Final Examination (SAMPLE ONLY)

This sample exam is intended to resemble the Final Examination (8:00–10:00 am, Wednesday, May 14 in our usual classroom, RH 247) in approximate length, difficulty, and style, although clearly the content may differ. The actual content may include any material covered this semester, either in class or assigned readings.

Instructions: Attempt all questions. Closed book; however, a 'cheat sheet' (one $8.5'' \times 11''$ sheet with your own handwriting) and a calculator are permitted. *Answer clearly and precisely.*

1. In each of the following cases, describe an algorithm appropriate for the specified computational task. Also indicate whether or not the algorithm is feasible for large integer inputs (say, hundreds of digits long).
   (a) determination of $\gcd(a,b)$ for two given integers a,b;
   (b) given a and m which are relatively prime, determination of the inverse of a mod m;
   (c) solution of a congruence $ax \equiv b \mod m$ where a,m are relatively prime integers.

2. Find the exact value of
$$\gamma = [\,\overline{2,1}\,] = 2 + \cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cdots}}}}}$$
   and express your answer in simplified form.

3. Compute each of the following.
   (a) $\phi(3000)$; (b) $\sigma(3000)$; (c) 2^{98} mod 97; (d) the Legendre symbol $\left(\frac{82}{97}\right)$;
   (e) the *number* of intger solutions of $x^2 + 4x + 73 \equiv 0 \mod 127$, with $0 \leqslant x < 127$.

4. (a) Determine which primes $p < 30$ are expressible in the form $a^2 + 3b^2$ for some integers a,b.
   (b) State a reasonable conjecture, based on (a), of the form: *A prime p is expressible in the form $a^2 + 3b^2$ if and only if p is congruent to ____ mod ____.*
   (c) Prove the 'only if' part of (b).

5. Clearly define each of the following. Also give an example of each.
   (a) a Mersenne prime
   (b) a perfect number
   (c) a primitive Pythagorean triple

6. Find an integer solution of Pell's equation $x^2 - 11y^2 = 1$ with $y > 100$.

7. Show that the equation $x^2 - 21y^2 = 4$ has infinitely many integer solutions. Also show that the equation $x^2 - 21y^2 = -1$ has no integer solutions.

8. Determine the continued fraction expansion of each of the real numbers
   (a) 3.14; (b) $1 + \sqrt{3}$.

9. Consider a prime $p \equiv 3 \mod 4$. How many solutions are there for the congruence $x^4 \equiv 4 \mod p$, $x \in \{0, 1, 2, \ldots, p-1\}$?

10. Answer TRUE or FALSE to each of the following statements.
   (a) The expression $\frac{\pi(n)}{\ln(n)}$ approaches 1 as $n \to \infty$. _____*(True/False)*
   (b) Fermat proved that there are infinitely many primes of the form $n^2 + 1$. _____*(True/False)*
   (c) There is an efficient algorithm for solving quadratic congruences of the form $x^2 \equiv a \mod m$ over the integers mod m, where a and m (and the coefficients of the equation) may be hundreds of digits long. _____*(True/False)*
   (d) The unit circle $x^2 + y^2 = 1$ contains infinitely many points with rational coordinates (x, y). _____*(True/False)*
   (e) If $13n$ is a sum of two integer squares, then so is n. _____*(True/False)*
   (f) The Riemann Hypothesis is the conjecture that every complex number of the form $s = \frac{1}{2} + it$ (where $t \in \mathbb{R}$) is a solution of $\zeta(s) = 0$. _____*(True/False)*
   (g) For every positive integer n, the interval $[n, n + 10^{10}]$ contains at least one prime. _____*(True/False)*
   (h) If $a \equiv b \mod 7$, then we must have $3^a \equiv 3^b \mod 7$. _____*(True/False)*
   (i) RSA, the Repeated Squaring Algorithm, is the basis for modern factoring methods. _____*(True/False)*
   (j) There are infinitely many primes of the form $3N-1$. _____*(True/False)*