Michaelmas 2012, NT III/IV, Solutions to Problem Sheet 5.

1 Let R be a UFD, and let K be its quotient field. Suppose $x \in K$ satisfies a monic equation

$$X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

with coefficients a_i in R and some $n > 0$. Then we have to show that x is already contained in R.

Recall that any $x \in K$ can be written as α/β where α, β are comprime in R (also $\beta \neq 0$). Hence we have

$$(\alpha/\beta)^n + a_{n-1}(\alpha/\beta)^{n-1} + \cdots + a_0\,,$$

and after multiplying by β^n we get

$$\alpha^n = -a_{n-1}\alpha^{n-1}\beta = \cdots - a_0\beta^n\,.$$

Now β divides any term on the right, hence must divide also the left hand side. But then it also must divide α. (Use inductively the fact that if β divides $\alpha\gamma$ and is coprime to α, then it must divide γ.)

Hence β must be a unit, and we conclude that x is indeed already in R.

2 (i) We work in the ring $R = \mathbb{Z}[i]$.

We know that R is Euclidean and hence a UFD.

Note that $R^* = \{\pm 1,\ \pm i\}$.

Put $\alpha = a + bi$ and $N = 2^3 \times 7^4 \times 37^5 \times 41$. Then

$$a^2 + b^2 = 2^3 \times 7^4 \times 37^5 \times 41 \ = N,\ \text{with } a,\ b \in \mathbb{Z} \tag{1}$$

may be written

$$\alpha\widetilde{\alpha} = N,\ \text{with } \alpha \in \mathbb{Z}[i]. \tag{1$'$}$$

If π is an irreducible element of R (and hence a prime element of R, since R is a UFD) which divides α then π divides $\alpha\widetilde{\alpha} = N$.

So π divides one of the prime integer factors p ($p = 2$, 7, 37 and 41) of N.

By results from the lectures, either p is itself irreducible or $p = \pm\alpha_p\widetilde{\alpha}_p = r^2 + s^2$, where $\alpha_p = r + is$ and $\widetilde{\alpha}_p$ are irreducible (and r and $s \in \mathbb{Z}$).

By inspection (trying to solve $p = r^2 + s^2$), we find:

$2 = \alpha_2\widetilde{\alpha}_2 = -i\alpha_2^2$ where $\alpha_2 = 1 + i$ (so 2 ramifies).

7 is prime (hence inert) in R (else $7 = r^2 + s^2$ which can't be done.)

$37 = \alpha_{37}\widetilde{\alpha}_{37}$ where $\alpha_{37} = 6 + i$, so 37 splits.

$41 = \alpha_{41}\widetilde{\alpha}_{41}$ where $\alpha_{41} = 5 + 4i$, so 41 splits.

So $\pi \sim \alpha_2$, α_{37}, $\widetilde{\alpha}_{37}$, α_{41} or $\widetilde{\alpha}_{41}$. And since these primes are non-associate α may be written uniquely as a product of powers of these primes times a unit:

$$\alpha = \left\{\begin{matrix} \pm 1 \\ or \\ \pm i \end{matrix}\right\} \times \alpha_2^r \times 7^s \times \alpha_{37}^t \times \tilde{\alpha}_{37}^u \times \alpha_{41}^v \times \tilde{\alpha}_{41}^w.$$

where r, s, t, u, v, w are non-negative integers. To satisfy (1$'$) the norm of the RHS must be N viz.

$$2^r \times 7^{2s} \times 37^{t+u} \times 41^{v+w} = 2^3 \times 7^4 \times 37^5 \times 41.$$

This holds iff $r = 3$, $s = 2$, $t + u = 5$ (viz. $t = 5 - u = 0$, 1, 2, 3, 4 or 5) and $v + w = 1$ (viz. $v = 1 - w = 0$ or 1).

