Solutions to Exercise Sheet 3
Algebraic Number Theory

January 4, 2026

Exercise 1 (Quadratic reciprocity law)**.** With this exercise we give a first (of many) proof[1] of the quadratic reciprocity law. We define the Legendre symbol.

$$\left(\frac{\cdot}{p}\right) : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}$$

by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if it exists } b \in (\mathbb{Z}/p\mathbb{Z})^\times : b^2 = a, \\ -1 & \text{otherwise.} \end{cases}$$

The quadratic reciprocity law says that for all distinct *odd prime numbers* p, q it holds that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

First we prove/recall the Euler's criterion:

1. Show the Euler's criterion, valid for every odd prime p and $a \in \mathbb{Z}$ coprime to p:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Now we are ready to prove the theorem:

2. Consider the group $G = ((\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times)/U$, where $U = \{\pm(1,1)\}$. Show that the following two subsets of $(\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$ are both a system of representatives for G:

$$S_1 = \{(i \pmod{p}, j \pmod{q}) \mid 1 \le i \le p-1, 1 \le j \le \frac{q-1}{2}\}$$
$$S_2 = \{(k \pmod{p}, k \pmod{q}) \mid 1 \le k \le \frac{pq-1}{2}, (k, pq) = 1\}.$$

3. Taking the product of all elements of G show that

$$\left((p-1)!^{\frac{q-1}{2}}\left(\frac{q}{p}\right), (q-1)!^{\frac{p-1}{2}}\left(\frac{p}{q}\right)\right)U = \left((p-1)!^{\frac{q-1}{2}}, (q-1)!^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right)U.$$

4. Conclude.

Solution. 1. Consider the map

$$\mathbb{F}_p^\times \to \mathbb{F}_p^\times;\ x \mapsto x^2.$$

This is a group homomorphism and its kernel is ± 1. Hence the image $\{x \in \mathbb{F}_p \mid \exists\, y \in \mathbb{F}_p : y^2 = x\}$ has cardinality $\frac{p-1}{2}$ (recall that the p is odd).

[1] This proof is due to G. Rosseau

Let $a \in \mathbb{F}_p^\times$, then $(a^{\frac{p-1}{2}}-1)(a^{\frac{p-1}{2}}+1) = a^{p-1}-1 \equiv 0 \pmod p$. In particular $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$ for every $a \in \mathbb{F}_p$.

If $a = b^2$ is a square, then $a^{\frac{p-1}{2}} = b^{p-1} = 1 \pmod p$. The polynomial $X^{\frac{p-1}{2}} - 1 \in \mathbb{F}_p[X]$ has at most $\frac{p-1}{2}$ solutions and since the squares are also exactly $\frac{p-1}{2}$ we see that they exhaust all possible solutions. Hence if a is not a square, then $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

2. It is clear that two distinct elements of S_1 define two distinct equivalenct classes. The cardinality of S_1 is easily computed to be $\frac{(p-1)(q-1)}{2} = |G|$, hence S_1 is a system of representatives. We have that $S_2' = \{k \pmod{pq}, 1 \le k \le \frac{pq-1}{2}, (k,pq) = 1\}$ is a system of representatives for $(\mathbb{Z}/pq\mathbb{Z})^\times/\{\pm 1\} \simeq G$ (chinese remainder theorem) and S_2 is the image of S_2' under this isomorphism, hence a system of representatives.

3. Let $\alpha = \prod_{x \in G} x$. We compute α using first the representatives S_1:

$$\alpha = \prod_{\substack{1 \le i \le p-1 \\ 1 \le j \le \frac{q-1}{2}}} (i,j) = ((p-1)!^{\frac{q-1}{2}} \pmod p, (\frac{q-1}{2})!^{p-1} \pmod q)U.$$

Notice that $((\frac{q-1}{2})!)^2 = (-1)^{\frac{q-1}{2}}(q-1)! \pmod q$ and so

$$\alpha = ((p-1)!^{\frac{q-1}{2}} \pmod p, (-1)^{\frac{p-1}{2}\frac{q-1}{2}}(q-1)!^{\frac{p-1}{2}} \pmod q)U$$

