Philadelphia University

Department of Basic Sciences

Exam 2 **Computational Number Theory** **23–12–2007**

1. (a) Illustrate Pollard rho method with $n = 143$. Use $x_0 = 3$.
   (b) Factor $n = 7801$ using Fermat factorization method. It is known that $n = a \times b$ where a is about 9 times larger than b.

2. The following table is taken from a Qudratic Sieve method with $n = 799$.

	29^2	31^2	40^2	58^2	75^2
2	1	1	1	3	5
3	1	4	–	1	–
5	–	–	–	–	–
7	1	–	–	1	–

   (a) Find three congruences in the form $x^2 \equiv y^2 \pmod{799}$. For each one, find out if it is trivial or non-trivial.
   (b) Factor n using gcd.

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

4. (a) Apply Miller-Rabin test for $n = 1729$ and $a = 2$. What is your conclusion?
   (b) Is $n = 1729$ a Carmichael number? Why or why not?

5. Given an odd integer $n > 1$. Suppose that a and b are inverses modulo n. Prove that n is a Fermat pseudoprime base a if and only if n is a Fermat pseudoprime base b.

–Amin Witno