Thus we have independent choices multiplying up to give

4 (for units) $\times$ 6 (for (t, u)) $\times$ 2 (for (v, w)) $= 48$ choices

for $\alpha \in \mathbb{Z}[i]$ satisfying (1$'$) and hence 48 solutions $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ satisfying (1).

Now every "positive" solution, $(a, b) \in \mathbb{N} \times \mathbb{N}$, gives rise to 4, $(\pm a, \pm b) \in \mathbb{Z} \times \mathbb{Z}$. We easily see that neither a nor b can be 0 in (1). So all solutions arise in this way. So there are $48/4 = 12$ solutions to (1) in $\mathbb{N} \times \mathbb{N}$.

2 (ii) Working as in (i) but with $N = 3^3 \times 41 \times 43$ we find that 3 cannot be written $r^2 + s^2$ so, like 7 in (i), 3 is inert in R. Proceeding as in (i) we find that, in this case, if $\alpha\widetilde{\alpha} = N$ then the power to which 3 occurs in the factorization of α has to be $3/2$, which is not possible. So, in this case there are no solutions.

2 (iii) Suppose that

$$a^2 + 25b^2 = 4 \times 29 \times 113^4 \ (= M, \text{ say}) \text{ with } a,\, b \in \mathbb{Z}. \qquad (*)$$

Put $\alpha = a + 5bi \in \mathbb{Z}[i] = R$, say. So, as before, R is a UFD.

We may then rewrite the equation of $(*)$ as $\qquad \alpha\bar{\alpha} = M. \qquad (**)$

We find $2 = -i(1+i)^2$ ramifies and that $29 = (2+5i)(2-5i)$ and $113 = (7+8i)(7-8i)$ split. We take $\alpha_2 = 1 + i$, $\alpha_{29} = 2 + 5i$ and $\alpha_{113} = 7 + 8i$.

Factoring α in terms of a unit and powers of these primes (and of their conjugates in the split cases), as in (i), we find that the solutions of $(**)$ are, without repetition:

$$\alpha = i^r \times \alpha_2^2 \times \alpha_{29}^t \times \bar{\alpha}_{29}^{(1-t)} \times \alpha_{113}^u \times \bar{\alpha}_{113}^{(4-u)} \qquad (\dagger)$$

where $r = 0$, 1, 2 or 3 and $t = 0$ or 1 and $u = 0$, 1, 2, 3 or 4.

So there are $4 \times 2 \times 5 = 40$ solutions to $(**)$ in R.

But which of these α give a solution to $(*)$?

They are those α with imaginary part divisible by 5,
that is, such that $\alpha \equiv a \mod 5R$ for some $a \in \mathbb{Z}$.

Now, modulo $5R$,

$\alpha_{113} \equiv -2i(1 + i)$,
$\bar{\alpha}_{113} \equiv 2(1 + i)$ and
$\alpha_{29} \equiv \bar{\alpha}_{29} \equiv 2$.

So with α as given at $(\dagger)$:

$$\alpha \equiv i^{r+u}(-1)^u(1 + i)^{2+4} \times 2^{1+4} \equiv (-1)^u i^{r+u+3}$$

(Note: $(1 + i)^2 = 2i$, $2^4 \equiv 1 \mod 5$).

Thus α is congruent to a rational integer mod $5R$ iff the power of i here is even, that is, iff $r \equiv u + 3 \bmod 2$.

But for any choice of t and u exactly half the possibilities for r satisfy this condition.

Thus half the α of $(\dagger)$ give solutions to $(*)$, which therefore has 20 solutions in $\mathbb{Z}^2$ and 5 in $(\mathbb{N})^2$ (cf. previous examples).

(Note that we have proved a bit more, namely that either the real part or the imaginary part of α (but not both) is divisible by 5. This is equivalent to saying that in every solution of

$$a^2 + c^2 = M, \quad a,\ c \in \mathbb{Z}$$

(and from $(\dagger)$ there are 40 of these) exactly one of a or c is divisible by 5. Maybe you can see a quick way of proving this fact (by reducing the equation mod 5). This would provide an alternative way of finishing the problem.)

