MT 430 Intro to Number Theory

MIDTERM 2 PRACTICE

1. Material covered

Midterm 2 is comprehensive but will focus on the material of all the lectures from February 19 up to April 4. Please review the following topics covered before Midterm 1:

1. Euler’s \(\phi\)-function.
3. Euler’s criterion.

New topics for Midterm 2 are:

1. Primitive roots of prime numbers.
2. Solving algebraic congruences \(x^d \equiv b \, (\text{mod } p)\).
3. Legendre’s symbol.
4. Gauss’ lemma.
5. Quadratic reciprocity laws.
6. Continued fractions.
7. Representation of rational numbers by simple continued fraction using Euclidean algorithm.
8. Infinite continued fractions.
9. Representation of quadratic irrationals by periodic infinite continued fractions.
10. Solving Pell’s equation using continued fractions (tentative).

To prepare for the midterm, review your lecture notes and redo Problems Sets 4, 5, 6 (also read and work through the posted solutions).

Here are a few extra practice problems:

2. Practice problems

Problem 1. What are all possible orders of elements in \(F_{19}^*\)?

Problem 2. Find all primitive roots of 19.

Problem 3. Find all solutions of \(x^{12} \equiv 7 \, (\text{mod } 19)\) and \(x^{12} \equiv 6 \, (\text{mod } 19)\).

Problem 4. Is 8 a square modulo 31? Does equation \(x^2 + 6x + 1 \equiv 0 \, (\text{mod } 31)\) have a solution?

Problem 5. Compute Legendre’s symbols \(\left(\frac{15}{17}\right)\) and \(\left(\frac{15}{31}\right)\).

Problem 6. For which primes \(p\) is 6 a square modulo \(p\)?

Problem 7. Calculate the continued fraction expansion of \(\frac{676}{107}\).

Problem 8. Find the infinite continued fraction representation of \(\sqrt{20}\).

Problem 9. Find the irrational number having continued fraction expansion \((4, 4, 8)\).
Problem 10. Suppose that $\frac{h_n}{k_n}$ and $\frac{h_{n+1}}{k_{n+1}}$ are two successive convergents of a number $x$. Show that for any reduced rational number $\frac{a}{b}$ in the open interval $(h_n/k_n, h_{n+1}/k_{n+1})$ one necessarily has $b \geq k_n + k_{n+1}$.

Conclude that $h_n/k_n$ is the best possible approximation of $x$ among all rational numbers $a/b$ satisfying $b \leq k_n$. 