

PHILADELPHIA UNIVERSITY  
DEPARTMENT OF BASIC SCIENCES

Final Exam

Computational Number Theory

06-06-2010

1. Evaluate the infinite periodic continued fraction  $[5, \overline{2, 3}]$ . Write your answer in the form  $\frac{P+\sqrt{n}}{Q}$  using  $P, Q, n$  integers.
2. Illustrate Miller-Rabin test with  $n = 1105$  and  $a = 2$ . What is the conclusion?
3. Illustrate quadratic sieve with  $n = 1457$ . The table has been provided below.

	$41^2$	$54^2$	$57^2$	$69^2$	$101^2$
2	5	1	1	1	1
3	-	-	1	1	-
5	-	-	1	1	-
7	1	-	-	-	-
11	-	-	1	-	-
13	-	-	-	1	-

4. Find a prime  $p < 20$  such that the number  $7 \times 31 \times p$  is Carmichael.
5. Prove that the Fermat number  $F_n = 2^{2^n} + 1$  is a prime or Fermat pseudoprime base 2, for all  $n \geq 0$ .
6. Prove that the number 107 is prime using Lucas's test,  $a = 2$ .

-Amin Witno