2 (iv) We have 2 units, all three primes involved are split in $\mathcal{O}_{-}7$, norm of $(a + b\sqrt{-7})/2$ is $2 \cdot 23 \cdot 43$ (note that we should divide by 4 first and then use that $\mathcal{O}_7$ is a UFD), hence we can find $2 \times 2 \times 2 \times 2 = 16$ solutions in $\mathbb{Z}$, as well as 4 ones in $\mathbb{N}$ (they come in packages of 4, as $a = 0$ or $b = 0$ is impossible), e.g. $(a, b) = (53, 27)$.

2 (v) Note that there should be a minus sign in the expression on the left hand side, giving a^2-ab+b^2. There are 6 units ω^j $(j=0,\ldots,5)$ in R; the three primes involved are 3 (ramified) as well as 7 and 61 (both split), all to exponent 1. For example, we find $7 = N(2+\sqrt{-3}) = N(3+2\omega) = N(1-2\omega)$ and $61 = N(7+2\sqrt{-3}) = N(9+4\omega) = N(5-4\omega)$. Overall, we get $6\times1\times2\times2 = 24$ solutions, all of which are integer solutions. This time, they also come in packets of four, but for a different reason: with (a,b) also (b,a), $(-a,-b)$ and $(-b,-a)$ are solutions. Moreover, there is a further symmetry: with (a,b) also $(a,a-b)$ gives a solution. With the help of those symmetries, we actually can group the solutions into two packets of 12, arising from $(a,b) = (11,40)$ and $(16,41)$. Each packet of 12 contains precisely 4 solutions in natural numbers.

2 (vii) Suppose that $a^2-2b^2 = 21$ for some $a,\ b\in\mathbb{Z}$.
If $3 \mid b$ then $3 \mid a$ and $3^2 \mid a^2-2b^2 = 21$. #
So $3 \not| \, b$ or a. And hence, $a^2 \equiv b^2 \equiv 1 \bmod 3$.
But $a^2 \equiv 2b^2 \bmod 3$. So $1 \equiv 2 \bmod 3$. #
Therefore $a^2-2b^2 = 21$ has no solutions $a,\ b\in\mathbb{Z}$.

2 (viii) We work in the ring $R = \mathbb{Z}[\sqrt{-2}]$.
We know that R is Euclidean and hence a UFD.

We have already seen $R^* = \{\pm1\}$.

Put $\alpha = a+b\sqrt{-2}$ and $N = 3^{14}\times43^{10}$. Then

$$a^2+2b^2 = 3^{14}\times43^{10} \;= N,\ \text{with } a,\ b\in\mathbb{Z} \tag{1}$$

may be written

$$\alpha\widetilde{\alpha} = N,\ \text{with } \alpha\in\mathbb{Z}[\sqrt{-2}]. \tag{1'}$$

If π is a prime of R which divides α then π divides $\alpha\widetilde{\alpha} = N$.
So π divides one of the prime integer factors (3 and 43) of N
We proceed to factorise these in R. We see by inspection (i.e. we try to solve $p = \pm\alpha_p\widetilde{\alpha}_p = r^2+2s^2$, where $\alpha_p = r+s\sqrt{-2}$) that

$3 = \alpha_3\widetilde{\alpha}_3$ where $\alpha_3 = 1+\sqrt{-2}$, so 3 splits in R

$43 = \alpha_{43}\widetilde{\alpha}_{43}$ where $\alpha_4 = 5+3\sqrt{-2}$, so 43 splits R.

