Math 261 — Exercise sheet 1

http://staff.aub.edu.lb/~nm116/teaching/2017/math261/index.html

Version: September 18, 2017

Answers are due for Monday 18 September, 11AM.

The use of calculators is allowed.

Exercise 1.1

Use Euclid's algorithm to prove that 2017 and 261 are coprime, and to find integers u and v such that $2017u + 261v = 1$.

Solution 1.1

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

$$\begin{array}{rl} 2\,0\,1\,7 & \mid\ 2\,6\,1 \\ \hline 1\,9\,0 & \mid\ 7 \end{array}$$

$$\begin{array}{rl} 2\,6\,1 & \mid\ 1\,9\,0 \\ \hline 7\,1 & \mid\ 1 \end{array}$$

$$\begin{array}{rl} 1\,9\,0 & \mid\ 7\,1 \\ \hline 4\,8 & \mid\ 2 \end{array}$$

$$\begin{array}{rl} 7\,1 & \mid\ 4\,8 \\ \hline 2\,3 & \mid\ 1 \end{array}$$

$$\begin{array}{rl} 4\,8 & \mid\ 2\,3 \\ \hline 2 & \mid\ 2 \end{array}$$

$$\begin{array}{rl} 2\,3 & \mid\ 2 \\ \hline 0\,3 & \mid\ 1\,1 \\ 1 & \mid \end{array}$$

$$\begin{array}{rl} 2 & \mid\ 1 \\ \hline 0 & \mid\ 2 \end{array}$$

The gcd is the last nonzero remainder, which is 1 in this case. This means that 2017 and 261 are coprime.

In order to find u and v such that $2017u + 261v = 1$, we first rewrite the above divisions in a way that isolates the remainder (in **bold**) on one side:

$$\begin{aligned} \mathbf{190} &= 2017 - 7 \times 261 \\ \mathbf{71} &= 261 - 190 \\ \mathbf{48} &= 190 - 2 \times 71 \\ \mathbf{23} &= 71 - 48 \\ \mathbf{2} &= 48 - 2 \times 23 \\ \mathbf{1} &= 23 - 11 \times 2 \end{aligned}$$

Then we use these equations to express **1** (the gcd) as a combination of the terms of each division from bottom up:

$$\begin{aligned} \mathbf{1} &= 23 - 11 \times \mathbf{2} \\ &= 23 - 11 \times (48 - 2 \times 23) = (1 + 11 \times 2) \times 23 - 2 \times 48 = 23 \times \mathbf{23} - 11 \times 48 \\ &= 23 \times (71 - 48) - 11 \times 48 = 23 \times 71 + (-23 - 11) \times 48 = 23 \times 71 - 34 \times \mathbf{48} \\ &= 23 \times 71 - 34 \times (190 - 2 \times 71) = (23 + 34 \times 2) \times 71 - 34 \times 190 = 91 \times \mathbf{71} - 34 \times 190 \\ &= 91 \times (261 - 190) - 34 \times 190 = 91 \times 261 + (-91 - 34) \times 190 = 91 \times 261 - 125 \times \mathbf{190} \\ &= 91 \times 261 - 125 \times (2017 - 7 \times 261) = 966 \times 261 - 125 \times 2017. \end{aligned}$$

So we can take $u = -125$, $v = 966$.

Exercise 1.2

1. Factor 261 into primes. Make sure to prove that you factorization is complete, i.e. that the factors you find are prime.

2. Deduce the number of divisors of 261, and the sum of these divisors.

3. Do the same computations with 6000 instead of 261.

Solution 1.2

1. Since $2 + 6 + 1 = 9$, 261 is divisible by 9. In fact, $261 + 9 = 270 = 30 \times 9$, so $261 = 29 \times 9$.

   Now, of course $9 = 3^2$ and 3 is prime; besides, if 29 were not prime, then it would be divisible by a prime $\leqslant 5$ since $\sqrt{29} < \sqrt{36} = 6$. But neither 2 nor 3 nor 5 divide 29, so 29 is prime.

