Department of mathematics,
Stockholm University
Examinator: Gregory Arone

Number Theory
Final Exam

Monday, August 15, 2016

Instructions: Closed book, no notes and no calculators allowed. Unless indicated otherwise, you may quote facts that appear in the textbook, or were proved in class. When you do, state precisely any result you are using. Be sure to justify your answers, and show clearly all steps of your solutions. Results of previous problems can be used even if you could not solve them

---

Part 1: Proofs

1 [10 points] Let n be an integer. Prove that $\Sigma_{d|n}\phi(d) = n$. Here ϕ is Euler's function, and the sum is over positive divisors of n.

2 [10 points] Let $\mathbb{F}$ be a finite field, and let $\mathbb{F}^*$ be the multiplicative group of non-zero elements of $\mathbb{F}$. Prove that $\mathbb{F}^*$ is a cyclic group.

3 [10 points] Suppose a, m are positive integers, with $\gcd(a, m) = 1$. Let $\mathcal{P}$ be the set of prime numbers p such that $p \equiv a \pmod{m}$. Prove that the Dirichlet density of $\mathcal{P}$ is $\frac{1}{\phi(m)}$. You may assume without proof the following fact about Dirichlet's L-functions. Let χ be a mod m Dirichlet character. Then if χ is a non-trivial character then $\frac{\ln L(s,\chi)}{s-1}$ is a bounded function for s in some interval $(1, 1+\epsilon)$. If $\chi = \chi_0$ is the trivial character then

$$\lim_{s\to 1^+} \frac{\ln L(s, \chi_0)}{-\ln(s-1)} = 1.$$

Here $\ln L(s, \chi)$ is defined using a suitable power series, as in textbook and the class. You may assume that this construction has the standard properties of the logarithm function that you need.

Part 2: Problems

4 (a) [5 points] Let p and q be distinct odd primes such that $p-1$ divides $q-1$. Let n be an integer not divisible by either p or q. Show that $n^{q-1} \equiv 1 \pmod{pq}$.

(b) [5 points] Let p be an odd prime. Show that if the number $1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$ is written as a reduced fraction, then its numerator is divisible by p.

5 (a) [5 points] Use quadratic reciprocity to find all the primes p such that 7 is a quadratic residue modulo p. Your answer should say that 7 is a quadratic residue mod p if and only if p is congruent to certain numbers (that you need to specify) modulo another number (which you also have to specify).

(b) [5 points] Suppose that p is a prime, $p \equiv 3 \pmod{4}$, and that $q = 2p+1$ is also a prime. Prove that $q|2^p - 1$. Hint: consider the question whether 2 is a quadratic residue modulo q.

6 Let F be an algebraic number field, and D its ring of integers.

(a) [2 points] Define the class number of F

(b) [3 points] Suppose that the class number of F is 2, and $\pi \in D$ is an irreducible element, such that (π) is not a prime ideal. Prove that there exists two prime ideals P_1, P_2 (not necessarily distinct), such that $(\pi) = P_1 \cdot P_2$.

(c) [2 points] Consider the number field $\mathbb{Q}(\sqrt{2}+\sqrt{5})$. Show that $\sqrt{2}$ is an element of this field.

(d) [3 points] Find the trace and the norm of $\sqrt{2}+\sqrt{5}$ in $\mathbb{Q}(\sqrt{2}+\sqrt{5})$. (Note: you may assume without proof that if p, q are distinct primes then $1, \sqrt{p}, \sqrt{q}, \sqrt{pq}$ are algebraically independent.)