Autumn Semester 2019

Introduction to Algebraic Number Theory

Lecturer: Prof. Dr. Özlem Imamoglu
Coordinator: Dr. Danylo Radchenko

Solutions to Exercise Sheet 1

Exercise 1.1. Consider the ring $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\}$.

(a) Show that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain with respect to $N(\alpha) = |\alpha|^2 = a^2 + 2b^2$, where $\alpha = a + b\sqrt{-2}$;

(b) Show that $\mathbb{Z}[\sqrt{-2}]^\times = \{\pm 1\}$;

(c) Show that if y is an odd integer, then $\gcd(y - \sqrt{-2}, y + \sqrt{-2}) = 1$.

Solution. (a) We view $\mathbb{Z}[\sqrt{-2}]$ as a subset of $\mathbb{C}$: it is a rectangular grid where each rectangle has side lengths 1 and $\sqrt{2}$.

Let $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$, and assume that $\beta \neq 0$. Let γ be the element of the grid (i.e., of $\mathbb{Z}[\sqrt{-2}]$) that is the closest to $\alpha/\beta \in \mathbb{C}$. Then the distance $|\gamma - \alpha/\beta|$ is less than or equal to half the length of a diagonal in the rectangle with sides 1 and $\sqrt{2}$, thus $|\gamma - \alpha/\beta|^2 \leq \frac{3}{4}$. Therefore if we set $\delta = \alpha - \beta\gamma$, then $\alpha = \gamma\beta + \delta$, and $N(\delta) \leq \frac{3}{4}N(\beta) < N(\beta)$, showing that $\mathbb{Z}[\sqrt{-2}]$ is Euclidean.

(b) The norm $N(\alpha)$ is multiplicative, and thus if $a + b\sqrt{-2}$ is a unit, then we must have $N(a+b\sqrt{-2}) = a^2+2b^2 = \pm 1$. A trivial estimate $1 = |a^2+2b^2| \geq 2b^2$ implies $b = 0$, and $a^2 = \pm 1$ implies that $a = \pm 1$.

(c) Assume that $\alpha \in \mathbb{Z}[\sqrt{-2}]$ is a common divisor of $y - \sqrt{-2}$ and $y + \sqrt{-2}$. Then α divides $2\sqrt{-2} = (y + \sqrt{-2}) - (y - \sqrt{-2})$, and thus $N(\alpha)$ divides $N(2\sqrt{-2}) = 8$. On the other hand, $N(\alpha)$ divides $N(y + \sqrt{-2}) = y^2 + 2$, which is odd, so $N(\alpha)$ also has to be odd. Thus $N(\alpha) = 1$, which implies that $\alpha = \pm 1$.

Exercise 1.2. Let $\omega = e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{-3}}{2}$, and consider the ring $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$.

(a) Show that $\mathbb{Z}[\omega]$ is Euclidean with respect to $N(a + b\omega) = a^2 - ab + b^2$;

(b) Show that $\mathbb{Z}[\omega]^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$;

(c) Using the fact that $\mathbb{Z}[\omega]$ is a UFD show that for all primes $p > 3$ we have

$$p = a^2 - ab + b^2 \ (a, b \in \mathbb{Z}) \quad \Leftrightarrow \quad p \equiv 1 \pmod 3 .$$

Solution. (a) When embedded into $\mathbb{C}$, the set $\mathbb{Z}[\omega]$ forms a triangular lattice. Let $\alpha, \beta \in \mathbb{Z}[\omega]$, $\beta \neq 0$, and let γ be the element of $\mathbb{Z}[\omega]$ that is the closest to $\alpha/\beta \in \mathbb{C}$. Since the point furthest from the vertices in an equilateral triangle is the center, we get that the distance $|\gamma - \alpha/\beta|$ is less than or equal to $\frac{1}{\sqrt{3}}$, thus $|\gamma - \alpha/\beta|^2 \leq \frac{1}{3}$. Therefore if we set $\delta = \alpha - \beta\gamma$, then $\alpha = \gamma\beta + \delta$ and $N(\delta) \leq \frac{1}{3}N(\beta) < N(\beta)$, showing that $\mathbb{Z}[\omega]$ is Euclidean.

(b) If $a+b\omega$ is a unit, then we must have $N(a+b\omega) = a^2 - ab + b^2 = 1$. From $1 = a^2 - ab + b^2 = (a - b/2)^2 + 3b^2/4 \geq 3b^2/4$, we get $|b| \leq 1$. If $b = 0$, then we have $a^2 = 1$ and thus $a = \pm 1$. Similarly, for $b = 1$ we get $a^2 = a$, and for $b = -1$ we get $a^2 + a = 0$, so we get the following set of solutions $\{(1,0), (-1,0), (1,1), (0,1), (-1,-1), (0,-1)\}$, which corresponds to $\{\pm 1, \pm\omega, \pm\omega^2\}$.

