Exercise sheet #9

Exercises marked with a ✎ are to be handed in before **Monday November 25** at noon, in the mailbox at Spiegelgasse 1. Each of these is worth a number of points, as indicated.
Questions marked with a $\star$ are more difficult.

Exercise 1 – Let $q \geqslant 2$ be an integer such that both q and $4q-1$ are squarefree. We let $\mathrm{K}_q := \mathbb{Q}(\sqrt{1-4q})$, $\mathcal{O}_q$ be the ring of integers in K_q, and $\theta_q := \frac{1+\sqrt{1-4q}}{2}$. Define $\mathrm{P}_q(\mathrm{X}) := \mathrm{X}^2 + \mathrm{X} + q \in \mathbb{Z}[\mathrm{X}]$.

1.1. For this question only, we assume that $q = 41$. Compute $\mathrm{P}_q(a)$ for all $a \in \{0, \ldots, 39\}$. What do you notice? Prove that $\mathcal{O}_q$ is principal.

1.2. For any $x, y \in \mathbb{Q}$, compute $\mathrm{N}_{\mathrm{K}_q/\mathbb{Q}}(x + y\theta)$ as a polynomial in x, y. Deduce that, if $\mathrm{N}_{\mathrm{K}_q/\mathbb{Q}}(z)$ is prime for some $z \in \mathcal{O}_q$, then $\mathrm{N}_{\mathrm{K}_q/\mathbb{Q}}(z) \geqslant q$.

1.3. Let $a \in \{0, \ldots, q-2\}$ be such that $\mathrm{P}_q(a)$ is not prime. Prove that there exists a prime $p \leqslant q-1$ such that $\mathrm{P}_q(a) \equiv 0 \bmod p$.

1.4. Assume that $\mathcal{O}_q$ is principal. Prove that $\mathrm{P}_q(a)$ is prime for all $a \in \{0, \ldots, q-2\}$.

Hint: $\mathrm{P}_q(a) = \mathrm{N}_{\mathrm{K}_q/\mathbb{Q}}(a + \theta)$.

1.5. Conversely, assume that $\mathrm{P}_q(a)$ is prime for all $a \in \{0, \ldots, q-2\}$. Prove that every prime number $p < q$ is inert in K_q. Using Minkowski's bound, deduce that $\mathcal{O}_q$ is principal.

Exercise 2 (The hyperbola method) – Let $\tau : \mathbb{N} \to \mathbb{N}$ denote the arithmetic function counting the number of positive divisors. For any $x \in \mathbb{R}_{>0}$, we let $\mathrm{D}(x) = \sum_{1 \leqslant n \leqslant x} \tau(n)$. We denote by $\delta_\square : \mathbb{N} \to \{0, 1\}$ the characteristic function of squares.

2.1. Let $n \geqslant 1$ be an integer and $\mathrm{D}_n := \{d \in \mathbb{N} : d \mid n\}$ be the set of its divisors. By exhibiting a bijection $\mathrm{D}_n \to \mathrm{D}_n$, prove that $\tau(n) = \delta_\square(n) + 2 \sum_{\substack{d \mid n \\ 1 \leqslant d < \sqrt{n}}} d$.

2.2. Prove that $\mathrm{D}(x) = \sum_{\substack{k,d \geqslant 1 \\ kd \leqslant x}} 1 = \sum_{n \leqslant x} \left\lfloor \frac{x}{n} \right\rfloor$.

2.3. Deduce from the above that $\mathrm{D}(x) = -\lfloor \sqrt{x} \rfloor^2 + 2 \sum_{1 \leqslant d \leqslant \sqrt{x}} \left\lfloor \frac{x}{d} \right\rfloor$.

2.4. Deduce that there is a constant $\mathrm{C} > 0$ such that $\mathrm{D}(x) = x \log x + \mathrm{C} \cdot x + \mathrm{O}(\sqrt{x})$, as $x \to \infty$.

We now give a more geometric proof of **2.3**. For $x \geqslant 2$, consider the region

$$\mathrm{R}_x := \{(u_1, u_2) \in \mathbb{R}^2 : u_1 \geqslant 1,\ u_2 \geqslant 1 \text{ and } u_1 \cdot u_2 \leqslant x\}.$$

2.5. Make a picture, and prove that $\mathrm{D}(x) = \#(\mathrm{R}_x \cap \mathbb{Z}^2)$.

2.6. Recover the identity **2.3** by writing R_x as the union of the three subregions of $\mathbb{R}^2$ defined by $\mathrm{S}_i = \{(u_1, u_2) \in \mathrm{R}_x : u_i \leqslant \sqrt{x}\}$ for $i = 1, 2$ and $\mathrm{S}_3 = \{(u_1, u_2) \in \mathrm{R}_x : u_1 \leqslant \sqrt{x} \text{ and } u_2 \leqslant \sqrt{x}\}$.

Exercise 3 (Quadratic Gauss sums) {✎ : 8 points} – Let p be an odd prime number, and write $\zeta_p = \exp(2i\pi/p) \in \mathbb{C}$. Recall the definition of the Legendre symbol $a \mapsto \left(\frac{a}{p}\right)$ from Sheet #7.

3.1. For any integer a, show that $\displaystyle\sum_{s=0}^{p-1} \zeta_p^{as} = \begin{cases} p & \text{if } a \equiv 0 \bmod p, \\ 0 & \text{otherwise.} \end{cases}$

3.2. Prove that $\displaystyle\sum_{s=0}^{p-1} \left(\frac{s}{p}\right) = 0$.

For any $a \in \mathbb{Z}$, define the quadratic Gauss sum

$$\mathrm{G}_p(a) := \sum_{s=0}^{p-1} \left(\frac{s}{p}\right) \zeta_p^{as} \in \mathbb{C}.$$

3.3. Prove that $\mathrm{G}_p(a) = 0$ if p divides a.

3.4. For any integer $a \in \mathbb{Z}$, check that $\mathrm{G}_p(a) = \left(\frac{a}{p}\right) \cdot \mathrm{G}_p(1)$.

3.5. For any $a \in \mathbb{Z}$ which is coprime to p, prove that $|\mathrm{G}_p(a)| = \sqrt{p}$. *Hint: compute* $\mathrm{G}_p(a) \cdot \overline{\mathrm{G}_p(a)}$

3.6. By evaluating the sum $\mathrm{S} = \sum_{a=0}^{p-1} \mathrm{G}_p(a)\mathrm{G}_p(-a)$ in two different ways, prove that $\mathrm{G}_p(a)^2 = (-1)^{(p-1)/2}p$.

3.7. For any integers $n \leqslant m$, and any $a \in \mathbb{Z} \smallsetminus \{0\}$, prove that $\displaystyle\left|\sum_{s=m}^{n} \zeta_p^{as}\right| \leqslant |\sin(\pi a/p)|^{-1}$.

3.8. For any $n \leqslant m$, prove the Pòlya–Vinogradov inequality for the Legendre symbol:

$$\left|\sum_{a=m}^{n} \left(\frac{a}{p}\right)\right| < \sqrt{p}\log p.$$

Hint: Sum **3.4** *over* $a \in \{m, \dots, n\}$. *You may use the inequality:* $|\sin(x)| \geqslant 2|x|/\pi$ *for* $|x| \leqslant \pi/2$.

3.9. ($\star$) Assume that p is a large enough prime. Let I be a set of consecutive integers. If $\#\mathrm{I} \geqslant 3\sqrt{p}\log p$, deduce from the previous question that there is at least one element $a \in \mathrm{I}$ with $\left(\frac{a}{p}\right) = 1$.