So $\pi\sim\alpha_3,\ \widetilde{\alpha}_3,\ \alpha_{43}$ or $\widetilde{\alpha}_{43}$. And since these primes are non-associate α may be written uniquely as a product of powers of these primes times a unit:

$$\alpha = \pm1\times\alpha_3^t\times\tilde{\alpha}_3^u\times\alpha_{43}^v\times\tilde{\alpha}_{43}^w.$$

where $t,\ u,\ v,\ w$ are non-negative integers. To satisfy (1′) the norm of the RHS must be N vis.

$$3^{t+u}\times43^{v+w} = 3^{14}\times43^{10}.$$

This holds iff $t+u = 14$ (viz. $t = 14-u = 0,\ 1,\ 2,\ldots$ or 14) and $v+w = 10$ (viz. $v = 10-w = 0,\ 1,\ 2,\ldots$ or 10).

Thus we have the following independent choices:

2 (for units) $\times$ 15 (for (t,u)) $\times$ 11 (for (v,w)).

This gives 330 choices for the element $\alpha\in\mathbb{Z}[\sqrt{-2}]$ satisfying (1′) and hence 330 solutions $(a,b)\in\mathbb{Z}\times\mathbb{Z}$ satisfying (1).

Now every "positive" solution, $(a,b)\in\mathbb{N}\times\mathbb{N}$, gives rise to 4, $(\pm a,\pm b)\in\mathbb{Z}^*\times\mathbb{Z}^*$. This does not exhaust all the solutions in $\mathbb{Z}\times\mathbb{Z}$ since there are also the solutions $(\pm3^7 43^5, 0)$. So there are $330-2 = 328$ solutions in $\mathbb{Z}^*\times\mathbb{Z}^*$ and therefore $328/4 = 82$ solutions to (1) in $\mathbb{N}\times\mathbb{N}$.

3 We work in the ring $R = \mathbb{Z}[\sqrt{-2}]$. We know (from the lectures) that R is Euclidean and hence a UFD. Moreover, we have already seen that the units of R are given by $R^* = \{\pm 1\}$.

One can re-interpret the equation

$$a^2 + 2b^2 = p^{11}q^{13} \ = N, \text{ with } a,\ b \in \mathbb{Z} \tag{1}$$

using norms, putting $\alpha = a + b\sqrt{-2}$ and $N = p^{11}q^{13}$. Then

$$\alpha\tilde{\alpha} = N, \text{ with } \alpha \in \mathbb{Z}[\sqrt{-2}]. \tag{1'}$$

Now we analyse the possible shape of primes dividing α.
Any prime π of R which divides α also divides $\alpha\tilde{\alpha} = N = p^{11}q^{13}$, hence divides either one of the prime integer factors (p and q) of N.

Since we work in a quadratic field, we can conclude that, up to sign, π has norm p, p^2, q or q^2. In fact, since we work in an imaginary quadratic field, only positive norms occur, so

$$N(\pi) \in \{p, p^2, q, q^2\}\,.$$

We will now restrict further by showing that p^2 and q^2 cannot occur. More precisely, we have the

Claim: Both p and q split in $\mathbb{Z}[\sqrt{-2}]$.

It suffices to show the claim for p, as q can be treated completely analogously.

The power of p dividing N is odd, hence there must be a prime α_p of norm p dividing α (here we use that there is at least one solution to (1′)); so p cannot be inert. But p cannot be ramified either: $p = \alpha_p\tilde{\alpha}_p$ with $\alpha_p \sim \tilde{\alpha}_p$ would necessarily entail $\alpha_p = -\tilde{\alpha}_p$ (since $R^* = \{\pm 1\}$, and $\alpha_p = \tilde{\alpha}_p$ would imply $\alpha_p \in \mathbb{Q}$), so if we write $\alpha_p = c + d\sqrt{-2}$, then we must have $c = 0$ and so $\alpha_p = d\sqrt{-2}$ with $p = N(\alpha_p) = 2d^2$. This contradicts our assumption that p is odd.

