Math 261 — Exercise sheet 1

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

Version: September 19, 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.

Solution 1.1:

1. We have $N = n^2 - 1^2 = (n+1)(n-1)$. Beware however that this does not mean that N is composite, since one of the factors could be ± 1! Since we are assuming $n \geq 2$, $n+1$ can never be ± 1; and we have $n - 1 = \pm 1$ only when $n = 2$. As a result, N is prime only when $n = 2$.

2. By the same principle, $9999 = 10000 - 1 = 100^2 - 1 = 99 \cdot 101$. Now $99 = 9 \cdot 11 = 3^2 \cdot 11$, and 11 is prime (else it would be divisible by a prime $\leq \sqrt{11} \approx 3.3$, but it is not divisible by 2 nor by 3. Similarly, if 101 were composite, if would be divisible by a prime $\leq \sqrt{101} \approx 10$, so by 2, 3, 5, or 7. But

$$2 \mid 101 \Longrightarrow 2 \mid (101 - 100) = 1, \text{ absurd,}$$

$$3 \mid 101 \Longrightarrow 3 \mid (101 - 99) = 2, \text{ absurd,}$$

$$5 \mid 101 \Longrightarrow 5 \mid (101 - 100) = 1, \text{ absurd,}$$

$$7 \mid 101 \Longrightarrow 7 \mid (101 - 70) = 31 \Longrightarrow 7 \mid (35 - 31) = 4, \text{ absurd.}$$

   So 101 is prime, and the complete factorisation of 9999 is

$$9999 = 3^2 \cdot 11 \cdot 101.$$

   Remark: This illustrates the fact that $(n+1)(n-1)$ *is not in general the complete factorisation of* $n^2 - 1$.

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 $\gcd(n, n+2)$?

Solution 1.2:

1. Remember that two integers a and b are coprime if and only if there exist integers x and y such that $ax + by = 1$.

   Since $(n)(-2) + (2n+1)(1) = 1$, n and $2n+1$ are coprime.

2. Let $g = \gcd(n, n+2)$. By Strong Bézout, $2 = n(-1) + (n+2)(1)$ is a multiple of g, so g can only be 1 or 2. Besides, if $n = 2k$ is even, then so is $n + 2 = 2k + 2 = 2(k+1)$, and if $n = 2k+1$ is odd, then so is $n + 2 = 2(k+1) + 1$. Conclusion: $g = 2$ if n is even, and $g = 1$ if n is odd.

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?

Solution 1.3:

1. To compute the gcd, Euclid's algorithm goes as follows:

$$\begin{array}{r|l} 543 & 210 \\ \cline{2-2} 123 & 2 \end{array}$$

$$\begin{array}{r|l} 210 & 123 \\ \cline{2-2} 87 & 1 \end{array}$$

$$\begin{array}{r|l} 123 & 87 \\ \cline{2-2} 36 & 1 \end{array}$$

$$\begin{array}{r|l} 87 & 36 \\ \cline{2-2} 15 & 2 \end{array}$$

$$\begin{array}{r|l} 36 & 15 \\ \cline{2-2} 6 & 2 \end{array}$$

$$\begin{array}{r|l} 15 & 6 \\ \hline 3 & 2 \end{array}$$

$$\begin{array}{r|l} 6 & 3 \\ \hline 0 & 2 \end{array}$$

The gcd is the last nonzero remainder, which is 3 in this case.

In order to find x and y, we read these divisions from the bottom up:

$$\begin{aligned} 3 &= 15 - 6 \cdot 2 \\ &= 15 - (36 - 15 \cdot 2) \cdot 2 = 15 \cdot 5 - 36 \cdot 2 \\ &= (87 - 36 \cdot 2) \cdot 5 - 36 \cdot 2 = 87 \cdot 5 - 36 \cdot 12 \\ &= 87 \cdot 5 - (123 - 87) \cdot 12 = 87 \cdot 17 - 123 \cdot 12 \\ &= (210 - 123) \cdot 17 - 123 \cdot 12 = 210 \cdot 17 - 123 \cdot 29 \\ &= 210 \cdot 17 - (543 - 210 \cdot 2) \cdot 29 \\ &= 210 \cdot 75 - 543 \cdot 29, \end{aligned}$$

so we can take $x = -29$, $y = 75$.

