Exercises in Algebraic Number Theory

Winter term 2009/2010

Universität Duisburg-Essen
Institut für Experimentelle Mathematik
Prof. Dr. Gabor Wiese, Dr. Tommaso Centeleghe

Sheet 6

To be handed in by: Friday, 27 November 2009, 2 pm.

1. (4 points) Let a, b be coprime integers with $b > 1$. Show that the following statements are equivalent:
   (i) a is a quadratic residue modulo b.
   (ii) a is a quadratic residue modulo every prime divisor of b and
   - $a \equiv 1 \mod 4$ if $4|b$,
   - $a \equiv 1 \mod 8$ if $8|b$.

2. (4 points) Show that an odd prime p is of the form $p = x^2 + 2y^2$ with $x, y \in \mathbb{Z}$ if and only if $p \equiv 1, 3 \bmod 8$.

3. (4 points) Let p be a prime and $a, b \in \mathbb{F}_p$. Sketch a fast algorithm that decides whether the equation
$$X^2 + aX + b = 0$$
has a solution in $\mathbb{F}_p$.

   Note: Trying out all possibilities is not considered a fast algorithm (unless $p = 2$)! It is not necessary to construct a solution.

4. (4 points)
   (a) Let L/K be a Galois extension of number fields and let $\mathfrak{P}$ be a prime of L such that $\mathfrak{P}/\mathfrak{p}$ is unramified (i.e. $e(\mathfrak{P}/\mathfrak{p}) = 1$) with $\mathfrak{p} = \mathfrak{P} \cap K$. Let q be the norm of $\mathfrak{p}/(p)$ with $(p) = \mathfrak{p} \cap \mathbb{Z}$. Show that there exists a unique element $\phi_{\mathfrak{P}}$ in the decomposition group $G_{\mathfrak{P}}$ such that its image in the Galois group of the residue fields $\mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ is given by $x \mapsto x^q$. Show also that $\phi_{\mathfrak{P}}$ generates $G_{\mathfrak{P}}$, which is hence a cyclic group.
   (b) Let L/K be a Galois extension of number fields with Galois group G which is not a cyclic group. Show that no prime is inert in L/K.