   So finally the prime factorization of 261 is

   $$261 = 3^2 \times 29.$$

2. From the formulas $\sigma_0\left(\prod p_i^{a_i}\right) = \prod(1 + a_i)$ and $\sigma_1\left(\prod p_i^{a_i}\right) = \prod \frac{p_i^{a_i+1}-1}{p_i-1}$, we find that

   $$\sigma_0(261) = (1 + 2) \times (1 + 1) = 6,$$

   and that

   $$\sigma_1(261) = \frac{3^3 - 1}{3 - 1} \times \frac{29^2 - 1}{29 - 1} = 13 \times 30 = 390.$$

3. We have $6000 = 6 \times 1000 = 2 \times 3 \times 10^3 = 2 \times 3 \times (2 \times 5)^3 = 2^4 \times 3 \times 5^3$, so

$$\sigma_0(6000) = (1+4) \times (1+1) \times (1+3) = 40$$

and

$$\sigma_1(6000) = \frac{2^5-1}{2-1} \times \frac{3^2-1}{3-1} \times \frac{5^4-1}{5-1} = 31 \times 4 \times 156 = 19344.$$

Exercise 1.3

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 1.3

Suppose that $d \in \mathbb{N}$ is such that $d \mid a$ and $d \mid bc$. Since $d \mid a$, d aqnd 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 Euclid'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 1.4: 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 1.4:

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.

Exercise 1.5: $\sqrt{n}$ is either an integer or irrational

Let n be a positive integer which is **not a square**, so that $\sqrt{n}$ is not an integer. The goal of this exercise is to prove that $\sqrt{n}$ is *irrational*, i.e. not of the form $\frac{a}{b}$ where a and b are integers.

1. Prove that there exists at least one prime p such that the p-adic valuation $v_p(n)$ is odd.

2. Suppose on the contrary that $\sqrt{n} = \frac{a}{b}$ with $a, b \in \mathbb{N}$; this may be rewritten as $a^2 = nb^2$. Examine the p-adic valuations of both sides of this equation, and derive a contradiction.

Solution 1.5:

1. Write the factorization of n as $\prod p_i^{a_i}$, where $a_i = v_{p_i}(n)$. If the a_i were all even, then the $a_i/2$ would all be integers, and so we would have $n = m^2$ with $m = \prod p_i^{a_i/2}$, contradicting our hypothesis that n is not a square. So at least one of the a_i is odd, and we can take p to be the corresponding p_i.

2. On the one hand, $v_p(a^2) = 2v_p(a)$ is even; on the other hand, $v_p(nb^2) = v_p(n) + v_p(b^2) = v_p(n) + 2v_p(b)$ is odd, since we have chosen p so that $v_p(n)$ is odd. So the p-adic valuation of the integer $a^2 = nb^2$ is both even and odd, which is absurd.

The exercise below is not mandatory. It is not worth any points, and it is also more difficult than the previous ones. I highly recommend that you try to solve it for practice. The solution will be made available with the solutions to the other exercises.

Exercise 1.6: Perfect numbers

A positive integer n is said to be *perfect* if it agrees with the sum of all of its divisors other than itself; in other words, if $\sigma_1(n) = 2n$. For instance, 6 is a perfect number, because its divisors other than itself are 1, 2 and 3, and $1 + 2 + 3 = 6$.

1. Let a be a positive integer, and let $n = 2^a(2^{a+1} - 1)$. Prove that if $2^{a+1} - 1$ is prime, then n is perfect.

   We now want to prove that all **even** perfect numbers are of this form.

2. Let n be an even number. Why may we find integers a and b such that $n = 2^a b$ and b is odd ?

3. In this question and in the following ones, we suppose that n is an even perfect number. Prove that $(2^{a+1}-1) \mid b$.

4. Let thus $c \in \mathbb{N}$ be such that $b = (2^{a+1}-1)c$. Prove that $\sigma_1(b) = b + c$.

5. Deduce that $c = 1$.

6. Conclude that $2^{a+1} - 1$ is prime.

7. Find two even perfect numbers (apart from 6).

Solution 1.6:

1. The relation $2 \times 2^a + (-1) \times (2^{a+1}-1) = 1$ proves that 2^a and $2^{a+1}-1$ are coprime, so
$$\sigma_1\big(2^a(2^{a+1}-1)\big) = \sigma_1(2^a)\sigma_1(2^{a+1}-1)$$
since σ_1 is a multiplicative function.

