(11 - 1/21)/2 = 241 + 242 - 22/21 = 481$.

   Whence $241 - 44\sqrt{30} = (\tilde{u})^2 = 1/u^2 < 1/481$.

   So that $0 < 241/44 - \sqrt{30} < 1/(44 \times 481) = 1/21164 < 1/20000 = 5 \times 10^{-5}$.

3. [Note that, since $n^2 \equiv 0$ or $1 \mod 4$, $d \equiv 2$ or $3 \mod 4$ and so d cannot be a square.]

   Let $u = n^2 - 1 + n\sqrt{d}$. Then $u\tilde{u} = (n^2 - 1)^2 - n^2(n^2 - 2) = 1$.

   So u is certainly a unit of $\mathbb{Z}[\sqrt{d}]$.

   If $v = a + b\sqrt{d}$ is the fundamental unit then, for some $r \geq 1$,

   $u = v^r = a^r + ra^{r-1}b\sqrt{d} + r(r-1)a^{r-2}b^2d/2 + \cdots$.

   If $r > 1$ then, equating rational parts,

   $n^2 - 1 \geq a^r + a^{r-2}b^2d \geq a^2 + b^2(n^2 - 2)$.

   So $a = b = 1$ and $\pm 1 = v\tilde{v} = 1 - d$. Thus $d = 2$ and $n = 2$. Contradiction.

   So $r = 1$ and u is the fundamental unit.

4. From Q1 the fundamental unit of $\mathbb{Z}[\sqrt{7}]$ is $8 + 3\sqrt{7}$.
   If we have $x, y \in \mathbb{Z}$ such that $9x^2 - 7y^2 = \pm 1$ then we can assume that $x, y > 0$.
   Then $3x + y\sqrt{7}$ is a unit greater than 1.
   So $3x + y\sqrt{7} = (8 + 3\sqrt{7})^r$ for some $r \in \mathbb{Z}^{>0}$.
   Reducing coefficients mod 3, we have $\pm\sqrt{7} \equiv (-1)^r$ which is impossible.

   So there are no solutions.

   (Actually there's a low-tech way of doing this. Can you see it?)

5. Take $K = \mathbb{Q}(\sqrt{6})$. We know that $R = \mathbb{Z}[\sqrt{6}]$ is a UFD.

(i) Put $\alpha = x + y\sqrt{6}$. Then we require those $\alpha \in R$ such that $N_K(\alpha)(= x^2 - 6y^2) = 1$, i.e. those units α of R of norm 1.

The fundamental unit of $\mathbb{Q}(\sqrt{6})$ is easily found to be $u = 5 + 2\sqrt{6}$. So α is a unit iff

$$\alpha = \pm u^t, \text{ with } t \in \mathbb{Z}. \qquad (*)$$

But $N(\pm u^t) = N(u)^t = (1)^t = 1$ for all t. So $(*)$ gives a solution for every value of t.

Recovering x and y from $\alpha = \pm u^t$ we get the complete solution of $(*)$:

$$\begin{aligned} x &= \pm\frac{u^t + \tilde{u}^t}{2} = \pm\frac{(5+2\sqrt{6})^t + (5-2\sqrt{6})^t}{2} \\ y &= \pm\frac{u^t - \tilde{u}^t}{2\sqrt{6}} = \pm\frac{(5+2\sqrt{6})^t - (5-2\sqrt{6})^t}{2\sqrt{6}} \end{aligned}$$

for $t \in \mathbb{Z}$.

(ii) This question differs from (i) only in that we are asked for to solve $N_K(\alpha) = -1$. i.e. to find those units α of R of norm -1. But we have just shown that all units of R have norm $+1$. So the equation has no solutions.

(iii) Take $\alpha = x + y\sqrt{6} \in R$, as before.
Then our equation demands those $\alpha \in R$ such that $\alpha\widetilde{\alpha} = 5$ (so α will be a prime in R and a factor of 5).

Put $\beta = 1 + \sqrt{6}$ and then $N(\beta) = -5$.

So β is prime in R and $5 = -\beta\tilde{\beta}$ is a prime factorization of 5.

$$\text{Hence } \alpha \sim \beta \text{ or } \tilde{\beta}. \text{ i.e. } \alpha = \pm u^m\beta \text{ or } \pm\widetilde{u^m\beta}. \qquad (\dagger)$$

Now β and $\tilde{\beta}$ both have norm -5. Furthermore, $N(u) = 1$.
So with α as in $(\dagger)$, $\alpha\widetilde{\alpha} = N(\alpha) = (1)^m(-5) = -5$.

Thus $N(\alpha) = 5$ is impossible for $\alpha \in R$ and the equation has no solution.

