MATH 332 - ALGEBRA AND NUMBER THEORY
FINAL EXAM - PRACTICE

Note: The final exam will be similar to the first and second prelim in format, except that the final exam will be longer (2 hours). Also, the final exam will cover all the material we have covered, with an emphasis on newer material. In order to review, it would be a good idea to go over the first and second prelim and their respective practice tests.

Theory Question 1. *Prove that if p is prime and $p|ab$ then either $p|a$ or $p|b$. Explain why the previous statement can be re-written as follows: if p is a prime and $ab \equiv 0 \mod p$ then $a \equiv 0 \mod p$ or $b \equiv 0 \mod p$ (or equivalently, if $ab \equiv 0$ in $\mathbb{Z}/p\mathbb{Z}$ then either $a \equiv 0$ or $b \equiv 0$ in $\mathbb{Z}/p\mathbb{Z}$).*

Theory Question 2. *Prove the Fundamental Theorem of Arithmetic, i.e. every natural number $n > 1$ is a product of primes, and the representation is unique, except for the order of factors.*

Theory Question 3. *Prove Euclid's theorem on the infinitude of primes, i.e. prove that there exist infinitely many prime numbers.*

Theory Question 4. *Write precise statements for the following theorems (you do not need to prove them):*

(1) *Wilson's Theorem.*
(2) *Fermat's Little Theorem.*

Theory Question 5. *Write a precise statement for Fermat's Little Theorem and prove it.*

Theory Question 6. *Write a precise statement for Euler's theorem and prove it.*

Theory Question 7. *Prove that every prime number has a primitive root (you may use Lagrange's theorem on the number of roots of polynomials over fields, but you certainly need to state it precisely and correctly).*

Theory Question 8. *Write precise statements for the following theorems/conjectures (you do not need to prove them):*

(1) *Law of Quadratic Reciprocity.*
(2) *Prime Number Theorem.*
(3) *Dirichlet's theorem on primes in arithmetic progressions.*
(4) *Goldbach's Conjecture.*
(5) *Twin Prime Conjecture.*
(6) *Fermat's Last Theorem.*

Theory Question 9. *Write a precise definition of the following:*

(1) *Quadratic residue modulo m.*
(2) *Legendre symbol.*
(3) *Mersenne prime.*
(4) *Perfect number.*

Problem 1. *Find the quadratic irrational numbers which correspond to the continued fractions:*

$$\langle 1, 2, \overline{3} \rangle, \quad \langle 1, \overline{2, 3} \rangle, \quad \langle \overline{1, 2, 3} \rangle.$$

Problem 2. *Find the continued fraction and the first* 5 *convergents of the numbers:*

$$\sqrt{3}, \quad \frac{1+\sqrt{5}}{2}, \quad \sqrt{23}, \quad \sqrt{101}$$

without using a calculator.

Problem 3. *Let* q_k *be defined as always (i.e.* $q_{-1} = 0$*,* $q_0 = 1$*,* $q_{k+1} = a_{k+1}q_k + q_{k-1}$*). Prove by induction that* $q_k \geq 2^{k/2}$ *if* $k \geq 2$*.*

Problem 4. *Find the first few terms and the first few convergents of* π *and* e*. Find the first few convergents of* π *and* e *(the more the merrier). Here you can use a calculator (but not during the test).*

Problem 5. *The infinite simple continued fraction of the number* e *is*

$$e = \langle 2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, 1, 1, 14, \dots \rangle$$

(1) *Justify:* e *is an irrational number.*
(2) *Justify:* e *is not a quadratic irrational number.*
(3) *Find the first eight convergents of the continued fraction of* e*.*
(4) *Find the best rational approximation to* e *having a denominator less than or equal to* 536*.*

Problem 6. *Let* d *be a positive integer.*

(1) *Show that the continued fraction of* $\sqrt{d^2+1}$ *is* $\langle d, \overline{2d} \rangle$*.*
(2) *Find the continued fractions of* $\sqrt{101}$*,* $\sqrt{290}$*,* $\sqrt{2210}$*.*

Problem 7. *Describe all the solutions of:*

$$x^2 + 3y^2 = 1, \quad x^2 - 3y^2 = 1, \quad x^2 - 23y^2 = 1.$$

Problem 8. *Find the fundamental solution of the following equations, by using continued fractions:*

$$x^2 - 23y^2 = 1, \quad x^2 - 101y^2 = 1, \quad x^2 - 29y^2 = 1.$$

Problem 9. *Use congruences to show that* $x^2 - 2006y^2 = -1$ *has no solutions in positive integers. Is the length of the period of* $\sqrt{2006}$ *even or odd?*