Algorithmic Number Theory Prof. Dr. Ulrich Thiel
WS 19/20 University of Kaiserslautern

Exercise Sheet 9

Jan 6, 2020

Exercise 1. Let $d > 1$ be square-free, let $\mathcal{O}$ be the ring of integers in $\mathbb{Q}(\sqrt{d})$, and let Δ be the discriminant of $\mathcal{O}$.

(a) Show that among all units ε of $\mathcal{O}$ with $\varepsilon > 1$ (under the obvious real embedding) there is a unique minimal one, and this unit is fundamental. We call it *the* fundamental unit of $\mathcal{O}$.
(b) Show that the fundamental unit is given by $\varepsilon = \frac{a+b\sqrt{\Delta}}{2}$, where $a, b \in \mathbb{N}_{>0}$ is the minimal solution to the equation $a^2 - b^2\Delta = \pm 4$.
(c) Generate a table of the fundamental units for $d \leq 150$.

Exercise 2 (The Battle of Hastings (October 14, 1066)).

> "The men of Harold stood well together, as their wont was, and formed thirteen squares, with a like number of men in every square thereof, and woe to the hardy Norman who ventured to enter their redoubts; for a single blow of a Saxon warhatched would break his lance and cut through his coat of mail... When Harold threw himself into the fray the Saxons were one mighty square of men, shouting the battle-cries, 'Ut!', 'Olicrosse!', 'Godemite!'."[1]

Question. How many troops does this suggest Harold II had at the battle of Hastings?

Exercise 3 (Difficult). Write a computer program that computes the unit group of an order in a number field using the proof of Dirichlet's unit theorem.[2] Use this to compute the unit group of the maximal order of the number fields defined by the following polynomials:

(a) $X^3 - 2$
(b) $X^3 - 3$
(c) $X^3 + X^2 - 1$
(d) $X^3 - X^2 + 3X - 2$
(e) $X^3 + X^2 - 2X - 1$
(f) $X^4 + X^3 - 2X - 1$

---

[1] Taken from J. Neukirch, *Algebraic Number Theory*. Fictitious historical text, following essentially problem no. 129 in: H.E. Dundeney, Amusements in Mathematics, 1917 (Dover reprints 1958 and 1970).

[2] Recall that this method is very inefficient; the purpose of the exercise is to get a better understanding of the proof and to see that it is indeed constructive.