Now compute we compute α using S_2. The product

$$\begin{aligned}\prod_{k \in S_2} k \pmod p &\equiv \frac{\prod_{i=1}^{p-1} i \times \prod_{i=1}^{p-1}(p+i) \times \cdots \times \prod_{i=1}^{p-1}(\frac{q-1}{2}-1)p+i) \prod_{i=1}^{\frac{p-1}{2}}(\frac{q-1}{2}p+i)}{1 \times 2q \times \cdots \times \frac{p-1}{2}q} \\ &\equiv \frac{(p-1)!^{\frac{q-1}{2}}(\frac{p-1}{2})!}{q^{\frac{p-1}{2}}(\frac{(p-1)}{2})!} \equiv (p-1)!^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod p\end{aligned}$$

and similarly for $\pmod q$, therefore

$$\alpha = ((p-1)!^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod p, (q-1)!^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \pmod q)U.$$

4. Comparing the two expressions we deduce

$$(1, (-1)^{\frac{p-1}{2}\frac{q-1}{2}})U = (\left(\frac{q}{p}\right), \left(\frac{p}{q}\right))U$$

and so the desired reciprocity law

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Exercise 2. Let $K/\mathbb{Q}$ be a quadratic extension, i.e., $\dim_{\mathbb{Q}} K = 2$. Denote by O_K the ring of integers of K. For this exercise, you may use the following criterion without proof. Let $z \in K$, then

$$z \in O_K \iff \mathrm{char}_z(X) \in \mathbb{Z}[X]$$

where $\mathrm{char}_z(X) \in \mathbb{Q}[X]$ is the characteristic polynomial of the $\mathbb{Q}$-linear map

$$[\times z] \colon K \to K$$

defined by $[\times z](k) = zk$, $k \in K$.

1. Show that $K = \mathbb{Q}(\sqrt{D})$ for some $D \in \mathbb{Z}$ squarefree.[2]

[2]Recall we call an integer $n \in \mathbb{Z}$ squarefree if there is no prime p so that $p^2 | n$.

2. For $z = a + b\sqrt{D}$, compute $\mathrm{char}_z(X)$.

3. Show that $O_K = \mathbb{Z}[\sqrt{D}]$ if $d \equiv 2, 3 \mod 4$ and $O_K = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ if $d \equiv 1 \mod 4$.

Recall that the group of units is defined by

$$O_K^\times = \{z \in O_K \mid \exists w \in O_K : zw = 1\}$$

4. Let $K = \mathbb{Q}(\sqrt{D})$ for some $D \in \mathbb{Z}$ squarefree, $D < 0$. We call such a field an *imaginary quadratic field*. Find $O_K^\times$ in this case. In particular show that $O_K^\times$ has 2,4 or 6 elements and characterize when each situation occurs.

Solution. 1. Let $K = \mathbb{Q}(\alpha)$. Let $p(X) = X^2 + aX + b$ be the minimal polynomial of α. Completing the square we can write $p(X) = (X - \frac{a}{2})^2 + (b - \frac{a^2}{4})$. Let $q(X) = X^2 - (b - \frac{a^2}{4}) = p(X + \frac{a}{2})$. Then $\alpha - \frac{a}{2}$ is a root of $q(X)$, that is $\beta = \pm\sqrt{q} \in \mathbb{Q}$, with $q = b - \frac{a^2}{4} \in \mathbb{Q}$. We observe that $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{q})$. Write $q = \frac{r^2 D}{u}$, where $r, D, u \in \mathbb{Z}$, $(rD, u) = 1$ and D is square free. Then clearly we have $\mathbb{Q}(\sqrt{q}) = \mathbb{Q}(\sqrt{D})$.

2. Consider the ordered basis $(1, \sqrt{D})$ of $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$. Then the multiplication by $z = a + b\sqrt{D}$ in this basis is given by the matrix

$$\begin{pmatrix} a & bD \\ b & a \end{pmatrix}.$$

The characteristic polynomial is therefore $\mathrm{char}_z(X) = (X-a)^2 - b^2 D = X^2 - 2aX + (a^2 - b^2 D)$.

