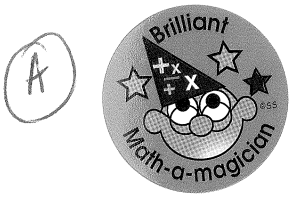

A

ALGEBRA AND NUMBER THEORY HOMEWORK

Matthew Palmer - Group 4

Due 10/11/09

35)

We have

$$R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}.$$

(i)

We have

$$(1 - \sqrt{2})(-1 - \sqrt{2}) = 1$$

— so there exists a β such that $(1 - \sqrt{2})\beta = 1$, and hence $1 - \sqrt{2}$ is a unit. ✓

Now, let α be a unit. Then

$$\alpha\beta = 1 = \beta\alpha$$

for some $\beta \in \mathbb{Z}[\sqrt{2}]$, and hence $N(\alpha\beta) = N(1)$ for some $\beta \in \mathbb{Z}[\sqrt{2}]$ (where N is the map $\mathbb{Z}[\sqrt{2}] \to \mathbb{Z}$ such that

$$N(a_1 + a_2\sqrt{2}) = a_1^2 - 2a_2^2. \text{)}$$

We know that $N(\alpha\beta) = N(\alpha)N(\beta)$ — so

$$N(\alpha)N(\beta) = 1.$$

The only units in $\mathbb{Z}$ are 1 and -1 — so if α is a unit, $N(\alpha) = \pm 1$. ✓

Now, suppose $N(\alpha) = \pm 1$ for some general $\alpha \in \mathbb{Z}[\sqrt{2}]$. Then

$$a_1^2 - 2a_2^2 = \pm 1$$

$$a_1 = \sqrt{2a_2^2 \pm 1}$$

(where this root is in $\mathbb{Z}$.) So we have $\alpha = \sqrt{2a_2^2 \pm 1} + a_2\sqrt{2}$. Choose $\beta = \pm(\sqrt{2a_2^2 \pm 1} - a_2\sqrt{2})$ — then

$$\alpha\beta = \pm(\sqrt{2a_2^2 \pm 1} + a_2\sqrt{2})(\sqrt{2a_2^2 \pm 1} - a_2\sqrt{2}) = \pm(2a_2^2 \pm 1 - 2a_2^2) = 1.$$

So if $N(\alpha) = \pm 1$, then α is a unit, and hence α is a unit if and only if $N(\alpha) = \pm 1$.

✓ Excellent

(ii)

Let u be a unit. Then

$$N(u) = \pm 1.$$

First we prove by induction that u^n is a unit for all $n \in \mathbb{Z}^+$. The base case of $n = 0$ is trivial — $u^0 = 1 \; \forall \; u \in \mathbb{C}$, and 1 is certainly a unit in $\mathbb{Z}[\sqrt{2}]$. Now we just need to prove the inductive step. Suppose that u^n is a unit. Then

$$N(u^n) = \pm 1.$$

We want to show that $u^{n+1} = u^n \cdot u$ is a unit. We know that α is a unit if and only if $N(\alpha) = \pm 1$ — so u^{n+1} is a unit if and only if

$$N(u^{n+1}) = \pm 1.$$

But $N(u^{n+1}) = N(u^n) \cdot N(u)$, and $N(u^n), N(u) \in \{1, -1\}$ — so $N(u^{n+1}) = \pm 1$, and hence u^{n+1} is a unit. And if u^n is a unit, u^{-n} is certainly a unit, as

$$u^n \cdot u^{-n} = u^0 = 1.$$

Then u^n is a unit for all $n \in \mathbb{Z}$. Now, if u^n is a unit, $-u^n$ is also a unit, as

$$(-u^n)(-u^{-n}) = (-1)^2 u^0 = 1.$$

Therefore all elements of the form $\pm u^n$ are units. Now we need only prove that all $\pm u^n$ are distinct. We know that $u^m = -u^m$ implies $u^m = 0$, and $u^m \neq 0 \; \forall \; m \in \mathbb{Z}$ — now suppose that $u^m = \pm u^n$ for $m \neq n$. Then

$$u^m u^{-n} = \pm u^n u^{-n}$$

$$u^{m-n} = \pm 1.$$

So $u^a = \pm 1$ for $a \neq 0$. But $u \in \mathbb{R}$, and

$$x^b = \pm 1, x \in \mathbb{R}, a \in \mathbb{Z} \Leftrightarrow x \in \{-1, 1\} \text{ or } b = 0.$$

We have $u \notin \{-1, 1\}$, and $a \neq 0$ — so $u^a \neq \pm 1$, and hence we have a contradiction. So $u^m \neq \pm u^n$ if $m \neq n$, and $u^m \neq -u^m \; \forall \; m \in \mathbb{Z}$ and hence all the units are distinct. So R^* has infinitely many units.