(iv) We now require those $\alpha \in R$ such that $\alpha\widetilde{\alpha} = -5$.

And again the possibilities for α are $\alpha = \pm u^m\beta$ or $\pm\widetilde{u^m\beta}$, where $m \in \mathbb{Z}$, and as observed above all these have norm -5 and give solutions to our problem. So the solution is

$$\begin{aligned} x &= \pm\frac{\beta u^m + \tilde{\beta}\tilde{u}^m}{2} = \pm\frac{(5+2\sqrt{6})^m(1+\sqrt{6}) + (5-2\sqrt{6})^m(1-\sqrt{6})}{2} \\ y &= \pm\frac{\beta u^m - \tilde{\beta}\tilde{u}^m}{2\sqrt{6}} = \pm\frac{(5+2\sqrt{6})^m(1+\sqrt{6}) - (5-2\sqrt{6})^m(1-\sqrt{6})}{2\sqrt{6}} \end{aligned}$$

for $m \in \mathbb{Z}$.

(v) We may reform the equation by multiplying by 3, obtaining $(3x)^2 - 2y^2 = 3$.
Note that *all* solutions to

$$z^2 - 6y^2 = 3 \qquad (**)$$

will give solutions to our equation, since z^2, and hence z, must be divisible by 3.
Put $\alpha = z + y\sqrt{6}$.

Then $(**)$ demands those $\alpha \in R$ such that $\alpha\widetilde{\alpha} = 3$.
(So α will be a prime in R and a factor of 3.)

Put $\beta = 3 + \sqrt{6}$ and then $N(\beta) = 9 - 6 = 3$.
So β is prime in R and $3 = \beta\tilde{\beta}$ is a prime factorization of 3.

Hence $\alpha \sim \beta$ or $\tilde{\beta}$. i.e. $\alpha = \pm u^m \beta$ or $\pm \widetilde{u^m \beta}$.

Now β and $\tilde{\beta}$ both have norm 3.

So with α as above, $\alpha\widetilde{\alpha} = N(\alpha) = (1)^m 3 = 3$, as required.

Hence the solution to the original equation is (taking care to divide z by 3 to get x):

$$\begin{aligned} x &= \pm\frac{\beta u^m + \tilde{\beta}\tilde{u}^m}{6} = \pm\frac{(5+2\sqrt{6})^m(3+\sqrt{6}) + (5-2\sqrt{6})^m(3-\sqrt{6})}{6} \\ y &= \pm\frac{\beta u^m - \tilde{\beta}\tilde{u}^m}{2\sqrt{6}} = \pm\frac{(5+2\sqrt{6})^m(3+\sqrt{6}) - (5-2\sqrt{6})^m(3-\sqrt{6})}{2\sqrt{6}} \end{aligned}$$

for $m \in \mathbb{Z}$.

6. (i) Take $K = \mathbb{Q}(\sqrt{13})$. Then $13 \equiv 1 \mod 4$.
So we take $R = \mathbb{Z}[\theta]$ $(= \int(K))$, where $\theta = \frac{1+\sqrt{13}}{2}$.

Put $\alpha = x + y\sqrt{13}$. Then our problem, to solve:

$x^2 - 13y^2 = -1$, such that $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ $(*)$

asks for those $\alpha \in \mathbb{Z}[\sqrt{13}]$ such that $N_K(\alpha) = -1$.

Now $N(\alpha) = \pm 1$, so α is a unit.
The fundamental unit of K is easily found to be $u = \frac{1}{2}(3 + \sqrt{13}) = 1 + \theta$.
So we must have $\alpha = \pm u^t$ for some integer t.
Then, since $N(u) = -1$, $N(\alpha) = (-1)^t = -1$ iff t is odd. $(\dagger)$

Again $\mathbb{Z}[\sqrt{13}] = \mathbb{Z}[2\theta] = \mathbb{Z} + 2R$.

So $\mathbb{Z}[\sqrt{13}] = \{\beta \in R \mid \beta \equiv b \mod 2R \text{ for some } b \in \mathbb{Z}\}$.

Thus $\alpha \in \mathbb{Z}[\sqrt{13}]$ demands that α be congruent to an integer mod $2R$.

Now $u^2 = \frac{1}{2}(11 + 3\sqrt{13}) = 4 + \theta$ and $u^3 = 18 + 5\sqrt{13} = 13 + 10\theta \equiv 1 \mod 2R$.
And also $u^{-3} = (-\tilde{u})^3 \equiv 1 \mod 2R$.

Thus, if $t = 3q + r$ with $r = 0$, 1 or 2 then

$u^t = u^{3q}u^r \equiv u^r \equiv 1$, $1 + \theta$ or θ mod $2R$, respectively.

