Philadelphia University

Department of Basic Sciences

Final Exam **Computational Number Theory** **5–2–2007**

Each problem is worth 5 points.

1. Apply Fermat Factorization technique to factor the number $n = 7313$.
2. Find the number represented by the periodic infinite continued fraction $[2, \overline{4}]$. Write your answer in the form $\frac{P+\sqrt{d}}{Q}$ with P, Q, d integers.
3. Evaluate $\sigma(n)$ given the prime factorization $n = 2^4 \cdot 13^2 \cdot 37$. Is n a perfect number?
4. Given the congruence $1123^2 \equiv 453^2 \pmod{13199}$, use Euclidean Algorithm to factor the number $n = 13199$.
5. Suppose $n = 4187$ is used in an RSA cryptosystem and that you discover $\phi(n) = 4056$. Use this information to find the factors of n.
6. Illustrate Lucas-Lehmer primality test using the Mersenne number M_7. What conclusion do you get?
7. Apply Pollard rho method to factor the number $n = 1807$, using initial term $x_0 = 3$.
8. Illustrate Miller-Rabin primality test using $n = 781$ and base number $a = 5$. What conclusion do you get?
9. Use the appropriate algorithm in order to express the quadratic irrational number
$$\alpha = \frac{5 - \sqrt{6}}{2}$$
as a periodic infinite continued fraction.
10. Prove that every Fermat number is either a Fermat prime or a Fermat pseudo-prime to the base 2.

–Amin Witno