3. We use the statement in the assignment. Let $z = a + b\sqrt{D}$, then $z \in O_K$ if and only $2a$ and $a^2 - b^2 D \in \mathbb{Z}$. Clearly we have $\mathbb{Z}[\sqrt{D}] \subset O_K$ so we study if O_K can be bigger.

We see that $z \in O_K$ implies that $a = \frac{a'}{2}$ for some $a' \in \mathbb{Z}$. Write $b = \frac{b'}{r}$ for some $b', r \in \mathbb{Z}$, $r > 0$, coprime. Then the second condition implies that $r^2(a'^2 - 4n) = 4(b'^2 d)$ for some $n \in \mathbb{Z}$. Suppose that $(a', 2) = 1$, then since $4 \nmid (a'^2 + 4n)$ it follows that $4|r^2$ and so $2|r$. Also $r^2|4b'^2 d$ implies that $r^2|4$ (since b' is coprime to r and d is square free), hence $r = 2$ and $a + b\sqrt{D} \in \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$. Suppose $2|a'$. Then we see that $r^2|b'^2 d$ and so $r = 1$ and in this case we see $a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$. This shows $O_K \subset \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$.

We see that $\frac{1+\sqrt{D}}{2} \in O_K$ if and ony if $\frac{1}{4} - \frac{d}{4} \in \mathbb{Z}$, and this happens if and only if $D \equiv 1 \,(\mathrm{mod}\, 4)$. So we conclude the claim for $D \equiv 1 \,(\mathrm{mod}\, 4)$. If $D \equiv 2, 3 \,(\mathrm{mod}\, 4)$ we have

$$\mathbb{Z}[\sqrt{D}] \subset O_K \subsetneq \mathbb{Z}[\frac{1+\sqrt{D}}{2}],$$

however since $\mathbb{Z}[\sqrt{D}]$ has index two in $\mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ we conclude that $O_K = \mathbb{Z}[\sqrt{D}]$.

4. Recall the norm map $N(z) = N_{K/\mathbb{Q}}(z) = \det([\times z])$, $z \in K$. The norm map is multiplicative and $N(1) = 1$. In particular, we see that the units have norm 1. On the other hand, it is easy to compute that $N(a + b\sqrt{D}) = a^2 - b^2 D$ and so in this case $a + b\sqrt{D}$ implies that

$$1 = N(a + b\sqrt{D}) = a^2 + b^2|D|. \tag{1}$$

Suppose $D = -1$, then by the previous subexercise we have $O_K = \mathbb{Z}[i]$ and so in this case (1) is for $a, b \in \mathbb{Z}$ and $|D| = 1$. There are readily only four solutions which are ± 1 and $\pm i$ and each of them is a unit.

Suppose $D = -3$, then by the previous subexercise we have $O_K = \mathbb{Z}[\frac{1+i\sqrt{3}}{2}]$ and (1) becomes $1 = a^2 + 3b^2$, for $a, b \in \frac{\mathbb{Z}}{2}$, which has 6 solutions $a = \pm 1, b = 0$ or $a = \pm\frac{1}{2}$ and $b = \pm\frac{1}{2}$. Each of the solutions give a unit (easy to verify or ague directly that if $z \in O_K$ has norm 1, then it is a unit).

Suppose $D \leq -5$ and $N(z) = \frac{a}{2} + \frac{b\sqrt{D}}{2} \in \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$. Then $N(z) = 1$ implies that

$$4 = a^2 + b^2|D|.$$

We see that if $b \neq 0$, then the right hand side is bigger than 5 and so equality can not happen. Hence the unique solutions is $a = \pm 2$, that is $z = \pm 1$. It is clear that ± 1 are both units in O_K.

Exercise 3. The aim of this exercise is to classify which prime ideals are inert, split and ramified in a quadratic extension. Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic extension. We know that $O_K = \mathbb{Z}[\alpha]$, for some $\alpha \in O_K$. Let p be a prime.

