Mathematics 115

Final Exam, May 18, 1994 — Professor K. A. Ribet

---

1. Let A be a finite abelian group. If $\varphi\colon A \to \mathbf{C}^*$ is a non-trivial homomorphism, show that $\sum_{a\in A} \varphi(a) = 0$.

2. Calculate the number of solutions to the congruence $x^3 \equiv 8 \bmod 5040$. (Note that $5040 = 7!$.)

3. A pseudoprime is a composite integer p for which $2^p \equiv 2 \bmod p$. Show that $11 \cdot 31$ is a pseudoprime. Prove that every Fermat number $2^{2^n}+1$ is either a prime or a pseudoprime. [The first known even pseudoprime—161038—was found by Berkeley's D. H. Lehmer in 1950.]

4. Suppose that p is an odd prime and that a is an integer prime to p. Gauss's lemma may be summarized as the identity $\left(\dfrac{a}{p}\right) = (-1)^\mu$. Explain the definition of the quantity μ that appears in this formula. Use Gauss's lemma to compute $\left(\dfrac{2}{p}\right)$ when $p \equiv 1 \bmod 8$.

5. Recall that $\zeta(s) = \sum_{n=1}^{\infty} \dfrac{1}{n^s}$ for $s > 1$. Prove that $\zeta(s) - 1 < \int_1^\infty t^{-s}\,dt < \zeta(s)$ by using techniques from first-year calculus. Use these inequalities to prove that the limit $\lim_{s\to 1^+} (s-1)\zeta(s)$ exists and equals 1. (In this problem, s is always a real number.)

6. Let $D = \mathbf{Z}[\omega]$, where ω is a complex third root of 1.

- **a.** Show that the unit group of D has order 6.
- **b.** If u is a unit of D which is congruent to 1 mod (3), prove that $u = 1$.

7. Let $\zeta = e^{2\pi i/p}$, where $p \geq 3$ is prime. Show that $\displaystyle\sum_{a \bmod p} \left(\frac{a}{p}\right)\zeta^a = \sum_{a \bmod p} \zeta^{a^2}$.

8. Let p be an odd prime, and let J be the Jacobi sum $\sum_{a\in\mathbf{F}_p} \psi(a)\varphi(1-a)$, where ψ and φ are non-trivial characters $\mathbf{F}_p^* \to \mathbf{C}^*$.

- **a.** What value did we find for J in case $\psi\varphi$ is the trivial character?
- **b.** What expression did we obtain for J if $\psi\varphi$ is *not* the trivial character?
- **c.** Show that every prime congruent to 1 modulo 4 is the sum of two integral squares.

This is a closed book exam. Time limit: three hours.