Exercise Sheet 7

1. Let p be a prime number.

1. Show that for any $a \in \mathbb{Z}$, the map $\psi_a \colon x \mapsto e^{2i\pi ax/p}$ is well-defined on the finite field $\mathbb{F}_p$ and is a character of the additive group of $\mathbb{F}_p$ which depends only on the class of a modulo p.
2. Let χ be a character of the multiplicative group $\mathbb{F}_p^\times$. We extend χ to $\mathbb{F}_p$ by defining
$$\chi(0) = \begin{cases} 1 & \text{if } \chi \text{ is the trivial character,} \\ 0 & \text{otherwise.} \end{cases}$$
The *Gauss sum* associated to $a \in \mathbb{F}_p$ and to χ is defined by
$$\tau_a(\chi) = \sum_{x \in \mathbb{F}_p} \chi(x)\psi_a(x).$$
Show that if $a \neq 0$ (in $\mathbb{F}_p$) and χ is non trivial, then $|\tau_a(\chi)| = \sqrt{p}$. Compute also $\tau_0(\chi)$ and $\tau_a(1)$ for all χ and all a.
3. Show that if $a \neq 0$ and χ is non-trivial, then $\tau_a(\chi)$ is an integer in the Galois extension $\mathbb{Q}(e^{2i\pi/p})$ of $\mathbb{Q}$; moreover show that it has the property that for any element σ of the Galois group, we have $|\sigma(\tau_a(\chi))| = \sqrt{p}$.
4. Let χ_1 and χ_2 be characters of $\mathbb{F}_p^\times$, extended to $\mathbb{F}_p$ as in the previous question. The associated *Jacobi sum* is defined by
$$J(\chi_1, \chi_2) = \sum_{x \in \mathbb{F}_p} \chi_1(x)\chi_2(1-x).$$
Show that if χ_1, χ_2 and $\chi_1\chi_2$ are all non-trivial, then
$$J(\chi_1, \chi_2) = \frac{\tau_1(\chi_1)\tau_1(\chi_2)}{\tau_1(\chi_1\chi_2)}.$$
(Hint: start with the product of the left-hand side with the Gauss sum in the denominator, and find a clever change of variable.)
5. Let L be the subfield of $\mathbb{C}$ generated by the values of χ_1 and those of χ_2. Show that L is a finite Galois extension of $\mathbb{Q}$ with abelian Galois group.
6. If χ_1 and χ_2 are distinct, non-trivial, and $\chi_1\chi_2$ is non-trivial, show that the Jacobi sum $J(\chi_1, \chi_2)$ is an integer of L and that for all $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, we have $|\sigma(J(\chi_1, \chi_2))| = \sqrt{p}$.

7. Assume that $p \equiv 1 \pmod 4$. Show that there exist non-trivial characters χ_1 and χ_2 of $\mathbb{F}_p^\times$ with

$$\begin{cases} \chi_1^2 = 1, & \\ \chi_2^4 = 1, & \chi_2^2 \neq 1. \end{cases}$$

Show that $z = J(\chi_1, \chi_2)$ is an element of $\mathbb{Z}[i]$ such that $|z|^2 = p$, and deduce (again) that p is the sum of two squares of integers.

2. Let p be an odd prime number, and let N_p be the number of solutions of the equation

$$x^2 + y^2 + 1 = 0$$

in $\mathbb{F}_p$.

1. Prove that
$$N_p = \sum_{a \in \mathbb{F}_p} \Big(1 + \Big(\frac{a}{p}\Big)\Big)\Big(1 + \Big(\frac{-1-a}{p}\Big)\Big).$$
2. Deduce that
$$N_p = p + J(\lambda, \lambda),$$
where λ denotes the Legendre symbol viewed as a character of $\mathbb{F}_p^\times$.
3. For any non-trivial character χ of $\mathbb{F}_p^\times$, prove that
$$J(\chi, \chi^{-1}) = -\chi(-1).$$
4. Deduce that
$$N_p = \begin{cases} p+1 & \text{if } p \equiv 3 \bmod 4, \\ p-1 & \text{if } p \equiv 1 \bmod 4, \end{cases}$$
and in particular that $N_p \geq 1$ for all p.

3. The goal of this exercise is to prove the existence of solutions to the Pell–Fermat equation *without using Dirichlet's Unit Theorem.*

We recall Dirichlet's Approximation Theorem: *given an irrational number $\alpha \in \mathbb{R}$, there are infinitely many rational numbers a/b, with $a \in \mathbb{Z}$ and $b \geq 1$, such that $|\alpha - a/b| \leq 1/b^2$.*

Let $d \geq 1$ be an integer which is not a square of an integer, so that $\sqrt{d}$ is irrational.

