Philadelphia University

Department of Basic Sciences

Final Exam **Computational Number Theory** **26–01–2010**

1. In an RSA example, Alia chooses $n = pq = 7169$. Given that $\phi(n) = 6996$, find p and q.

2. Illustrate Fermat factorization with $n = 7169$.

3. The following table is used to illustrate the quadratic sieve factorization method with $n = 3959$. Complete the algorithm.

	63^2	89^2	90^2	91^2
2	1	–	1	–
3	–	1	–	1
5	1	–	–	–
7	–	–	1	–
11	–	–	–	2
13	–	–	1	–

4. Evaluate the periodic infinite continued fraction $[\,2, \overline{6, 1}\,]$. Write your answer in the form $\frac{P+\sqrt{n}}{Q}$ where P, Q, and n are all integers.

5. Illustrate Lucas test (extended Fermat test) to show that $n = 149$ is a prime number, using the base $a = 2$.

6. Consider the Fermat numbers $F_n = 2^{2^n} + 1$. Prove the recurrence relation

$$F_n = F_0 F_1 F_2 \cdots F_{n-1} + 2$$

for all $n \geq 1$.

7. The number 8191 is prime. Let $n = 2^{12} \times 8191$. Is n a perfect number? Why or why not?

–Amin Witno