

MATH 601 (DUE 10/2)

HIDENORI SHINOHARA

CONTENTS

1. The Quadratic Equation $x^2 - 2y^2 = n$	1
--	---

1. THE QUADRATIC EQUATION $x^2 - 2y^2 = n$

Exercise. (Problem 15) Find a solution to $x^2 - 2y^2 = 7$.

Proof. $3^2 - 2 \cdot 1^2 = 9 - 2 = 7$. Thus $(x, y) = (3, 1)$ is a solution to $x^2 - 2y^2 = 7$. \square

Exercise. (Problem 16) Is 7 irreducible in $\mathbb{Z}[\sqrt{2}]$? If not, find a factorization into irreducible elements.

Proof. By Problem 3 from the previous assignment, we know that $\alpha \in \mathbb{Z}[\sqrt{2}]$ is a unit if and only if $N(\alpha) = \pm 1$. We will use this result in this solution.

By Problem 15, we know that $7 = (3 + \sqrt{2})(3 - \sqrt{2})$. Since $N(3 + \sqrt{2}) = N(3 - \sqrt{2}) = 7 \neq \pm 1$, 7 can be expressed as a product of two non-unit elements, so 7 is not irreducible.

Suppose $3 + \sqrt{2} = (a + b\sqrt{2})(c + d\sqrt{2})$ for some $a, b, c, d \in \mathbb{Z}$. By Problem 2 from the previous assignment, we know that $N(3 + \sqrt{2}) = N(a + b\sqrt{2})N(c + d\sqrt{2})$. Since N maps $\mathbb{Z}[\sqrt{2}]$ into integers, exactly one of $N(a + b\sqrt{2})$ and $N(c + d\sqrt{2})$ must be 1 or -1, and the other one is 7 or -7. Therefore, one of $a + b\sqrt{2}$ or $c + d\sqrt{2}$ is a unit, so $3 + \sqrt{2}$ is irreducible.

Similarly, if $3 - \sqrt{2} = (a' + b'\sqrt{2})(c' + d'\sqrt{2})$, then $7 = N(3 - \sqrt{2}) = N(a' + b'\sqrt{2})N(c' + d'\sqrt{2})$. Therefore, one of $a' + b'\sqrt{2}$ or $c' + d'\sqrt{2}$ is a unit, so $3 - \sqrt{2}$ is irreducible. \square

Exercise. (Problem 17) Let $p \in \mathbb{Z} \setminus \{0\}$ and suppose $\alpha\beta = p$ in $\mathbb{Z}[\sqrt{2}]$. Show that $\beta = c\gamma(\alpha)$ with $c \in \mathbb{Q}$.

Proof. Choose $a, b, c, d \in \mathbb{Z}$ such that $a + b\sqrt{2} = \beta, c + d\sqrt{2} = \alpha$. Since $\alpha\beta = p \neq 0$, $\alpha \neq 0$. This implies at least one of c or d is nonzero. Therefore, $\gamma(\alpha) = c - d\sqrt{2} \neq 0$.

We have $\alpha\beta = (ac + 2bd) + \sqrt{2}(ad + bc)$. Since $\alpha\beta \in \mathbb{Z}$, $ad + bc = 0$.

$$\begin{aligned} \frac{\beta}{\gamma(\alpha)} &= \frac{a + b\sqrt{2}}{c - d\sqrt{2}} \\ &= \frac{(a + b\sqrt{2})(c + d\sqrt{2})}{c^2 - 2d^2} \\ &= \frac{(ac + 2bd) + (ad + bc)\sqrt{2}}{c^2 - 2d^2} \\ &= \frac{ac + 2bd}{c^2 - 2d^2}. \end{aligned}$$

Therefore, $\frac{\beta}{\gamma(\alpha)} = \frac{ac+2bd}{c^2-2d^2} \in \mathbb{Q}$. In other words, $\beta = \frac{ac+2bd}{c^2-2d^2}\gamma(\alpha)$. \square

Exercise. (Problem 18) Let $p \in \mathbb{Z}$ be an odd prime. Show that $p = N(\alpha)$ for some $\alpha \in \mathbb{Z}[\sqrt{2}]$ if and only if p is not irreducible as an element of $\mathbb{Z}[\sqrt{2}]$.

Proof. By Problem 3 from the previous assignment, we know that $\alpha \in \mathbb{Z}[\sqrt{2}]$ is a unit if and only if $N(\alpha) = \pm 1$. We will use this result in this solution.

Suppose $p = N(\alpha)$ for some $\alpha \in \mathbb{Z}[\sqrt{2}]$. Since $N(\alpha) = \alpha\gamma(\alpha)$, p can be written as a product of α and $\gamma(\alpha)$.

- $N(\alpha) = p \neq \pm 1$, so α is not a unit.
- Since $N(\gamma(\alpha)) = \gamma(\alpha)\gamma(\gamma(\alpha)) = \gamma(\alpha)\alpha = N(\alpha) = p \neq \pm 1$, $\gamma(\alpha)$ is not a unit.

Therefore, p is a product of two non-unit elements $\alpha, \gamma(\alpha)$, so p is not irreducible.

On the other hand, suppose that p is not irreducible as an element of $\mathbb{Z}[\sqrt{2}]$. Then $p = \alpha\beta$ where $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$ are non-unit elements. Then $N(p) = N(\alpha)N(\beta)$.

- $N(p) = p^2$ because p is an integer.
- $N(\alpha) \neq \pm 1$ because α is not a unit.
- $N(\beta) \neq \pm 1$ because β is not a unit.

Since $N(\alpha), N(\beta)$ are both integers, $N(\alpha) = N(\beta) = p$ or $N(\alpha) = N(\beta) = -p$. If $N(\alpha) = p$, then we are done. If $N(\alpha) = -p$, then $N(\alpha(1+\sqrt{2})) = N(\alpha)N(1+\sqrt{2}) = (-p)(-1) = p$. \square

Exercise. (Problem 19) Let $p \in \mathbb{Z}$ be an odd prime. Show that $x^2 - 2y^2 = p$ has a solution if and only if p is not irreducible in $\mathbb{Z}[\sqrt{2}]$.

Proof. Let an odd prime p be given. There exists an $\alpha \in \mathbb{Z}[\sqrt{2}]$ such that $p = N(\alpha)$ if and only if there exist $x, y \in \mathbb{Z}$ such that $p = x^2 - 2y^2$ because $N(x + \sqrt{2}y) = x^2 - 2y^2$. By combining this with the results of Problem 18, we have $x^2 - 2y^2 = p$ has a solution if and only if p is not irreducible in $\mathbb{Z}[\sqrt{2}]$. \square