1. Since O_K is a Dedekind domain we can factorise $(p) = pO_K$ into prime ideals. Show that exactly one of the following holds,
   - The ideal (p) is prime in O_K. In this case we say (p) is *inert*.
   - The ideal (p) splits into two distinct prime ideals in O_K. In this case we say (p) is *totally split*.
   - The ideal (p) is a square of a prime ideal in O_K. In this case we say (p) is *ramified*.
2. Prove that
$$O_K/pO_K \simeq \mathbb{F}_p[X]/\overline{\mu_\alpha}$$
where $\mu_\alpha \in \mathbb{Z}[X]$ is the minimal polynomial of α and $\overline{\mu_\alpha}$ is its reduction $(\mathrm{mod}\, p)$.
3. Use the above statement to first find the inert primes in terms of D.
4. Prove that p is a ramified prime iff O_K/pO_K has nilpotents. Find the ramified and split primes in terms of D.

Solution. 1. [3] First note that the inclusion $\mathbb{Z} \hookrightarrow O_K$ induces an inclusion $\mathbb{Z}/p \hookrightarrow O_K/pO_K$. Hence O_K/pO_K is naturally a non trivial $\mathbb{Z}/p$-vector space. We claim that it has dimension 2, which would imply $|O_K/pO_K| = p^2$. Since $O_K = \mathbb{Z}[\omega_D]$, for ω_D as in the previous exercise, we see that O_K/pO_K is generated, as $\mathbb{Z}$-module, by at most two elements. Hence O_K/pO_K is generated, as $\mathbb{Z}/p\mathbb{Z}$ vector space, by at most two elements and we see that $\dim_{\mathbb{Z}/p\mathbb{Z}} O_K/pO_K \leq 2$. For the other inequality, we have that $1 + pO_K$ and $\omega_D + pO_K$ (recall $\omega_D = \sqrt{D}$ if $D \equiv 2, 3 \,(\mathrm{mod}\, 4)$ or $\omega_D = \frac{1+\sqrt{D}}{2}$ if $D \equiv 1 \,(\mathrm{mod}\, 4)$) are $\mathbb{Z}/p\mathbb{Z}$-linearly independent. In fact, let $\lambda_1, \lambda_2 \in \mathbb{Z}/p\mathbb{Z}$ so that
$$\lambda_1(1 + O_K) + \lambda_2(\omega_D + O_K) = 0 + O_K$$
, that is there exists $x = a + b\omega_D \in O_K$, $a, b \in \mathbb{Z}$, so that
$$\lambda_1 + \lambda_2\omega_D = pa + pb\omega_D.$$
By uniqueness of the linear combination, we see that $\lambda_1 = pa$ and $\lambda_2 = pb$ and so $\lambda_1 \equiv \lambda_2 \equiv 0 \,(\mathrm{mod}\, p)$.

Now we go back to the question, if $(p) = pO_K$ is inert there is nothing to show. Suppose $(p) = \prod_{i=1}^n \beta_i^{l_i}$ for some pairwise distinct prime ideals β_i and $l_1 > 1$ or $n > 1$. Then we have by the Chinese remainder theorem
$$O_K/pO_K \simeq \prod_{i=1}^n O_K/\beta_i^{l_i}$$
and $\prod_{i=1}^n |O_K/\beta^{l_i}| = |O_K/pO_K| = p^2$ (otherwise pO_K would be maximal and hence prime). Suppose $n > 1$, then, since $|O_K/\beta_i^{l_i}| \neq 1$, the only possibility is that $n = 2$ and $pO_K = \beta_1\beta_2$, with $|O_K/\beta_i| = p$. Suppose $l_1 > 1$, then since $|O_K/\beta_1| \mid |O_K/\beta_1^{l_1}|$ and $|O_K/\beta_1| < |O_K\beta_1^{l_1}|$ we see that $|O_K/\beta_1| = p$ and $|O_K/\beta^{l_1}| = p^2$. Also we deduce that $l_1 = 2$, since O_K/β^2 is between O_K/β and O_K/β^{l_1}. Also, we see that $n = 1$ in this case.

