Philadelphia University

Department of Basic Sciences

Final Exam **Computational Number Theory** **24–01–2011**

1. In the RSA algorithm, we use $n = 893 = 19 \times 47$ and $e = 325$. Find the value of the decryption key d.

2. Let $n = 10t + u$, where u is the unit digit of n. Prove that $19 \mid n$ if and only if $19 \mid t + 2u$.

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

4. Illustrate QSA with $n = 91027$. The table has been provided below.

	1091^2	523^2	675^2	854^2	1001^2
2	1	6	1	2	6
3	2	–	–	–	–
5	1	–	1	2	–
7	1	1	2	–	–
11	1	–	–	1	1
13	–	–	–	–	–

5. (a) Given that $3^{112} \equiv 1 \pmod{113}$, illustrate Lucas' test to see if 113 is a prime number. (b) What is your conclusion?

6. (a) Prove that the number $2^{48} + 1$ is composite and find one of its factors. (b) Find two non-trivial factors of the number $2^{55} - 1$.

7. Let $F_n = 2^{2^n} + 1$. Use induction to prove that $F_n = F_0 \times F_1 \times F_2 \times \cdots \times F_{n-1} + 2$ for all integers $n \geq 1$.

8. Let $p > 2$ be a prime number and $M_p = 2^p - 1$. Prove that M_p is either a Mersenne prime or a Fermat pseudoprime base $a = 2$.

–Amin Witno