The University of Sydney
School of Mathematics and Statistics

Tutorial 1 (Week 2)

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

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

Tutorials will be held in Weeks 2–13, so Tutorial n is held in Week $n+1$; it usually relates to the material introduced in the lectures in Week n. In the tutorials you should work in small groups, and aim to complete the part labelled "tutorial exercises"; you are encouraged to try the "extra exercises" afterwards. **Full solutions to Tutorial n will be available from the MATH2068 webpage by the end of Week $n+1$.** Numerical answers to selected tutorial exercises are at the end of the sheet.

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. Write down the (positive integer) divisors of 28 in increasing order; you should find that there are six of them. Observe that they can be grouped into three pairs where the two numbers in each pair multiply together to give 28. Bearing this in mind, which positive integers n have an odd number of divisors?

2. In each case, use the Euclidean Algorithm to find the greatest common divisor $\gcd(a, b)$.

(a) $a = 35$, $b = 14$. (b) $a = 168$, $b = 132$. (c) $a = 847$, $b = 510$.

3. For each of the pairs a, b in the previous question, find integers s, t such that $\gcd(a, b) = sa + tb$.

4. Find the prime factorizations of 2016 and 2068. (Simple trial division will work.)

5. Use Fermat's factorization method to factorize 629 and 3139.

***6.** (a) Suppose that $a = qb$, with $a, b, q \in \mathbb{Z}^+$. Show that $2^b - 1$ divides $2^a - 1$.

(b) Hence show that if a is a composite number, then so is $2^a - 1$.

(c) Now suppose that $a = qb + r$, with $a, b, q \in \mathbb{Z}^+$ and $0 \leq r < b$, so that r is the residue of a modulo b. Show that $2^r - 1$ is the residue of $2^a - 1$ modulo $2^b - 1$.

(d) Bearing the Euclidean Algorithm in mind, show that for any positive integers a, b we have $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$.

Extra Exercises:

7. Find the prime factorization of 2017.

8. Let k be a positive integer and p a prime. Find a formula for the sum of all the (positive integer) divisors of p^k.

*__9.__ Use the identity

$$(x^2 - 2xy + 2y^2)(x^2 + 2xy + 2y^2) = x^4 + 4y^4$$

to determine all pairs of positive integers n, m such that $n^4 + 4m^4$ is prime.

**__10.__ Suppose we want to factorize $n = 10875593$. It turns out that, if we were to apply Fermat's method naively, it would take a long search before we found our desired m such that $m^2 - n$ is a square. However, we might notice as we carried out that search (presumably with the help of a calculator or MAGMA) that

$$3306^2 - n = 11 \times 17^3,$$
$$3834^2 - n = 11^3 \times 13^2 \times 17.$$

Neither of these right-hand sides is a square, as you can tell from the odd exponents, but their product is a square:

$$(3306^2 - n)(3834^2 - n) = 11^4 \times 13^2 \times 17^4 = (11^2 \times 13 \times 17^2)^2.$$

Use this information (and your calculator) to find a nontrivial divisor of n.

Selected numerical answers:
1. 1, 2, 4, 7, 14, 28. **2.** 7, 12, 1. **4.** $2^5 \times 3^2 \times 7$, $2^2 \times 11 \times 47$. **5.** 17×37, 43×73.