2. We have
$$\mathbb{Z}[X]/(\mu_\alpha) \simeq \mathbb{Z}[\alpha] = O_K,$$
via the evaluation map. In fact if $f \in \mathbb{Z}[X]$ is so that $f(\alpha) = 0$, then $\mu_\alpha | f$ in $\mathbb{Q}[X]$. Since μ_α is monic one can see that $\mu_\alpha | f$ already in $\mathbb{Z}[X]$ (check it!). Hence we have
$$O_K/pO_K \simeq \mathbb{Z}[X](p, \mu_\alpha) \simeq \mathbb{F}_p[X]/(\overline{\mu_\alpha}),$$
where the second arrow is the reduction $(\mathrm{mod}\, p)$ of the coefficients.

[3] Thanks to Marilyne Plumey and Felix Shenyi Shang for pointing out a mistake in previous Solutions

3. If $D \equiv 2, 3 \pmod 4$, we use $\alpha = \sqrt{D}$ and we have $\mu_\alpha = X^2 - D$ and $\overline{\mu_\alpha} = X^2 - D \pmod p$. From the first subexercise, p is inert in O_K if and only if $\overline{\mu}_\alpha$ is irreducible in $\mathbb{F}_p[X]$ and the latter happens if and only if $\overline{\mu_\alpha}$ does note have roots in $\mathbb{F}_p$ and, finally, this happens if and only if D is not a square $\pmod D$, i.e. $(p, D) = 1$ and $\left(\frac{D}{p}\right) = -1$. Suppose now $D \equiv 1 \pmod 4$, in this case we use $\alpha_D = \frac{1+\sqrt{D}}{2}$. Then $\mu_\alpha(X) = X^2 - X + \frac{1-D}{4}$. In particular, we deduce as before that p is inert in O_K if and only if $X^2 - X + \frac{1+D}{4}$ does not have roots in $\mathbb{F}_p[X]$, and this happens again if and only if D is not a square in $\mathbb{F}_p$.

4. From the first subexercise we know that if p is ramified, then $O_K/pO_K \simeq O_K/\beta^2$ for some prime ideal β and so it contains a nilpotent element, namely β. On the other hand $O_K/\beta_1 \times O_K/\beta_2$ and O_K/β for prime ideals β, β_1, β_2 do not contain nilpotent elements.

   In particular, we deduce that p is ramified if and only if $\overline{\mu_\alpha}$ is a square in $\mathbb{F}_p[X]$.

   Suppose first $D \equiv 2, 3 \pmod 4$, $\overline{\mu_\alpha}(X) = X^2 - D \pmod p$ is always a square if $p = 2$. If $p > 2$, then it happens if and only if $D \equiv 0 \pmod p$. We conclude, in this case, that p is split, if $p > 2$ and $D \neq 0 \pmod p$ and D is a square $\mod p$.

   Now we consider the case $D \equiv 1 \pmod 4$. Then $\overline{\mu_\alpha}(X) = X^2 - X + \frac{1-D}{4}$ is a square if any only if $D \equiv 0 \pmod p$. We conclude, that the ramified primes $p|D$ and the split primes are $p \nmid D$ so that D is a square $\pmod p$.

Exercise 4 (A PID that is not Euclidean)**.** Let $\alpha := \frac{1+i\sqrt{19}}{2}$. The goal of this exercise is to prove that $\mathbb{Z}[\alpha]$ is a Principal Ideals Domain (PID), but not en Euclidean domain.

An integral domain A is called Euclidean if there exists a function $f\colon A \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ satisfying the following property: for all $a \in A$, $b \in A \setminus \{0\}$, there exist $q, r \in A$ so that $a = qb + r$ and $r = 0$ or $f(r) < f(b)$. If such a f exists, it is called a Euclidean function.

First, we show that $\mathbb{Z}[\alpha]$ is not Euclidean. Aiming to a contradiction, we assume that $\mathbb{Z}[\alpha]$ is Euclidean.

