# Philadelphia University

## Department of Basic Sciences

**Final Exam** **Computational Number Theory** **07–06–2009**

1. For the RSA encryption, Alia has selected the product $n = 5429 = 61 \times 89$ with the encryption key $e = 19$. What is her secret decryption key $d$?

2. Illustrate Fermat factorization with $n = 314869$.

3. Given the congruence $987^2 \equiv 654^2 \pmod{20239}$. Factor the number 20239 using the GCD algorithm.

4. Represent the number $\alpha = \sqrt{222}$ using a periodic infinite continued fraction, using the algorithm given by the following recursion.

$$\begin{array}{llll} P_0 = 0 & Q_0 = 1 & \alpha_0 = \sqrt{n} & a_0 = \lfloor \sqrt{n} \rfloor \\ P_k = a_{k-1}Q_{k-1} - P_{k-1} & Q_k = \dfrac{n - P_k^2}{Q_{k-1}} & \alpha_k = \dfrac{P_k + \sqrt{n}}{Q_k} & a_k = \lfloor \alpha_k \rfloor \end{array}$$

5. Let $M_p = 2^p - 1$, where $p$ is prime. Suppose that $M_p$ is composite. Prove that $M_p$ is a Fermat pseudoprime to the base $a = 2$.

6. Let $n = 2552$.
   (a) Factor $n$ into primes.
   (b) Find all the divisors of $n$.
   (c) Evaluate $\sigma(n)$.
   (d) Is $n$ a perfect number? Why or why not?

–Amin Witno