Conclusion: Any prime π of R dividing α is associate to either one of α_p, $\tilde{\alpha}_p$, α_q or $\tilde{\alpha}_q$.
Since these primes are non-associate, α may be written uniquely as a product of powers of these primes times a unit:

$$\alpha = \pm 1 \times \alpha_p^t \times \tilde{\alpha}_p^u \times \alpha_q^v \times \tilde{\alpha}_q^w\,.$$

where t, u, v, w are non-negative integers. To satisfy (1′) the norm of the RHS must be equal to N, which gives

$$p^{t+u} \times q^{v+w} = p^{11} \times q^{13}.$$

This holds iff $t + u = 11$ (viz. $t = 11 - u = 0,\ 1,\ 2, \ldots$ or 11) and $v + w = 13$ (viz. $v = 13 - w = 0,\ 1,\ 2, \ldots$ or 13).

Thus we have the following independent choices:

2 (for units) $\times$ 12 (for (t, u)) $\times$ 14 (for (v, w)).

This gives 336 choices for the element $\alpha \in \mathbb{Z}[\sqrt{-2}]$ satisfying (1′) and hence 336 solutions $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ satisfying (1).

4 We work in the ring $R = \mathbb{Z}[(1 + \sqrt{-11})/2]$. From the lectures we know that R is a UFD, and we find again that $R^* = \{\pm 1\}$.

Put $\alpha = X + Y\sqrt{-11}$ and $N = 4p^{23}$. Then

$$X^2 + 11Y^2 = 4p^{23} \ = N, \text{ with } X,\ Y \in \mathbb{Z} \tag{1}$$

may be written

$$\alpha\tilde{\alpha} = N, \text{ with } \alpha \in \mathbb{Z}[\sqrt{-11}]. \tag{1'}$$

First consider the primes dividing 2: note that since there is no integer solution to $c^2 + 11d^2 = 8$, there is no element of norm 2 in R. So 2 is inert and prime in R.

Then analyse the decomposition of p: since p is not prime in R, we deduce $p = \alpha_p\tilde{\alpha}_p$ for some $\alpha_p = (c + d\sqrt{-11})/2 \in R$.

We show that p does not ramify: if $\alpha_p \sim \tilde{\alpha}_p$ then $\alpha_p = -\tilde{\alpha}_p$ (since $R^* = \{\pm 1\}$). This would imply $c = 0$, i.e., $\alpha = d\sqrt{-11}/2$, whence $p = 11b^2/4$ and p must be 11. #

Conclusion: The prime integer p *splits* as $p = \alpha_p\tilde{\alpha}_p$.

Now if π is a prime of R which divides α then π also divides $\alpha\tilde{\alpha} = 2^2(\alpha_p\tilde{\alpha}_p)^{23}$. Hence the possibilities for such π are $\pi \sim 2$, α_p or $\tilde{\alpha}_p$.

Since these primes are non-associate, α may be written uniquely as a product of powers of these primes times a unit:

$$\alpha = \pm 1 \times 2^s \times \alpha_p^t \times \tilde{\alpha}_p^u,$$

where s, t and u are non-negative integers. To satisfy $(1')$ the norm of the RHS must be N, i.e.

$$2^{2s} \times p^{t+u} = 4p^{23}.$$

This holds iff $s = 1$ and $t + u = 23$.

Note that, in (1), $p \mid X \iff p \mid Y$.

We are looking for solutions with $p \nmid X$ and $p \nmid Y \iff p\,(= \alpha_p\tilde{\alpha}_p) \nmid \alpha \iff$ either $u = 0$ or $v = 0$.

Clearly, with this condition, we get just 4 elements α of norm N.
Moreover, since for each of these we need $s = 1$, we find $\alpha \in 2R \subset \mathbb{Z}[\sqrt{-11}]$.
So each α yields a solution to our problem and there are therefore 4 such solutions.

