# Math 261 — Exercise sheet 1

`http://staff.aub.edu.lb/~nm116/teaching/2018/math261/index.html`

Version: September 10, 2018

Answers are due for Wednesday 19 September, 11AM.

The use of calculators is allowed.

## Exercise 1.1: An "obvious" factorisation (20 pts)

1. (10 pts) Let $n \geq 2$ be an integer, and let $N = n^2 - 1$. Depending on the value of $n$, $N$ can be prime or not; for example $N = 3$ is prime if $n = 2$, but $N = 8$ is composite if $n = 3$. Find all $n \geq 2$ such that $N$ is prime.

   *Hint:* $a^2 - b^2 =$ *?*

2. (10 pts) Factor $N = 9999$ into primes. Make sure to prove that the factors you find are prime.

## Exercise 1.2: (In)variable gcd's (20 pts)

Let $n \in \mathbb{Z}$.

1. (10 pts) Prove that $\gcd(n, 2n + 1) = 1$, no matter what the value of $n$ is.

   *Hint: How do you prove that two integers are coprime?*

2. (10 pts) What can you say about $\gcd(n, n + 2)$?

## Exercise 1.3: Euclid and Bézout (40 pts)

1. (10 pts) Compute $g = \gcd(543, 210)$, and find integers $x, y$ such that

$$543x + 210y = g.$$

2. (10 pts) Find all $x$ and $y \in \mathbb{Z}$ such that $543x + 210y = 261$.

3. (10 pts) Find all $x$ and $y \in \mathbb{Z}$ such that $543x + 210y = 2018$.

4. (10 pts) (*From last year's midterm*) How many different ways are there are to pay \$10000 using only banknotes of \$20 and \$50?

   *Hint: Why is this question in this exercise?*

## Exercise 1.4: Another algorithm for the gcd (20 pts)

1. (10 pts) Let $a, b \in \mathbb{Z}$ be integers. Prove that $\gcd(a, b) = \gcd(b, a - b)$.
2. (10 pts) Use the previous question to design an algorithm to compute $\gcd(a, b)$ similar to the one seen in class, but using subtractions instead of Euclidean divisions. Demonstrate its use on the case $a = 50$, $b = 22$.

---

**The exercises below are not mandatory. They are not worth any points, but I highly recommend that you try to solve them for practice. The solutions will be made available with the solutions to the other exercises.**

## Exercise 1.5

Let $a$, $b$ and $c$ be integers. Suppose that $a$ and $b$ are coprime, and that $a$ and $c$ are coprime. Prove that $a$ and $bc$ are coprime.

## Exercise 1.6: Fermat numbers

Let $n \in \mathbb{N}$, and let $N = 2^n + 1$. Prove that if $N$ is prime, then $n$ must be a power of 2.

*Hint: use the identity* $x^m + 1 = (x + 1)(x^{m-1} - x^{m-2} + \cdots - x + 1)$, *which is valid for all* ***odd*** $m \in \mathbb{N}$.

*Remark: The* Fermat numbers *are the* $F_n = 2^{2^n} + 1$, $n \in \mathbb{N}$. *They are named after the French mathematician Pierre de Fermat, who noticed that* $F_0$, $F_1$, $F_2$, $F_3$ *and* $F_4$ *are all prime, and conjectured in 1650 that* $F_n$ *is prime for all* $n \in \mathbb{N}$. *However, this turned out to be wrong: in 1732, the Swiss mathematician Leonhard Euler proved that* $F_5 = 641 \times 6700417$ *is not prime. To this day, no other prime Fermat number has been found; in fact it is unknown if there is any ! This is because* $F_n$ *grows very quickly with* $n$, *which makes it very difficult to test whether* $F_n$ *is prime, even with modern computers.*