Philadelphia University

Department of Basic Sciences

Exam 2 **Computational Number Theory** **29–12–2011**

1. Factor $n = 407$ using Polard rho method with $x_0 = 3$. Complete the table.

k	x_k	$\gcd(x_{2k} - x_k, n)$
1	10	$--$
2	101	$\gcd(101 - 10, 407) = 1$
3		
4		

2. Factor $n = 143$ using Polard $p - 1$ method with $x_1 = 2$. Complete the table.

k	x_k	$\gcd(x_k - 1, n)$
1	2	$\gcd(1, 143) = 1$
2	4	$\gcd(3, 143) = 1$
3		
4		

3. Factor $n = 897$ using Quadratic Sieve using $x = 43, 60, 90, 109$ and $p \in \{2, 3, 5, 7, 11\}$.

4. Let $n = 7 \times 13 \times 19 \times 37$. Is n a Carmichael number? Why or why not?

–Amin Witno