Therefore $\pm u^t$ is congruent to an integer mod $2R$ iff $t \equiv 0 \mod 3$. $(\dagger\dagger)$

So the solutions to $(*)$ are given by those $\alpha = \pm u^t$ satisfying $(\dagger)$ and $(\dagger\dagger)$

That is, we require $t \equiv 3 \mod 6$.

The solutions to $(*)$ are, therefore:

$$\begin{aligned} x &= \pm\frac{u^{6m+3} + \tilde{u}^{6m+3}}{2} \\ y &= \pm\frac{u^{6m+3} - \tilde{u}^{6m+3}}{2\sqrt{13}} \end{aligned}$$

for $m \in \mathbb{Z}$.

(ii): Now $12 = 2^2 \times 3$. So take $K = \mathbb{Q}(\sqrt{3})$ and $R = \mathbb{Z}[\sqrt{3}]$, a UFD (see, e.g., the list in Stewart–Tall, or simply check it as for other cases).

Putting $\alpha = x + 2y\sqrt{3}$ with $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, our equation,

$x^2 - 12y^2 = 13,$

becomes

$N_K(\alpha) = 13.$

So we require those $\alpha = x + z\sqrt{3}$ in $\mathbb{Z}[\sqrt{3}]$ such that

(a) $N(\alpha) = 13$ and
(b) 2 divides z.

Now $13 = \beta\widetilde{\beta}$ where $\beta = 2 + \sqrt{3}$. So 13 splits (since $3 \not| \, 13$).

Thus α is either β or $\widetilde{\beta}$ times a unit.

The fundamental unit of K is easily found to be $u = 2 + \sqrt{3}$, of norm 1.

So α is $\pm\beta u^t$ or its conjugate, for some $t \in \mathbb{Z}$.

Since $N(u) = 1$, all these possibilities have norm 13 and so satisfy (a), above.

Thus it remains to find out which of them satify (b).

Note that $u^{-1} = \tilde{u}$. So if $\alpha = \pm\beta u^t$, then, choosing $\epsilon = \pm 1$ so that $t = \epsilon|t|$,

$$\alpha = \pm(2+\sqrt{3})^t(4+\sqrt{3}) = \pm(2+\epsilon\sqrt{3})^{|t|}(4+\sqrt{3}) \equiv \sqrt{3}^{|t|+1} \mod 2R.$$

So, for this $\alpha = x + z\sqrt{3}$, we have $z \equiv 0 \mod 2$ iff $|t| + 1$ is even, i.e. t odd.

The same argument works for the associates of $\widetilde{\beta}$.

Hence the required α are the $\pm\beta u^{2s+1}$ and their conjugates ($s \in \mathbb{Z}$).

So the solution is:

$$\begin{aligned} x &= \pm\frac{\beta u^{2s+1} + \tilde{\beta}\tilde{u}^{2s+1}}{2} \\ y &= \pm\frac{\beta u^{2s+1} - \tilde{\beta}\tilde{u}^{2s+1}}{4\sqrt{3}} \end{aligned}$$

for $s \in \mathbb{Z}$.

7. $894 = 2 \times 3 \times 149$ and since 2, 3, 5, 7, 11 do not divide 149, it is prime.
Thus 894 is squarefree and hence $\mathcal{O}_{\mathbb{Q}(\sqrt{894})} = \mathbb{Z}[\sqrt{894}]$.
So the fundamental unit is $v = a + b\sqrt{894}$, for some $a, b \in \mathbb{Z}^{>0}$.
Put $u = 299 + 10\sqrt{894}$. Then $u\tilde{u} = 299^2 - 89400 = 1$ so u is a unit.
Hence $u = v^r$ for some $r \in \mathbb{Z}^{>0}$. That is

$u = v^r = a^r + ra^{r-1}b\sqrt{894} + r(r-1)a^{r-2}b^2 894/2 + \cdots.$

If $r > 1$ then, equating rational parts,

$299 \geq a^r + a^{r-2}b^2 894 \geq 894$. Contradiction.

So $r = 1$ and u is the fundamental unit.

8. Check that θ satisfies

$$\theta^3 = \frac{(1+\sqrt[3]{2})^3}{3} = \frac{1 + 3\sqrt[3]{2} + 3\sqrt[3]{2}^2 + 2}{3} = 1 + \sqrt[3]{2} + \sqrt[3]{2}^2$$

and hence

$$(\theta^3 - 1)^3 = \sqrt[3]{2}^3(1+\sqrt[3]{2})^3 = 2 \cdot 3\theta^3\,,$$

the last equality being deduced form the previous equality.

So θ is a root of the *monic* (degree 9) integer polynomial $(x^3-1)^3 - 6x^3$.