   Now, we have $\sigma_1(2^a) = \frac{2^{a+1}-1}{2-1} = 2^{a+1}-1$. Besides, for every prime $p \in \mathbb{N}$ we obviously have $\sigma_1(p) = 1 + p$, so if $2^{a+1}-1$ is prime, then $\sigma_1(2^{a+1}-1) = 2^{a+1}$, which implies that
$$\sigma_1(n) = (2^{a+1}-1)2^{a+1} = 2n,$$
   which means that n is perfect.

2. Let $n = \prod_{i=1}^{r} p_i^{a_i}$ be the factorization of n. Since n is even, one of the p_i, say p_1 is equal to 2, and it exponent a_1 is $\geqslant 1$. We can thus take $a = a_1$ and $b = \prod_{i=2}^{r} p_i^{a_i}$; indeed, since the p_i are prime and $\neq 2$ for $i \geqslant 2$, they are odd, so b, as a product of odd numbers, is odd.

   Alternative proof: since 2 is prime and does not divide any of the p_i for $i \geqslant 2$, it does not divide b by Euclid's lemma.

3. Since b is odd, 2^a and b are coprime, so by multiplicativity of σ_1 we get
$$\sigma_1(n) = \sigma_1(2^a)\sigma_1(b) = (2^{a+1}-1)\sigma_1(b).$$
   But if n is perfect, then $\sigma_1(n) = 2n$, so we find that $(2^{a+1}-1) \mid 2n$. Next, $(2^{a+1}-1)$ is clearly odd, so it is coprime to 2; by Euclid's lemma, we must have $(2^{a+1}-1) \mid n$.

4. We have
$$2^{a+1}b = 2n = \sigma_1(n) = (2^{a+1}-1)\sigma_1(b),$$
   so
$$\sigma_1(b) = \frac{2^{a+1}b}{2^{a+1}-1} = \frac{2^{a+1}(2^{a+1}-1)c}{2^{a+1}-1} = 2^{a+1}c = (2^{a+1}-1)c + c = b + c.$$

5. If $c > 1$, then 1, c, and b are three *distinct* divisors of b, so that
$$1 + c + b \leqslant \sigma_1(b) = b + c,$$
   which is impossible. So necessarily $c = 1$.

6. From $c = 1$, we deduce that $b = (2^{a+1} - 1)c = 2^{a+1} - 1$, and that $\sigma_1(b) = b + c = b + 1$. Now, clearly 1 and b are divisors of b, and they are disctinct since $a \geqslant 1$. If b had other divisors, then we would have $\sigma_1(b) > 1 + b$, which is not the case. So the only divisors of b are 1 and b itself, which means that b is prime.

7. According to the previous questions, we need to look for integers $a \in \mathbb{N}$ such that $2^{a+1} - 1$ is prime; and then $n = 2^a(2^{a+1} - 1)$ will be a perfect number. We see that $a = 1$ works, but it corresponds to $n = 6$, so we need to try larger values of a.

   For $a = 2$, we have $2^{a+1} - 1 = 7$, which is prime; so $n = 2^a \times 7 = 28$ is a perfect number.

   For $a = 3$, we have $2^{a+1} - 1 = 15 = 3 \times 5$, which is composite; so we keep looking.

   For $a = 4$, we have $2^{a+1} - 1 = 31$, which is prime; so $n = 2^a \times 31 = 496$ is another perfect number.

Remarks: Prime numbers of the form $2^a - 1$ are called Mersenne primes *after Marin Mersenne (French, 17th century). Not all numbers of the form $2^a - 1$ are prime though; in fact, it is not very difficult to show that if $2^a - 1$, then a is also prime. However this condition is not sufficient, as the counter-example $2^{11} - 1 = 23 \times 89$ shows. In fact, as of today, only 49 primes a such that $2^a - 1$ is prime are known. As a result, only 49 Mersenne primes, and so only 49 even perfect numbers, are known. It is conjectured that there exist infinitely many Mersenne primes, and so infinitely many even perfect numbers, but this has never been proved. As for odd perfect numbers, if is unknown if any exist.*