Exercise Sheet 4
Algebraic Number Theory

January 9, 2026

Exercise 1 (Quadratic reciprocity, again)**.** Recall that the quadratic reciprocity law says that for all distinct *odd prime* numbers p, q it holds that

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

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. In this exercise we give a second proof of this result, which historically is the sixth published proof by Gauss. Define

$$\tau = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} (\frac{a}{p}) e^{\frac{2\pi a i}{p}}.$$

1. Prove that for all $a.b \in \mathbb{Z}$ with $(ab, p) = 1$ one has
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$
2. Prove that
$$\tau^2 = (-1)^{\frac{p-1}{2}} p.$$
Hint: Recall from Exercise Sheet 3 the Euler criterion. **Remark** By Galois theory, $\mathbb{Q}[\tau] \subseteq \mathbb{Q}[e^{\frac{2\pi i}{p}}]$ is the unique quadratic extension (of $\mathbb{Q}$) in $\mathbb{Q}[e^{\frac{2\pi i}{p}}]$. That was the historical motivation for considering the quadratic Gauss sum.
3. Prove that the ideals generated by q and τ are coprime in $\mathbb{Z}[e^{\frac{2\pi i}{p}}]$.
4. Prove that
$$\tau^{q-1} \equiv \left(\frac{q}{p}\right) \mod q.$$
5. Conclude

Solution. 1. It follows from the fact that

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \,(\mathrm{mod}\, p) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \,(\mathrm{mod}\, p) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \,(\mathrm{mod}\, p),$$

and since $\left(\frac{\cdot}{p}\right)$ takes values in ± 1 the above is already an equality over $\mathbb{Z}$.

2. We compute

$$\begin{aligned}\tau^2 &= \sum_{a,b\in(\mathbb{Z}/p\mathbb{Z})^\times}\left(\frac{ab}{p}\right)e^{\frac{2\pi i(a+b)}{p}}\\ &\overset{c=ab}{=}\sum_{a,c\in(\mathbb{Z}/p\mathbb{Z})^\times}\left(\frac{c}{p}\right)e^{\frac{2\pi i(a+a^{-1}c)}{p}}\\ &\overset{c=a^2c}{=}\sum_{a,c\in(\mathbb{Z}/p\mathbb{Z})^\times}\left(\frac{c}{p}\right)e^{2\pi ia(1+c)}\\ &=\sum_{c\in(\mathbb{Z}/p\mathbb{Z})^\times}\left(\frac{c}{p}\right)\Big(\sum_{a\in\mathbb{Z}/p\mathbb{Z}}e^{2\pi ia(1+c)}-1\Big)\\ &=\sum_{c\in(\mathbb{Z}/p\mathbb{Z})^\times}\left(\frac{c}{p}\right)\sum_{a\in\mathbb{Z}/p\mathbb{Z}}e^{2\pi ia(1-c)}-\sum_{c\in(\mathbb{Z}/p\mathbb{Z})^\times}\left(\frac{c}{p}\right).\end{aligned}$$

The inner sum of the left summand is equal to p if $c=-1$ and to 0 otherwise. The second summand is 0, since the numbers of squares and non squares in $\mathbb{F}_p^\times$ are equal. Hence we get

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

3. Since q,p^2 are coprime in $\mathbb{Z}$ there $a,b\in\mathbb{Z}$ so that $1=aq+bp^2$. Then $1=aq+b'\tau^2$, with $b'=(-1)^{\frac{p-1}{2}}b$. In particular q and τ^2 are coprime in $\mathbb{Z}[e^{\frac{2\pi i}{p}}]$.

4. The binomial expansion gives $(a+b)^q=\sum_{k=0}^q\binom{q}{k}a^kb^{q-k}$. Hence by induction we get

$$\begin{aligned}\tau^q &= \left(\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)e^{\frac{2\pi ia}{p}}\right)^q\\ &=\sum_{k_1\geq k_2\geq\cdots\geq k_{p-2}\geq 0}\binom{q}{k_1}\cdots\binom{k_{p-3}}{k_{p-2}}\left(\left(\frac{1}{p}\right)e^{\frac{2\pi 1}{p}}\right)^{q-k_1}\left(\left(\frac{2}{p}\right)e^{\frac{2\pi 2}{p}}\right)^{k_1-k_2}\cdots\left(\left(\frac{p-1}{p}\right)e^{\frac{2\pi i(p-1)}{p}}\right)^{k_{p-2}}.\end{aligned}$$

Now notice that $q|\binom{q}{k_1}\cdots\binom{k_{p-2}}{k_{p-1}}$ whenever there is $0<k_i<q$, in fact if $0<k_1<q$, then $\binom{q}{k_1}=\frac{q!}{(q-k_1)!k_1!}$. Notice q divides $q!$ and it does not divide any of the terms in the denominator (by uniqueness of the factoriazion) and so again by uniqueness $q|\binom{q}{k_1}$. Suppose $k_1=\cdots=k_j=q$ and $0<k_{j+1}<q$, then we have

$$\binom{q}{k_1}\cdots\binom{k_{p-3}}{k_{p-2}}=\binom{q}{k_{j+1}}\cdots\binom{k_{p-3}}{k_{p-2}}$$

which is for the same reason as before divisible by q. Hence the only we get $(\mathrm{mod}\, q)$

$$\tau^q\equiv\sum_{1\leq a\leq p-1}\left(\frac{a}{p}\right)^q e^{\frac{2\pi iaq}{p}}\,(\mathrm{mod}\, q).$$