1. Show that if (a, b) are integers with $b \geq 1$ such that
$$\Big|\sqrt{d} - \frac{a}{b}\Big| \leq \frac{1}{b^2},$$
then
$$|a^2 - db^2| \leq 1 + 2\sqrt{d}.$$

2. Deduce that there exists an integer $k \neq 0$ such that the equation

$$x^2 - dy^2 = k$$

has infinitely many integer solutions (x, y).

3. Deduce that the equation $x^2 - dy^2 = 1$ has infinitely many integral solutions. (Hint: show that the previous question implies that the unit group of $\mathbb{Z}_{\mathbb{Q}(\sqrt{d})}$ must be infinite.)

4. Let d be an odd non-zero squarefree integer. We denote by ξ_d the map from prime numbers coprime to d to $\{-1, 1\}$ defined for all $p \nmid d$ by

$$\xi_d(p) = \left(\frac{d}{p}\right).$$

1. Show that there exists a character χ_d of the finite group $(\mathbb{Z}/4d\mathbb{Z})^\times$ such that

$$\xi_d(p) = \chi_d(p \bmod 4d)$$

for all primes $p \nmid 4d$.

2. Show that χ_d is a non-trivial real character.

3. Let

$$S_d = \{p \mid d \text{ is a square modulo } p\}.$$

Prove that

$$\sum_{p \in S_d} \frac{1}{p^\sigma} = \frac{1}{2} \sum_p \frac{1}{p^\sigma} + O(1)$$

for all real numbers $\sigma > 1$. (Hint: express the condition that d is a square modulo p in terms of ξ_d.)

4. Let k be an arbitrary odd integer and let $n(k) \geq 1$ be the number of irreducible factors of $X^2 - k$ as a polynomial in $\mathbb{Q}[X]$. Let $\nu_k(p)$ denote the number of roots of the equation $X^2 = k$ in $\mathbb{F}_p$. Prove that

$$\sum_p \frac{\nu_k(p)}{p^\sigma} = n(k) \sum_p \frac{1}{p^\sigma} + O(1)$$

for all real numbers $\sigma > 1$.
(This is a special case of Kronecker's Theorem from Section 1.4 of the lecture notes; it can be extended without much work to all $k \geq 1$.)

5. The goal of this exercise is to prove a theorem of Lagrange: every integer $n \geq 1$ is the sum of four squares of non-negative integers. Because of the identity

$$\begin{aligned}(a^2 + b^2 + c^2 + d^2)(r^2 + s^2 + t^2 + u^2) = \\ (ar + bs + ct + du)^2 + (as - br + cu - dt)^2 + \\ (at - bu - cr + ds)^2 + (au + bt - cs - dr)^2, \quad (1)\end{aligned}$$

(which you can check!), it suffices to prove this when n is a prime number, and this may be assumed to be odd since $p = 2 = 1^2 + 1^2 + 0^2 + 0^2$.

1. Show that there exists (a, b) in $\mathbb{Z}^2$ and an integer m with $1 \leq m < p$ such that

$$mp = a^2 + b^2 + 1$$

(Hint: you can use Exercise 2, although there are other more elementary arguments.)

2. We denote by m_0 the smallest positive integer such that $m_0 p = a^2 + b^2 + c^2 + d^2$ is a sum of four squares of integers, not all of which are divisible by p. By the previous question, this exists and we have $1 \leq m_0 < p$.
3. Show that m_0 is odd. (Hint: otherwise, show that one can order a, b, c, d so that $a + b$, $a - b$, $c + d$ and $c - d$ are even, and then compute the sum of the squares of these numbers.)
4. *We assume that* $m_0 \geq 2$. Show that not all of (a, b, c, d) are divisible by m_0, and that there exist integers r, s, t, u, not all zero, such that

$$a \equiv r \bmod m_0, \quad b \equiv s \bmod m_0, \quad c \equiv t \bmod m_0, \quad d \equiv u \bmod m_0,$$
$$\max(|r|, |s|, |t|, |u|) < \frac{m_0}{2},$$
$$r^2 + s^2 + t^2 + u^2 < m_0^2,$$
$$r^2 + s^2 + t^2 + u^2 \equiv 0 \bmod m_0.$$

5. Let $m_1 \geq 1$ be such that $r^2 + s^2 + t^2 + u^2 = m_0 m_1$. Show that

$$m_1 m_0^2 p = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$$

where α, β, γ, δ are integers divisible by m_0. (Hint: use the identity (1).)

6. Obtain a contradiction and deduce that we must have had $m_0 = 1$, concluding the proof.

Vacation exercises – no due date