1. Show that $\alpha^2 - \alpha + 5 = 0$
2. Denote by $|\cdot|$ the usual absolute value in $\mathbb{C}$. Show that $|a|^2 \in \mathbb{Z}$ for every $a \in \mathbb{Z}[\alpha]$ and deduce that $\mathbb{Z}[\alpha]^\times = \{z \in \mathbb{Z}[\alpha] \mid \exists w \in \mathbb{Z}[\alpha] : zw = 1\} = \{\pm 1\}$.
3. Let f be a Euclidean function of $\mathbb{Z}[\alpha]$. Let $z_0 \in \mathbb{Z}[\alpha]$ be so that $f(z_0) = \min\{f(z) \mid z \in \mathbb{Z}[\alpha] \setminus \mathbb{Z}[\alpha]^\times\}$. Show that $\mathbb{Z}[\alpha]/(z_0)$ has at most 3 elements.
4. Show that $X^2 - X + 5$ is irreducible in both $\mathbb{F}_2[X]$ and $\mathbb{F}_3[X]$ and deduce the desired contradiction.

Next, we show that $\mathbb{Z}[\alpha]$ is a PID. Consider $\mathbb{Z}[\alpha] \subset \mathbb{C}$ and define

$$U = \{z + a \in \mathbb{C} \mid |z| < 1, a \in \mathbb{Z}[\alpha]\}$$

the union of all open disks of radius 1 with center an element of $\mathbb{Z}[\alpha]$.

5. Show that if $z \in \mathbb{C} \setminus U$, then $|\mathrm{im}(z) - \frac{n\sqrt{19}}{2}| \geq \frac{\sqrt{3}}{2}$ for all $n \in \mathbb{Z}$.
6. Show that if $z_1, z_2 \in \mathbb{C} \setminus U$, then $z_1 + z_2 \in U$.

We say that a pair $(a, b) \in \mathbb{Z}[\alpha] \times (\mathbb{Z}[\alpha] \setminus \{0\})$ has (DR) property, if there exists $q, r \in \mathbb{Z}[\alpha]$ so that $a = qb + r$ and $|r| < |b|$.

7. Prove the following statements
   - (a, b) has (DR) if and only if $\frac{a}{b} \in U$.
   - If (a, b) does not have (DR), then $(2a, b)$ has (DR).
   - If (a, b) does not have (DR), then $(\alpha a, b)$ or $((1 - \alpha)a, b)$ has (DR).
8. Show that 2 is coprime to α and $1 - \alpha$ in $\mathbb{Z}[\alpha]$, that is, there is no irreducible element that divides both 2 and α (resp. 2 and $1 - \alpha$).

9. Conclude that $\mathbb{Z}[\alpha]$ is a PID.

Solution. 1.

$$\alpha^2 - \alpha + 5 = \frac{-18 + 2i\sqrt{19}}{4} - \frac{2 + 2i\sqrt{19}}{4} + 5 = 0.$$

2. Let $x, y \in \mathbb{Z}$. We have $|x + y\frac{1+i\sqrt{19}}{2}|^2 = (x + \frac{y}{2})^2 + \frac{19y^2}{4} = x + xy + 5y^2 \in \mathbb{Z}$. If $u \in \mathbb{Z}[\alpha]^\times$, then $|u||1$ in $\mathbb{Z}$ and so it is 1. If $u \in \mathbb{Z}[\alpha]$ and $|u| = 1$, then $u\overline{u} = 1$ and $\overline{u} \in \mathbb{Z}[\alpha]$.

   The equation $(x + \frac{y}{2})^2 + \frac{19y^2}{4} = 1$, $x, y \in \mathbb{Z}$ has only two solutions $x = \pm 1$. In fact, if $y > 0$, then $\frac{19}{4}y^2 > 1$.

3. Let $z \in \mathbb{Z}[\alpha]$. Then, since $\mathbb{Z}[\alpha]$ is Eculidean, we can write $z = qz_0 + r$ for some r either 0 or $f(r) < f(z_0)$. If $r = 0$, then $z \in (z_0)$. If $r \neq 0$, then since $f(r) < f(z_0)$ implies that $r \in \mathbb{Z}[\alpha]^\times$ and so $r \in \{\pm 1\}$.