Notice that $\left(\frac{a}{q}\right)^q\equiv\left(\frac{a}{q}\right)(\mathrm{mod}\, q)$. By a change of varialbes $b=aq$ we see then that

$$\tau^q\equiv\left(\frac{q}{p}\right)\tau\,(\mathrm{mod}\, q)$$

and so $\tau^{q-1}\equiv\left(\frac{q}{p}\right)(\mathrm{mod}\, q)$ or $\tau\equiv 0\,(\mathrm{mod}\, q)$, but the latter cannot happen since τ and q are coprime in $\mathbb{Z}[e^{\frac{2\pi i}{p}}]$.

5. We have

$$\left(\frac{q}{p}\right)\equiv(\tau^2)^{\frac{q-1}{2}}\equiv((-1)^{\frac{p-1}{2}}p)^{\frac{q-1}{2}}\equiv(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)(\mathrm{mod}\, q).$$

Again the equality is already over $\mathbb{Z}$ since every term is ±1.

Exercise 2. Consider the Diophantine equation

$$Y^2 = X^3 - 2. \tag{1}$$

We are interested in integer solutions of this equation.

1. Show that $\mathbb{Z}[\sqrt{-2}]$ is an euclidean domain, hence a PID.
2. Use the above information to find all integer solutions of (1).

Solution. 1. Let $a, q \in \mathbb{Z}[\sqrt{-2}]$, $q \neq 0$. Let $\frac{a}{q} = x + y\sqrt{-2}$. Let $a_0, b_0 \in \mathbb{Z}$ so that $|x - a_0|, |y - b_0| \leq \frac{1}{2}$. Then $|\frac{a}{q} - (a_0 + b_0\sqrt{-2})|^2 \leq \frac{1}{4} + \frac{1}{2} < 1$. Set $r = a - q(a_0 + b_0\sqrt{-2})$ and we are done.

2. We have $y^2 = x^3 - 2$ if and only if $y^2 + 2 = x^3$.

   Suppose $(x, y) \in \mathbb{Z}^2$ is a solution, in particular $y \neq 0$. Then $x^3 = (y - \sqrt{-2})(y + \sqrt{-2}) \in \mathbb{Z}[\sqrt{-2}]$.

   We claim that $y + \sqrt{-2}$ and $y - \sqrt{-2}$ are coprime, in fact if π divides $y + \sqrt{-2}$ and $y - \sqrt{-2}$, then it divides $2\sqrt{-2}$. We compute the divisors of $2\sqrt{-2}$. Note that if $(a + b\sqrt{-2})|(2\sqrt{-2})$, then

   $$|a + b\sqrt{-2}|^2 = a^2 + 2b^2 \mid |2\sqrt{-2}|^2 = 8.$$

   Hence, the set of divisors of $2\sqrt{-2}$ is contained in (and readily is) the set

   $$\{\pm 1, \pm 2, \pm\sqrt{-2}, \pm 2\sqrt{-2}\}.$$

   The only possible non-unit divisors of $y + \sqrt{-2}$ in the above set are $\pm\sqrt{-2}$ and $\pm 2\sqrt{-2}$, and in fact it they are, then y is even. We claim that y must be odd.

   We go back to the equality $x^3 = y^2 + 2$. We claim that both x and y are odd. First, x and y have the same parity. Suppose they are both even, then $x^3 \equiv 0 \pmod 8$, which would imply that $y^2 \equiv 6 \pmod 8$, but 6 is not a square $\pmod 8$ (the only squares $\pmod 8$ are $0, 1, 4$).

   Going back to our problem, we deduce finally that $y + \sqrt{-2}$ and $y - \sqrt{-2}$ are coprime.

   As in the previous exercise sheet, we deduce that both $(y + \sqrt{-2})$ and $(y - \sqrt{-2})$ are cubes, up to unit. So suppose $(a + b\sqrt{-2})^3 = y + \sqrt{-2}$. Expanding the cube we get

   $$(a^3 - 6b^2a) + (3a^2b - 2ab^3)\sqrt{-2} = y + \sqrt{-2}.$$

   Comparing coefficients, we have

   $$ab(3a - 2b^2) = 1,$$

   which implies $a = \pm 1$. If $a = 1$, then $b = 1$ as well, if $a = -1$, then there is no solution (since in this case $3a - 2b^2 < -1$).

   The unique solutions of the equation are $(x, y) = (3, \pm 5)$ (the fact that $y = 5$ is also a solutions is hidden into the *up to unit*).