THE UNIVERSITY OF SYDNEY
SCHOOL OF MATHEMATICS AND STATISTICS

Tutorial 7 (Week 8)

MATH2068/2988: Number Theory and Cryptography — Semester 2, 2017

Web Page: http://www.maths.usyd.edu.au/u/UG/IM/MATH2068/
Lecturer: Dzmitry Badziahin

More difficult questions are marked with either * or **. Those marked * are at the level which MATH2068 students will have to solve in order to be sure of getting a Credit, or to have a chance of a Distinction or High Distinction. Those marked ** are mainly intended for MATH2988 students.

Tutorial Exercises:

1. Let $a \geq 2$ be an integer. A composite number $n > 1$ is said to be a *pseudoprime for the base* a if $a^{n-1} \equiv 1 \pmod{n}$. Find the prime factorization of 341, and hence show that 341 is a pseudoprime for the base 2 but not for the base 3.

2. A composite number $n > 1$ is called a *Carmichael number* if it is a pseudoprime for any base a such that $\gcd(a, n) = 1$.

(a) Show that any Carmichael number must be odd. (Hint: consider $a = n - 1$.)

(b) Find the prime factorization of 561 and show that, for each of its prime factors p, we have $p - 1 \mid 560$.

(c) Hence show that 561 is a Carmichael number.

(d) Similarly, show that 6601 is a Carmichael number.

3. Let n be an odd integer greater than 1. To try to decide whether n is prime, we could test whether $a^{n-1} \equiv 1 \pmod{n}$ for various $a \in \{2, 3, \cdots, n-1\}$. A prime number will always pass this test, by Fermat's Little Theorem; but as seen in the previous questions, there are some composite numbers which will pass this test for many values of a. This question suggests a slight improvement to the test.

(a) Show that if n is prime and $a \in \{2, \cdots, n-1\}$, then $a^{(n-1)/2} \equiv \pm 1 \pmod{n}$.

(b) Show that when $n = 561$ and $a = 5$, we have $a^{(n-1)/2} \not\equiv \pm 1 \pmod{n}$, despite the fact that, as seen in the previous question, $a^{n-1} \equiv 1 \pmod{n}$.

4. Show that the function $f(k) = k^4 + k^3 + 2068k + 2988$ is $O(k^4)$.

***5.** Which of the following functions of a positive integer variable k are $O(k^a)$ for some positive integer a?

$$\log_2(k), \quad k\log_2(k), \quad k!, \quad \log_2(k!), \quad k^{\log_2(k)}, \quad \frac{(1.01)^k}{k^2}.$$

For the last function you can use the result from analysis: for any $c > 1$ and $b > 0$,

$$\lim_{k\to\infty} \frac{c^k}{k^b} = \infty.$$

**6. Recall the Fibonacci numbers F_n from Tutorial 3. Describe a polynomial-time algorithm which determines, for given positive integers n and m, the residue of F_n modulo m. To say that the algorithm is polynomial-time means that there is some positive integer a such that the maximum number of bit operations it requires when n and m have k bits is $O(k^a)$.

Extra Exercises:

7. It was shown in lectures that if $\frac{f(n)}{g(n)} \to L$ as $n \to \infty$ for some (finite) real number L, then $f(n)$ is $O(g(n))$. As an example to show that the converse doesn't hold, prove that $\phi(n)$ is $O(n)$, but $\frac{\phi(n)}{n}$ does not tend to any limit as $n \to \infty$.

8. Show that $2047 = 2^{11} - 1$ is a pseudoprime for the base 2.

*9. Suppose that $n > 1$ is odd and $2^{n-1} \equiv 1 \pmod{n}$. (This implies that n is either prime or a pseudoprime for the base 2.) Let $m = 2^n - 1$.

(a) Show that $2^{m-1} \equiv 1 \pmod{m}$. (Hint: Question 6 of Tutorial 1 showed that $b \mid a$ implies $2^b - 1 \mid 2^a - 1$.)

(b) Hence show that there are infinitely many pseudoprimes for the base 2.

*10. Describe a polynomial-time algorithm which determines, for a given positive integer n, whether n is a Fibonacci number.

**11. Show that every Carmichael number n is squarefree, i.e. n is the product of distinct primes. (Hint: suppose for a contradiction that $n = p^k m$ where p is prime, $k \geq 2$ and $\gcd(p, m) = 1$. Consider $a = (n/p) + 1$, and the residue of a^p modulo p^k.)