4. From the previous subexercise we deduce that $\mathbb{Z}[\alpha]/(z_0) \simeq \mathbb{F}_2$ or $\mathbb{Z}[\alpha]/(z_0) \simeq \mathbb{F}_3$. In particular the polynomial $f(X) = X^2 - X + 5$ has a solution (the image of $\alpha + (z_0)$) in $\mathbb{F}_2$ or $\mathbb{F}_3$, hence to show the desired contradiction we show that this is not the case.

   Over $\mathbb{F}_2$ we have that $f(X) = X^2 + X + 1$ which does not have roots in $\mathbb{F}_2$. Over $\mathbb{F}_3$ we have that $f(X) = X^2 - X + 2$ and it has no roots in $\mathbb{F}_3$.

5. Let $z \in \mathbb{C} \smallsetminus U$. Then for all $a \in \mathbb{Z}[\alpha]$ it holds that $|z - a| \geq 1$. Let $m =\in \mathbb{Z}$ be so that $|\mathrm{re}(z) - \frac{n}{2} - m| \leq \frac{1}{2}$. Hence

$$|\mathrm{im}(z) - \frac{n\sqrt{19}}{2}|^2 \geq |z - ((m + \frac{n}{2}) + n\frac{i\sqrt{19}}{2})|^2 - \frac{1}{4} \geq \frac{3}{4}$$

   and so the claim.

6. Suppose $z_1, z_2 \in \mathbb{C} \smallsetminus U$. After translating by elements of $\mathbb{Z}[\alpha]$ we may assume that $0 \leq \mathrm{im}(z_1), \mathrm{im}(z_2) \leq \sqrt{19}/2$. Using the previous subexercise we get $\sqrt{3}/2 \leq \mathrm{im}(z_1), \mathrm{im}(z_2) \leq (\sqrt{19} - \sqrt{3})/2$. Then we see

$$\sqrt{3} \leq \mathrm{im}(z_1) + \mathrm{im}(z_2) \leq \sqrt{19} - \sqrt{3}.$$

   We have so

$$|\mathrm{im}(z_1) + \mathrm{im}(z_2) - \sqrt{19}/2| \leq \max(|\sqrt{3} - \sqrt{19}/2|, ||\sqrt{19} - \sqrt{3} - \sqrt{19}/2|) < \frac{\sqrt{3}}{2},$$

   as you can check. Hence $z_1 + z_2 \in U$.

7. Suppose (a, b) has (DR), that is there are q, r so that $a = qb + r$, $|r| < |b|$. Then $\frac{a}{b} = q + \frac{r}{b} \in U$. On the other hand suppose $\frac{a}{b} \in U$. Then there is $q \in \mathbb{Z}[\alpha]$ so that $|\frac{a}{b} - q| < 1$. Hence $r = a - qb \in \mathbb{Z}[\alpha]$ satisfies $|r| < |b|$.

   From the previous subexercise we have $\frac{a}{b} \notin U$ implies that $\frac{a}{b} + \frac{a}{b} = \frac{2a}{b} \in U$ and so $(2a, b)$ has (DR). Similarly if $(\alpha a, b)$ and $((1 - \alpha)a, b)$ do not have (DR), then $\frac{a}{b} = \alpha\frac{a}{b} + (1 - \alpha)\frac{a}{b} \in U$ and so (a, b) has DR.

8. Suppose $\pi \in \mathbb{Z}[\alpha]$ so that $\pi|2, \alpha$. Then $\mathbb{Z} \ni |\pi|^2$ divides both 4 and $|\alpha|^2 = 5$ but this is not possible. Notice this also show that $-2 \cdot 2 + \alpha(1 - \alpha) = 1$

9. Let $\mathfrak{a} \subset \mathbb{Z}[\alpha]$ an ideal. If $\mathfrak{a} = 0$ there is nothing to show. Let $a_0 \in \mathfrak{a} \smallsetminus \{0\}$ be an element of minimal absolute value. Let $a \in \mathfrak{a}$. If (a, a_0) has (DR), then we deduce that $a_0|a$ by minimality of a_0. Suppose (a, a_0) does not have (DR). Then we may assume wlog that $(2a, a_0)$ and $(\alpha a, a_0)$ have (DR), write then $2a = q_2a_0 + r_2$ and $\alpha a = q_\alpha a_0 + r_\alpha$. Again by minimality of a_0 we deduce $r_2 = 0 = r_\alpha$. Hence $a_0|2a$ and $a_0|\alpha a$ and so $a_0|a = ((-2)2a + \alpha(1 - \alpha)a)$.

