The University of Sydney
School of Mathematics and Statistics

Tutorial 5 (Week 6)

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.

Recall from lectures the following multiplicative functions of a positive integer n:

$$\begin{aligned}
\phi(n) &= \text{the number of nonnegative integers } a < n \text{ such that } \gcd(a, n) = 1,\\
\tau(n) &= \text{the number of positive integer divisors of } n,\\
\sigma(n) &= \text{the sum of the positive integer divisors of } n.
\end{aligned}$$

If n has prime factorization $p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ with $p_1, p_2, \cdots, p_r$ being distinct primes, then

$$\begin{aligned}
\phi(n) &= p_1^{k_1-1}(p_1-1)\, p_2^{k_2-1}(p_2-1) \,\cdots\, p_r^{k_r-1}(p_r-1),\\
\tau(n) &= (k_1+1)(k_2+1)\cdots(k_r+1),\\
\sigma(n) &= \frac{p_1^{k_1+1}-1}{p_1-1}\,\frac{p_2^{k_2+1}-1}{p_2-1}\cdots\frac{p_r^{k_r+1}-1}{p_r-1}.
\end{aligned}$$

Tutorial Exercises:

1. Calculate $\phi(n)$, $\sigma(n)$ and $\tau(n)$ for each of $n = 27, 28, 29, 30$.

2. What is the smallest positive integer n such that $\tau(n) = 6$?

3. Recall that a positive integer n is said to be *perfect* if $\sigma(n) = 2n$ (in other words, n equals the sum of all proper positive divisors of n). Even perfect numbers were discussed in lectures; it is not known whether odd perfect numbers exist.

(a) Show that a power of a prime number cannot be perfect.

(b) Show that a number of the form $3^a\, 5^b$ (for some nonnegative integers a, b) cannot be perfect.

4. For this question, let $f(n)$ be the *product* of the positive integer divisors of n.

(a) Find $f(2)$, $f(3)$, $f(6)$. Is f a multiplicative function?

*(b) Express $f(n)$ in terms of n and $\tau(n)$. (Hint: the first question of Tutorial 1 is relevant here.)

5. Primes p satisfy $\phi(p) = p - 1$. Which positive integers n satisfy $\phi(n) = n - 2$?

*6. Suppose that p is a prime number such that $p \equiv 3 \pmod 4$. Show that there is no integer x such that $x^2 \equiv -1 \pmod p$. (Hint: use Fermat's Little Theorem.)

Extra Exercises:

7. What is the smallest positive integer n such that $\tau(n) = 8$?

***8.** Suppose that p is a prime number such that $p \equiv 1 \pmod 4$.

(a) By considering the product

$$2 \times 4 \times 6 \times \cdots \times \left(\frac{p-1}{2}\right) \times \left(\frac{p+3}{2}\right) \times \cdots \times (p-5) \times (p-3) \times (p-1)$$

of all the even integers from 2 to $p-1$ inclusive, show that

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} \pmod p.$$

(b) Note that we either have $p \equiv 1 \pmod 8$ or $p \equiv 5 \pmod 8$. Show that if $p \equiv 5 \pmod 8$, there is no integer x such that $x^2 \equiv 2 \pmod p$.

****9.** Let n be a positive integer. Show that $\sigma(n) + \phi(n) \geq 2n$, with equality if and only if n is either prime or equal to 1. (Hint: write $n = p^k m$ where p is a prime factor of n and $\gcd(p, m) = 1$, and find a lower bound for $\sigma(n) + \phi(n)$ in terms of $\sigma(m) + \phi(m)$.)

Selected numerical answers:
1. 18, 4, 40; 12, 6, 56; 28, 2, 30; 8, 8, 72. **2.** 12.