Philadelphia University

Department of Basic Sciences

Final Exam **Computational Number Theory** **15–06–2008**

1. Illustrate Fermat factorization with $n = 4747$.
2. Illustrate the Polard rho method with $n = 407$. Use $x_0 = 3$.
3. Illustrate quadratic sieve with $n = 1457$. Use the following table.

	39^2	54^2	69^2	78^2
2				
3				
5				
7				
11				
13				

4. Prove that every Mersenne number $M_p = 2^p - 1$ is either a prime or a Fermat pseudoprime to the base 2.
5. Illustrate Miller-Rabin test with $n = 273$, using the base $a = 2$. What is your conclusion? Choose one answer from the following.
   (a) prime
   (b) composite
   (c) strong pseudoprime
   (d) either prime or strong pseudoprime
6. Evaluate $\sigma(100)$. Is 100 a perfect number? Why or why not?
7. Is 1234 a triangular number? Why or why not?

–Amin Witno