MATEMATISKA INSTITUTIONEN	Tentamensskrivning i
STOCKHOLMS UNIVERSITET	Number Theory, 7,5 hp
Avd. Matematik	23 May 2014
Examinator: Jonas Bergström	9.00-14.00

To get grade E (or higher) one needs at least 15p (out of 30p) on the part called Proofs and 15p (out of 30p) on the part called Problems.
Higher grades are given by the following intervals: A 60-50p, B 50-45p, C 45-40p, D 40-35p, where one also needs to have at least 18p on the part called Problems for C (respectively 21p for B and 24p for A).

No calculators or computers may be used. Best of luck!

Proofs

In this part you should prove some theorems from the book and you can use all previous results in the book, but do not forget to properly: state any theorem/proposition/lemma that you use and to define the main notions.

1. Assuming that we know that $\theta(x) := \sum_{p \leq x} \log p < c_1 x$ for some constant c_1 (where the sum is over all primes p at most equal to x), show that

$$\pi(x) < c_2 \cdot \frac{x}{\log x}$$

for some constant c_2. 8 p

2. Prove that if p is prime then the group of units $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic. 8 p

3. Prove the law of quadratic reciprocity for two odd primes, either using Gauss' lemma or using Gauss sums with complex roots of unity, or using Gauss sums with roots of unity from finite fields. 14 p

Problems

4. Let us consider the ring $\mathbb{Z}/n\mathbb{Z}$ and its group of units $(\mathbb{Z}/n\mathbb{Z})^*$, where n is an integer with prime factorization $n = \prod_{i=1}^{r} p_i^{e_i}$.

   a) Express the number of elements of $(\mathbb{Z}/n\mathbb{Z})^*$ (in terms of p_i and e_i). 1 p

   b) For which n is $(\mathbb{Z}/n\mathbb{Z})^*$ cyclic? 1 p

   c) Find all a mod 203 such that the equation $x^{14} \equiv_{203} a$ has a solution. 4 p

   d) Express the maximal order of an element in $(\mathbb{Z}/n\mathbb{Z})^*$ (in terms of p_i and e_i) and prove that this expression holds. 4 p

5. a) Let A be an ideal in a ring of integers D_F of an algebraic number field F. Say that $\alpha_1, \ldots, \alpha_k$ are elements of A. What do these elements need to fullfill to be an integral basis of A? 1 p

   b) Define the class number of an algebraic number field. 1 p

   c) Define the (inertia) degree of a prime ideal P of the ring of integers D_F of an algebraic number field F. 1 p

d) Put $F = \mathbb{Q}(\alpha)$ and α is a root of the polynomial $x^3 + x + 1$. Compute the discriminant of $1, \alpha, \alpha^2$. 5 p

e) Let $F = \mathbb{Q}(\alpha)$ be defined as in c). Show that $1, \alpha, \alpha^2$ is an integral basis of D_F. 2 p

6. a) Define Dirichlet characters modulo m and give a non-trivial example. 2 p

b) Let χ be a Dedekind character modulo m. First define the Dedekind L-function $L(s, \chi) : D \to \mathbb{C}$ where $D := \{s \in \mathbb{C} : \Re(s) > 1\}$. For which $s \in \mathbb{C}$ does $L(s, \chi)$ have a meromorphic continuation, and at which points will it have a pole? 3 p

c) Put $\Lambda(s) := \pi^{-s/2}\zeta(s)\Gamma(\frac{s}{2})$. The functional equation $\Lambda(s) = \Lambda(1 - s)$ then holds as meromorphic functions if $\Re(s) > 0$. Assume it to be known that $\zeta(s) \neq 0$ if $\Re(s) > 1$ and $\Gamma(s) \neq 0$ for all s where it is defined. Use these facts to find all zeroes of $\zeta(s)$ when $\Re(s) < 0$. 5 p

The exam will be returned 14.00 on Thursday the 5th of June in room 410 in house 6. After that it can be collected in room 204 in house 6.