2. Since $261/3 = 87$ is an integer, $3 \mid 261$, so there are infinitely many solutions. Thanks to the previous question, we have the solution $x = -29 \cdot 87 = -2523$, $y = 75 \cdot 87 = 6525$. Besides, we can simplify the equation by 3, which yields

$$181x + 70y = 87;$$

and since 3 was the gcd, we know that 181 and 70 must be coprime, so that we get all the solutions by adding a multiple of 70 to x, and subtracting the same multiple of 181 from y. Therefore, the solutions are

$$x = -2523 + 70t, y = 6525 - 181t \quad (t \in \mathbb{Z}).$$

Remark: We can use this formula to discover simpler solutions. For instance, for $t = 36$ we find the solution $x = -3$, $y = 9$, which is much more appealing! This also means that the general solution can also be described as $x = -3+70t$, $y = 9 - 181t$ $(t \in \mathbb{Z})$.

3. This time $3 \nmid 2018$, so there are no solutions.

4. This corresponds to finding the integer solutions of $20x + 50y = 10000$. Since $\gcd(20, 50) = 10$ divides 10000, there are solutions, and the equation can be simplified into

$$2x + 5y = 1000.$$

One solution is $x = 500$, $y = 0$, so the solutions are given by

$$x = 500 - 5t, \; y = 2t, \; t \in \mathbb{Z}.$$

But we also must have $x \geqslant 0$ and $y \geqslant 0$! In other words, $500 - 5t \geqslant 0$, so $t \leqslant 100$, and $2t \geqslant 0$, so $t \geqslant 0$. So the solutions with $x \geqslant 0$ and $y \geqslant 0$ are given by the $t \in \mathbb{Z}$ such that $0 \leqslant t \leqslant 100$. That is 101 ways.

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 $a = 50$, $b = 22$.

Solution 1.4:

1. If d divides a and b, then d also divides $a - b$. Conversely, if d divides b and $a - b$, then it also divides $b + (a - b) = a$. Therefore, the two pairs (a, b) and $(b, a - b)$ have the same common divisors, and in particular the same gcd.

2. We can repeatedly replace the pair (a, b) and $(b, a - b)$ so as to make its size decrease until the gcd is obvious. For instance,

$$\begin{aligned}
\gcd(50, 22) &= \gcd(22, 50 - 22) = \gcd(28, 22) \\
&= \gcd(22, 28 - 22) = \gcd(22, 6) \\
&= \gcd(22 - 6, 6) = \gcd(16, 6) \\
&= \gcd(16 - 6, 6) = \gcd(10, 6) \\
&= \gcd(6, 10 - 6) = \gcd(6, 4) \\
&= \gcd(4, 6 - 4) = \gcd(4, 2) \\
&= \gcd(2, 4 - 2) = \gcd(2, 2) \\
&= 2.
\end{aligned}$$

Remark: This is how Euclid's original algorithm worked. The version with Euclidean divisions seen in class is more efficient: if the division is $a = bq + r$, it goes from (a, b) to (b, r) directly in one step, whereas this version takes (a, b) to $(b, a - b)$, then to $(b, a - 2b)$, and so on, and thus takes q steps to reach (b, r).

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.

Solution 1.5

Suppose that $d \in \mathbb{N}$ is such that $d \mid a$ and $d \mid bc$. Since $d \mid a$, d and b are coprime. Indeed, a divisor of d is also a divisor of a, so a common divisor of d and b is a common divisor of a and b, which can only be ± 1 since a and b are coprime. We can now conclude by Gauss's lemma: since $d \mid bc$ and d is coprime to b, we must have $d \mid c$. So d is a common divisor of a and c; since a and c are coprime, d can only be ± 1. So the only common divisors of a and bc are ± 1.

Here is an alternative, less obvious proof using Bézout: since a and b are coprime, there are u and $v \in \mathbb{Z}$ such that $au + bv = 1$. Similarly, there are u' and $v' \in \mathbb{Z}$ such that $au' + cv' = 1$. By multiplying these identities, we get

$$1 = (au + bv)(au' + cv') = a(uau' + ucv' + bvu') + bc(vv').$$

This last identity has the form $1 = ax + (bc)y$ with $x, y \in \mathbb{Z}$, which proves 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*** $m \in \mathbb{N}$.

Solution 1.6:

Suppose on the contrary that n is not a power of 2. Then n is divisible by at least one odd prime. Let p be such a prime, and write $n = pq$ with $q \in \mathbb{N}$. We thus have

$$N = 2^n + 1 = 2^{pq} + 1 = (2^q)^p + 1 = (2^q + 1)(2^{q(p-1)} - 2^{q(p-2)} + \cdots - 2^q + 1)$$

according to the hint, since p is odd.

In order to conclude that N is composite, it is therefore enough to prove that none of these two factors is ± 1. But clearly $2^q + 1 > 1$, and if we had $2^{q(p-1)} - 2^{q(p-2)} + \cdots - 2^q + 1 = \pm 1$, then we would have $2^{pq} + 1 = \pm(2^q + 1)$, which is clearly impossible since $p \geqslant 3$. We have thus found a non-trivial factorization of N, so N is composite.

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.*