5 The equation in question

$$X^2 + 11 = Y^3 \tag{1}$$

can be rewritten as

$$\alpha\tilde{\alpha} = y^3$$

with $\alpha = X + \sqrt{-11}$, and $X \in \mathbb{Z}$.

We want to work in the ring $R = \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$ instead of $\mathbb{Z}[\sqrt{-11}]$ since the former is a UFD (as we know from set work), and so we can apply our usual arguments.

For this, we first need to distinguish the primes dividing both α and $\tilde{\alpha}$ from the primes dividing precisely one of them.

The former are the primes π dividing a gcd of α and $\tilde{\alpha}$ (in a UFD, we can form a gcd of two numbers!), hence dividing also their sum $\alpha + \tilde{\alpha} = 2X$, of norm $4X^2$, and their difference $\alpha - \tilde{\alpha} = 2\sqrt{-11}$, of norm $4 \cdot 11$.

Now X cannot be divisible by 11 ⟦otherwise 11 divides the LHS of (1) and hence also its RHS, but every exponent on the RHS is divisible by 3, while the LHS is not divisible by 11^2⟧.

Hence the only possibility for a π dividing $\gcd(\alpha, \tilde{\alpha})$ is $\pi|2$.

We note that 2 is inert in R $\left(\text{as } N\left(\frac{a+b\sqrt{-11}}{2}\right) = 2 \text{ is impossible for } a, b \in \mathbb{Z} \text{ where } a \equiv b \pmod 2\right)$, and so $\pi \sim 2$ or $\pi \sim 1$. This implies that α has the form

$$\alpha = u \times 2^{s_0}\pi_1^{s_1} \cdots \pi_r^{s_r}$$

for some unit u and (mutually non-associate) irreducibles π_i $(i = 1, \ldots, r)$ which are also non-associate to 2, and for $\tilde{\alpha}$ we get the same powers but instead for the irreducibles $\tilde{\pi}_i$. Therefore

$$\alpha\tilde{\alpha} = u\tilde{u} \times 2^{2s_0}\pi_1^{s_1}\tilde{\pi}_1^{s_1} \cdots \pi_r^{s_r}\tilde{\pi}_r^{s_1}$$

and we know that units in R must have the form $u = \pm 1$, so $u\tilde{u} = 1$. Furthermore, we can deduce that all exponents s_i $(i = 0, \ldots, r)$ are divisible by 3. This allows us to take a cube root β of α in R by setting

$$\beta := 2^{s_0/3}\pi_1^{s_1/3} \cdots \pi_r^{s_r/3} .$$

But β must also have the form $\frac{m+n\sqrt{-11}}{2}$ for some $m, n \in Z$ with $m \equiv n \pmod 2$. This yields the further constraint (we multiply both sides by 8 to get rid of denominators)

$$\begin{aligned} 8(X + \sqrt{-11}) = 8\alpha &= (2\beta)^3 = (m + n\sqrt{-11})^3 \\ &= m^3 - 33mn^2 + \sqrt{-11}(3m^2 n - 11n^3) . \end{aligned}$$

Comparing the coefficient of $\sqrt{-11}$ gives the condition

$$n(3m^2 - 11n^2) = 8 ,$$

hence in particular $n|8$, which already cuts it down to only 8 possible cases,

$$n \in \{\pm 1, \pm 2, \pm 4, \pm 8\},$$

and this will produce only two solutions for the remaining factor: for $n = -1$, this leads to $m = \pm 1$, while $n = 2$ allows a further solution $m = \pm 4$. All the other possibilities for n easily lead to a quadratic equation for m which has no integer solutions.

Conclusion: the only possible solutions are given for

$$\beta \in \left\{ \frac{1 - \sqrt{-11}}{2}, 2 + \sqrt{-11} \right\}$$

which leads, via $\alpha = \beta^3$, to the following solutions of (1):

$$(X, Y) = (\pm 4, 3) \quad \text{or} \quad (X, Y) = (\pm 58, 15) .$$