Great

(iii)

Consider the equation

$$X^2 - 2Y^2 = \pm 1, \; X, Y \in \mathbb{Z}.$$

The solution set of this equation comprises all the units in $\mathbb{Z}[\sqrt{2}]$. Suppose (a, b), with $a > 1, b > 1$, satisfies the equation — then

$$a^2 - 2b^2 = \pm 1.$$

Now suppose $a' = 2b - a, b' = a - b$. Then

$$a'^2 - 2b'^2 = (2b - a)^2 - 2(a - b)^2 = 4b^2 - 4ab + a^2 - 2a^2 + 4ab - 2b^2 = 2b^2 - a^2 = -(a^2 - 2b^2) = \mp 1.$$

So (a', b') is another solution to the equation.

Furthermore, since we know $b > 1$, clearly $2b^2 > 2$. We also know that

$$a^2 - 2b^2 = \pm 1 < 2,$$

and we can combine the two facts to give

$$a^2 - 2b^2 < 2b^2$$

$$a^2 < 4b^2.$$

As $a, b > 0$, this implies

$$a < 2b,$$ ✓

and from this we can deduce both that $2b - a > 0$ and hence that $a' > 0$, and that $a - b < b$, and hence that $b' < b$. Also from $b > 1$, we know that

$$-b^2 < -1,$$

and hence

$$-b^2 < a^2 - 2b^2.$$

So

$$a^2 > b^2,$$

and hence, again using $a, b > 0$,

$$a > b.$$ ✓

Again, we can deduce two facts from this — one being that $a - b > 0$ and hence that $b' > 0$, and the other being that $2b < 2a$, which implies that $2b - a < a$ and hence that $a' < a$. So if (a, b) is a solution of $X^2 - 2Y^2 = \pm 1$, then $(a', b') = (2b - a, a - b)$ is another solution, and obeys $0 < a' < a, 0 < b' < b$. ✓

We know that $3^2 - 2 \cdot 2^2 = 1$, and hence that $(a, b) = (3, 2)$ is a solution — so $((2 \cdot 2) - 3, 3 - 2) = (1, 1)$ is also a solution. This is clearly the smallest solution, as $(1, 0)$ does not have $a', b' > 0$.

Now, let $\alpha = \pm(a + b\sqrt{2})$ be any unit in R with $a, b > 1$. Then, if we multiply by $\mp(1 - \sqrt{2}) = \mp u$, we get

$$-(a + b\sqrt{2})(1 - \sqrt{2}) = -(a + b\sqrt{2} - \sqrt{2}a - 2b) = (2b - a) + (a - b)\sqrt{2}.$$

Call this solution $\alpha' = a' + b'\sqrt{2}$. We showed earlier that this element will have $0 < a' < a, 0 < b' < b$. Now, either $\alpha' = 1 + \sqrt{2}$, in which case we are done, or we still have $a', b' > 1$. Multiply again and again by $\mp(1 - \sqrt{2}) = \mp u$ until we get $1 + \sqrt{2}$ (and eventually we will, as the coefficients keep decreasing towards 1). ✓ If we multiply n times, we have $\alpha = (\mp u)^n(1 + \sqrt{2}) = (\mp u)^n u^{-1} = \mp u^{n-1}$.

We can apply the same process to any unit $\beta = \pm(a - b\sqrt{2}) \in R$ with $a, b > 1$, except we multiply by $\mp(1 + \sqrt{2}) = \mp u^{-1}$, and express any unit of this type as $\mp u^{1-n}$.

Units of type α and β comprise all units in R (except for 1, which can be divided by $1 - \sqrt{2}$ to give $1 + \sqrt{2}$) — hence all units in R are of the form $\pm u^n, n \in \mathbb{Z}$.

✓ Great stuff!