(c) Since $a^2 - ab + b^2 \equiv (a+b)^2 \pmod 3$, we have that $a^2 - ab + b^2 \equiv 0, 1 \pmod 3$. Thus, if $p > 3$ and $p = a^2 - ab + b^2$, then we must have $p \equiv 1 \pmod 3$.

Now assume that $p \equiv 1 \pmod 3$. Since the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$, which is divisible by 3, it must contain a cyclic subgroup of order 3, and thus there exists $x \not\equiv 1 \pmod p$ such that $x^3 \equiv 1 \pmod p$. Since $x^3 - 1 = (x-1)(x^2 + x + 1)$, we have $x^2 + x + 1 \equiv 0 \pmod p$. (Alternatively, the existence of x follows from the fact that $(\frac{-3}{p}) = 1$ using quadratic reciprocity.)

Therefore, p divides $x^2 + x + 1 = (x - \omega)(x + 1 + \omega)$. If p were prime in $\mathbb{Z}[\omega]$, then this would mean that it divides one of $x - \omega$ or $x + 1 + \omega$, which is impossible since $\frac{x-\omega}{p}, \frac{x+1+\omega}{p} \notin \mathbb{Z}[\omega]$. Therefore, p is not prime in $\mathbb{Z}[\omega]$, and since $\mathbb{Z}[\omega]$ is a UFD, p must have a nontrivial factorization $p = (a + b\omega)(c + d\omega)$. Since $N(p) = p^2$, we must have $N(a + b\omega) = p$, and hence $p = a^2 - ab + b^2$.

Exercise 1.3. Find all integral solutions of

(a) $y^2 = x^3 + 7$;

(b) $y^2 = x^3 - 6$;

(c) $y^2 = x^3 - 4$.

Solution. (a) Considering the equation modulo 4 we see that y has to be even, and that $x \equiv 1 \pmod 4$. Rewrite the equation as

$$y^2 + 1 = x^3 + 8 = (x+2)(x^2 - 2x + 4)\,.$$

Since $x \equiv 1 \pmod 4$, we have $x + 2 \equiv 3 \pmod 4$, and since $y^2 + 1 > 0$, we must have $x + 2 > 0$. Then $x+2$ must have a nontrivial prime divisor $p \equiv 3 \pmod 4$ (since if all prime divisors of $x + 2$ were $\equiv 1 \pmod 4$, then so would be $x + 2$). But then $y^2 \equiv -1 \pmod p$, i.e., -1 is a quadratic residue modulo p, which contradicts the fact that the Legendre symbol is $(\frac{-1}{p}) = (-1)^{(p-1)/2} = -1$. Therefore, the equation has no integral solutions.

(b) Considering the equation modulo 4 we see that x and y have to be odd. Then, reducing modulo 8 we have $y^2 \equiv 1 \pmod 8$, and from this, using $x^3 \equiv x \pmod 8$ (since x is odd), we get $x \equiv 7 \pmod 8$.

Rewrite the equation as $y^2 - 2 = x^3 - 8 = (x-2)(x^2 + 2x + 4)$. Since $y = 0, \pm 1$ do not work, we may assume that $y^2 - 2 > 0$, and hence $x > 2$. Then $x - 2$ is a positive integer $\equiv 5 \pmod 8$, and thus it must have a prime divisor $p \equiv \pm 3 \pmod 8$ (again, otherwise we would have $x - 2 \equiv \pm 1 \pmod 8$). But then $y^2 \equiv 2 \pmod p$, i.e., 2 is a quadratic residue modulo p, but this contradicts the supplementary law of quadratic reciprocity that tells us $(\frac{2}{p}) = (-1)^{(p^2-1)/8} = -1$. Therefore, the equation has no integral solutions.

(c) We will use the fact that $\mathbb{Z}[i]$ is a UFD (since it is Euclidean). We factorize the equation as $(y + 2i)(y - 2i) = x^3$. Consider two cases.

If y is odd, then $y+2i$ and $y-2i$ are coprime, and hence both have to be cubes in $\mathbb{Z}[i]$ (note that units in $\mathbb{Z}[i]$ are all cubes).

If y is even, then considering the equation modulo 8 we see that $y = 4k+2$, $x = 2l$. But then $(y \pm 2i)/(1 \pm i)^3 = \mp i - k(1 \pm i)$ are coprime and their product is l^3.

