

Name: _____

Math 4150 – Introduction to Number Theory

Spring 2008

PRACTICE QUESTIONS FOR FINAL EXAM

Topics to be covered on the final exam: GCD's and the Euclidean algorithm, linear diophantine equations, Pythagorean triples, the Fundamental Theorem of Arithmetic, modular arithmetic, divisibility tests, successive squaring, Fermat's Little theorem and Euler's theorem, pseudoprimes and strong pseudoprimes (Miller-Rabin test), Chinese Remainder Theorem, Mersenne primes and perfect numbers, Carmichael numbers and Korselt's criterion, order and primitive roots, Lucas' theorem, indices, RSA (cryptosystem and digital signature scheme), Diffie-Hellman key exchange protocol, El Gamal cryptosystem, quadratic residues and Euler's criterion, Quadratic Reciprocity (statement and applications), Pepin's test, computing modular square roots ($p \equiv 3 \pmod{4}$ only), index calculus (basic idea only), flipping a coin over the telephone, sums of two squares, basic properties of Gaussian integers.

In addition to reviewing your class notes, the course text, and the study guides for Midterms 1 and 2, you should also work through the following problems, which cover material discussed towards the end of the course.

1. If p, q are distinct odd primes, how many solutions are there to the congruence $x^2 \equiv 1 \pmod{pq}$? Explain your answer.
2. Find all solutions to the congruence $x^2 \equiv 134 \pmod{143}$. [Note that $143 = 11 \cdot 13$.]
3. Given that 5 is a primitive root modulo 73 and that $5^{10} \equiv 50 \pmod{73}$ and $5^{12} \equiv 9 \pmod{73}$, find $\text{ind}_5(2)$ and $\text{ind}_5(3)$.
4. The smallest primitive root for the prime 103 is 5. Given that $5^{11} \equiv 2^4 \cdot 3 \pmod{103}$ and $5^{16} \equiv 2^5 \pmod{103}$, solve the equation $5^x \equiv 27 \pmod{103}$. [**Hint:** $5 \cdot 41 \equiv 1 \pmod{102}$.]

5. Suppose $n \geq 2$ is an integer and there are integers x, y such that $x^2 \equiv y^2 \pmod{n}$ but $x \not\equiv \pm y \pmod{n}$. Prove that n is composite, and explain how to efficiently compute a proper factor of n .
6. Find all solutions to the equation $x^2 \equiv -1 \pmod{101}$. (**Hint:** 2 is a quadratic nonresidue modulo 101.)
7. If $p \equiv 3 \pmod{4}$ is prime and a is a quadratic residue modulo p , explain how to efficiently find the solutions to the equation $x^2 \equiv a \pmod{p}$.
8. Explain the protocol for flipping a coin over the telephone using quadratic congruences.
9. State how to determine from the prime factorization of the positive integer n whether or not n can be written as a sum of two integer squares.
10. Prove that if $m = a^2 + b^2$ and $n = c^2 + d^2$ with $a, b, c, d \in \mathbf{Z}$, then $mn = e^2 + f^2$ for some $e, f \in \mathbf{Z}$.
11. If a prime number $p > 5$ can be written in the form $p = a^2 + 5b^2$ with $a, b \in \mathbf{Z}$, prove that $p \equiv 1$ or $9 \pmod{20}$.
12. If $a + bi$ divides $c + di$ as Gaussian integers, prove that $a^2 + b^2$ divides $c^2 + d^2$ (as usual integers).
13. Write the Gaussian integer $15 + 15i$ as the product of a Gaussian unit and normalized Gaussian primes.