Exercise 5 (A Diophantine equation)**.** In this exercise, we determine the solution $(x, y) \in \mathbb{Z}^2$ to the equation

$$x^2 + 1 = y^3 \tag{2}$$

1. Let A be a PID and $n \geq 2$ and integer. Suppose $u, v \in A$ are coprime elements so that uv is a n'th power in A. Show that, up to multiplication by units, also u and v are n'th powers.

2. Prove that, up to multiplication by units, the only two irreducible elements dividing 2 in $\mathbb{Z}[i]$ are $1 + i$ and $1 - i$

3. Suppose $x \in \mathbb{Z}$ is odd. Show that $x^2 + 1$ can not be a cube.

   Hint: Check it $\pmod 4$

Now suppose $(x, y) \in \mathbb{Z}^2$ is a solution to (2):

4. Show that $x + i, x - i \in \mathbb{Z}[i]$ are coprime.

5. Deduce that there exists $a, b \in \mathbb{Z}$ such that $x + i = (a + ib)^3$.

6. Conclude that the only solution to (2) in $\mathbb{Z}^2$ is $(0, 1)$.

Solution. 1. Since A is a PID it is in particular a UFD. Since uv is a n'th power we can write $uv = o\pi_1^n \cdots \pi_m^n$, for $\pi_1, \ldots, \pi_m$ prime elements and o a unit. Since u and v are coprimes, then π_i divides either u or v. After relabeling $\pi_1, \ldots, \pi_m$ if necessary we may assume that there exists $0 \leq j \leq m$ so that $i > j$ if and only if $\pi_i | v$. And so by the uniqueness of the factorization we deduce $u = o'\pi_1^n \cdots \pi_j^n$ (or $u = o'$ if $j = 0$) and $v = o''\pi_{j+1}^n \cdots \pi_m^n$ (or $v = o''$ if $j = m$), with o', o'' units.

2. We have $(1 + i)(1 - i) = 2$. If $(a + bi)|2$ is a non unit then $\mathbb{Z} \ni |a + ib|^2||2|^2 = 4$. However since $(a + bi)$ is not a unit, it follows $|a + ib|^2 = a^2 + b^2 = 2$. The unique solutions are $a = \pm 1$, $b = \pm 1$.

3. For x odd we have $x^2 + 1 \equiv 2 \mod (4)$. However the only cubes $\mod 4$ are $0, \pm 1$.

4. We know that if $(x, y) \in \mathbb{Z}^2$ is a solution, then x is even. Suppose $(a + bi)|(x + i), (x - i)$, then $(a + bi)|2i$. Hence we see that $a + bi$ is, up to unit, equal to $1 + i$ or $1 - i$. But $1 + i$ does not divide $x + i$, indeed $(1 + i)(a + bi) = (a - b) + i(a + b)$ and in particular $a - b$ and $a + b$ have same parity, while x and 1 not.

5. Since $(x^2 + 1) = (x + i)(x - i) = y^3$ we deduce from the first point that there exists $(a + ib) \in \mathbb{Z}[i]$ so that $(a + ib)^3 = x + i$.

6. Suppose we have a solution (x, y), then there exists $a, b \in \mathbb{Z}$ so that $x + i = (a + ib)^3$. We expand the cube and see that

   $$x + i = (a^3 - 3ab^2) + 3iba^2 - ib^3$$

   and so $1 = b(3a^2 - b^2)$. This forces $b = \pm 1$. If $b = 1$, then we get $2 = 3a^2$ which has no integer solution. If $b = -1$, then we get $0 = -3a^2$ which has the unique solution $a = 0$. Hence $x = 0$ and $y = 1$ is the unique solution.