The University of Sydney
School of Mathematics and Statistics

Tutorial 6 (Week 7)

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. This question illustrates the principles of the RSA cryptosystem with small (and hence unrealistic) numbers. Suppose that an RSA user has a public key of $(33, 3)$.

(a) Encrypt the message $[5, 30, 7]$.

(b) Use the prime factorization of 33 to find $\phi(33)$ and hence determine the private decryption exponent d.

(c) Hence decrypt the message $[2, 4, 6]$.

2. The number $n = 127349$ is the product of two different primes p and q. But, as this question will show, it would be a bad modulus for the RSA cryptosystem.

(a) Suppose that a website posts the pair (n, e) as its public RSA key, where $n = 127349$ and $e = 5$. If someone wants to send the (single-letter) message 100 to the website using this cryptosystem, what should their ciphertext be?

(b) Now suppose you are an eavesdropper and want to be able to decrypt messages sent to the website. Apply Fermat's factorization method to the number n to find p and q, and hence find $\phi(n)$.

(c) Find the private decryption exponent d for this cryptosystem.

3. The number $n = 35203807$ is the product of two different primes p and q. Given that $\phi(n) = 35191440$, find p and q.

*__4.__ Using RSA moduli as small as those in the above questions would be insecure enough, but what would be even worse would be using a public key (n, e) for which the decryption exponent d was *equal* to the encryption exponent e. This happens when e is self-inverse modulo $\phi(n)$, i.e. $e^2 \equiv 1 \pmod{\phi(n)}$.

(a) Show that if $n = 35$, every possible choice of encryption exponent e has this property.

(b) Suppose that n is a product of distinct odd primes p and q. Show that there is a solution of $e^2 \equiv 1 \pmod{\phi(n)}$ which is not one of the obvious solutions $e \equiv \pm 1 \pmod{\phi(n)}$.

**5. The Möbius Inversion Formula tells us that, if f and F are two functions on the positive integers such that

$$F(n) = \sum_{d|n} f(d) \qquad \text{for all } n \in \mathbb{Z}^+,$$

then we have

$$f(n) = \sum_{d|n} \mu(n/d)\, F(d) \qquad \text{for all } n \in \mathbb{Z}^+.$$

Use this to find a formula for the number $B(n)$ of strings of n bits (each bit being either 0 or 1) which are *aperiodic*, meaning that there is no proper divisor d of n such that the string is periodic with period d. (For example, when $n = 4$, the string 0110 is aperiodic, but 0101 is not since it has period 2.)

Extra Exercises:

6. Suppose that an RSA cryptosystem has public key $(454980781, 17)$. Given that the prime factorization of 454980781 is 15581×29201, find the decryption exponent.

***7.** Let n be a positive integer. Prove that

$$\sum_{d|n} \frac{\mu(d)^2}{\phi(d)} = \frac{n}{\phi(n)},$$

where ϕ is Euler's phi function, μ is the Möbius function, and the sum on the left-hand side is over all positive integer divisors of d.

8. (a) For which values of $n \in \mathbb{Z}^+$ is Euler's phi function odd?

(b) Find all values $n \in \mathbb{Z}^+$ (if any) that solve

$$\phi(n) = \frac{n}{2}.$$

(c) Find all values $n \in \mathbb{Z}^+$ (if any) such that $\phi(n) = 98$.

****9.** Let n be a positive integer. A complex number z is said to be a *primitive nth root of unity* if $z^n = 1$ and there is no smaller positive integer m such that $z^m = 1$. Use the Möbius Inversion Formula to show that the sum of the primitive nth roots of unity is $\mu(n)$. (Hint: if $n > 1$, the sum of all the complex nth roots of unity is zero, because the coefficient of z^{n-1} in the polynomial $z^n - 1$ is zero.)

Selected numerical answers:
1. [26,6,13], 7, [29,16,30]. **2.** 47124, 126636, 101309. **3.** 4441, 7927.