Hence, in both cases we have $y + 2i = (a + bi)^3$, and thus $b(3a^2 - b^2) = 2$, from which we find $a = 1$, $b = 1, -2$. This gives $(a, b) = (1, 1), (1, -2)$, from which we find that the only solutions of the original equation are $(x, y) = (2, 2), (5, 11)$.

Exercise 1.4*. Find all integral solutions of $y^2 + 2 = 3^n$.

Solution. First, note that n has to be strictly positive. We work in $\mathbb{Z}[\sqrt{-2}]$, which is a UFD by a previous exercise. In this ring we have $3 = (1 + \sqrt{-2})(1 - \sqrt{-2})$ and hence

$$(y + \sqrt{-2})(y - \sqrt{-2}) \;=\; (1 + \sqrt{-2})^n (1 - \sqrt{-2})^n \,.$$

Since 3^n is odd, y also has to be odd, and thus $\gcd(y + \sqrt{-2}, y - \sqrt{-2}) = 1$. Therefore

$$(1 + \sqrt{-2})^n \;=\; \pm(y \pm \sqrt{-2}) \,,$$

and hence

$$\frac{(1 + \sqrt{-2})^n - (1 - \sqrt{-2})^n}{2} \;=\; \pm\sqrt{-2} \,.$$

If we denote the left-hand side by $A_n\sqrt{-2}$, then we need to find n such that $A_n = \pm 1$.

Expanding $(1 \pm \sqrt{-2})^n$ using the binomial identity we get $A_n = \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2k+1} (-2)^k$, from which we immediately obtain $A_n \equiv n \pmod 2$. Therefore n has to be odd. Next, reducing modulo 4 we get that $A_n \equiv -1 \pmod 4$ is impossible, therefore we can only have $A_n = 1$. Reducing modulo 8 we find that $A_n \equiv 1 \pmod 8$ if and only if $n \equiv 1, 3 \pmod 8$.

Let n_1 and n_2 be two solutions to $A_n = 1$ such that $8 | (n_1 - n_2)$. We will show that then $n_1 = n_2$. Since $A_1 = A_3 = 1$, this would imply that $A_n = 1$ if and only if $n \in \{1, 3\}$.

First, by induction on l we check that for $l \geq 3$ we have

$$(1 \pm \sqrt{-2})^{2^l} \equiv 1 - (2 \pm \sqrt{-2})2^l \pmod{2^{l+2}} \,.$$

Indeed, for $l = 3$ we have $(1 \pm \sqrt{-2})^8 = 17 \pm 56\sqrt{-2} = 1 - (2 \pm \sqrt{-2})8 + 32(1 \pm 2\sqrt{-2})$. For the induction step we compute for $l \geq 3$

$$(1 \pm \sqrt{-2})^{2^{l+1}} = (1 - 2^l(2 \pm \sqrt{-2}) + 2^{l+2}s)^2 \equiv 1 - 2^{l+1}(2 \pm \sqrt{-2}) \pmod{2^{l+3}} \,.$$

Assume that $n_1 \neq n_2$, and let 2^l, $l \geq 3$, be the largest power of 2 dividing $n_1 - n_2$. Raising the above congruence to the power $(n_2 - n_1)/2^l$ we get

$$(1 \pm \sqrt{-2})^{n_2 - n_1} \equiv 1 - (2 \pm \sqrt{-2})(n_2 - n_1) \pmod{2^{l+2}} \,.$$

Since $A_{n_1} = A_{n_2} = 1$, we have $a^{n_1} - b^{n_1} = a^{n_2} - b^{n_2}$, where $a = 1 + \sqrt{-2}$ and $b = 1 - \sqrt{-2}$. From this we get

$$\begin{aligned} 0 = a^{n_2} - b^{n_2} - a^{n_1} + b^{n_1} &= a^{n_1}(a^{n_2 - n_1} - 1) - b^{n_1}(b^{n_2 - n_1} - 1) \\ &\equiv (n_1 - n_2)(a^{n_1}(2 + \sqrt{-2}) - b^{n_1}(2 - \sqrt{-2})) \pmod{2^{l+2}} \,. \end{aligned}$$

Using $(1 \pm \sqrt{-2})^n \equiv 1 \pm n\sqrt{-2} - n(n-1) \pmod{2\sqrt{-2}}$ we calculate that the last expression is congruent to $2\sqrt{-2}(n_1 - n_2)$ modulo 2^{l+2}. But then this implies that $2^{l+1} | (n_1 - n_2)$, contradicting our assumption that 2^l is the largest power of 2 dividing $n_1 - n_2$.

Thus we conclude that the only solutions are $(y, n) = (\pm 1, 1)$ and $(y, n) = (\pm 5, 3)$.