Algebraic Number Theory 2018 — Set 6

Tutor: Vivien Vogelmann, vivienvogelmann[at]web.de
Deadline: 12.00 on Thursday, the 7th of June, 2018

Each exercise is worth 4 points. The bonus exercise is also worth 4 points. If you get more then 16 points, you can transfer the excess points to other exercise sets.

Exercise 1. Determine whether 29 is a square modulo 43.

Hints: (1) Use that the Legendre symbol $(\frac{x}{p})$ is multiplicative in x, and use that $(\frac{x}{p})$ only depends on the residue class $x \pmod p$. (2) Use quadratic reciprocity.

Exercise 2 (Neukirch, ex.I.10.1)**.** For every integer $n \geq 1$, prove that there are infinitely many prime numbers p satisfying $p \equiv 1 \pmod n$.

Hint: Suppose that there are finitely many primes p with $p \equiv 1 \pmod n$, and let P denote their product. Let ϕ_n be the n-th cyclotomic polynomial. Show that there is an integer k such that $\phi_n(knP) > 1$. Let q be a prime that divides $\phi_n(knP)$. Derive that $q \nmid nP$. Compute the order of knP modulo q, and use Fermat's little theorem to derive a contradiction.

Exercise 3. Let p be an odd prime number, and $k \geq 1$ an integer. Prove that $(\mathbb{Z}/p^k\mathbb{Z})^*$ is a cyclic group.

Hints: (1) In the first exercise sheet, you showed that this statement is true for $k = 1$. You may use this fact without proof. (2) Show that it suffices to prove that $X^n - 1$ has at most n solutions in the ring $\mathbb{Z}/p^k\mathbb{Z}$. This can be done in the same manner as for fields. (3) Show that a solution of $X^n - 1$ in $\mathbb{Z}/p\mathbb{Z}$ lifts uniquely to a solution in $\mathbb{Z}/p^k\mathbb{Z}$. (Aside: look up Hensel's lemma to see how this strategy generalises to the lifting of roots of arbitrary polynomials.)

Exercise 4 (Neukirch, ex.I.10.3)**.** Let d be a squarefree integer. Show that there is an integer $n \geq 1$ such that $\mathbb{Q}(\sqrt{d})$ can be embedded in the cyclotomic field $\mathbb{Q}(\zeta_n)$.

Exercise 5 (Bonus)**.** In Sage write a function `legendre(x,p)` that computes $(\frac{x}{p})$, without using the existing implementation `legendre_symbol`. (Use the same hints as in exercise 1.)