Introduction to number theory
Exercise sheet 1

`https://www.maths.tcd.ie/~mascotn/teaching/2020/MAU22301/index.html`

Version: October 16, 2020

Answers are due for Friday October 16th, 2PM.
The use of electronic calculators and computer algebra software is allowed.

Exercise 1 *Money money money (100 pts)*

How many ways are there to pay one million euros, using only 20 euro and 50 euro notes? (For instance, we could use 50,000 20 euro notes and 0 50 euro notes, or 25,000 20 euro notes and 10,000 50 euro notes, etc.)

Hint: Solve the Diophantine equation $20x + 50y = 1,000,000$.

NB you are not allowed to give a negative amount of one kind of notes, even to compensate for a large positive amounts of the other kind! So for instance, 100,000 20 euro notes plus -20,000 50 euro notes is not an acceptable form of payment — unless you claim to master the creation of antimatter, but I will definitely want to see proof of that.

Solution 1

We want to solve the equation $20x + 50y = 1,000,000$ with x and y non-negative integers. We will begin by solving it without the non-negativity condition, and then impose this condition later.

We thus begin by solving $20x + 50y = 1,000,000$ for $x, y \in \mathbb{Z}$. We have $\gcd(20, 50) = 10$, as can be seen either by Euclid's algorithm ($50 = 20 \times 2 + 10$, $20 = 10 \times 2 + 0$), or by direct inspection of the divisors of $20 = 2^2 \times 5$ and of $50 = 2 \times 5^2$. Since $10 \mid 1,000,000$, we do have solutions.

In order to proceed, we simplify by $\gcd(20, 50) = 10$, which yields $2x + 5y = 100,000$ (an 2 and 5 are automatically coprime).

Next, we need a particular solution. We may take $x_0 = 50,000$, $y_0 = 0$, which corresponds to the first example given in the question.

As 2 and 5 are coprime, we know that the solutions to the equation are $x = x_0 - 5k = 50,000 - 5k$, $y = y_0 + 2k = 2k$ for $k \in \mathbb{Z}$. This solves the equation for $x, y \in \mathbb{Z}$.

Finally, we re-inject the non-negativity condition. The fact that $y \geqslant 0$ yields $k \geqslant 0$, and the fact that $x \geqslant 0$ say that $50,000 - 5k \geqslant 0$, which amounts to $k \leqslant 10,000$. This shows that the solutions to $20x+50y = 1,000,000$ are $x = 50,000-5k$, $y = 2k$, for $0 \leqslant k \leqslant 10,000$ an integer. As there are $10,001$ such k, and as each value of k corresponds to a different solution (obviously, since $y = 2k$), we conclude that

There are 10,001 ways to make this payment.

This was the only mandatory exercise, that you must submit before the deadline. The following exercises are not mandatory; they are not worth any points, and you do not have to submit them. However, I highly recommend that you try to solve them for practice, and you are welcome to email me if you have questions about them. The solutions will be made available with the solution to the mandatory exercise.

Exercise 2 *Euclid at work*

Prove that 2020 and 353 are coprime, and find integers u and v such that

$$2020u + 353v = 1.$$

Solution 2

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

$$\begin{array}{r|l} 2\,0\,2\,0 & \underline{3\,5\,3} \\ 2\,5\,5 & 5 \end{array}$$

$$\begin{array}{r|l} 3\,5\,3 & \underline{2\,5\,5} \\ 9\,8 & 1 \end{array}$$

$$\begin{array}{r|l} 2\,5\,5 & \underline{9\,8} \\ 5\,9 & 2 \end{array}$$

$$\begin{array}{r|l} 9\,8 & \underline{5\,9} \\ 3\,9 & 1 \end{array}$$

$$\begin{array}{r|l} 5\,9 & \underline{3\,9} \\ 2\,0 & 1 \end{array}$$

$$\begin{array}{r|l} 3\,9 & \underline{2\,0} \\ 1\,9 & 1 \end{array}$$

$$\begin{array}{r|l} 2\,0 & \underline{1\,9} \\ 1 & 1 \end{array}$$

$$\begin{array}{r|l} 1\,9 & \underline{1} \\ 0\,9 & 1\,9 \\ 0 & \end{array}$$

The gcd is the last nonzero remainder, which is 1 in this case. This means that 2020 and 353 are coprime.

In order to find u and v such that $2020u + 353v = 1$, we first rewrite the above divisions in a way that isolates the remainder (in **bold**) on one side:

$$\begin{aligned}
\mathbf{255} &= 2020 - 5 \times 353 \\
\mathbf{98} &= 353 - 255 \\
\mathbf{59} &= 255 - 2 \times 98 \\
\mathbf{39} &= 98 - 59 \\
\mathbf{20} &= 59 - 39 \\
\mathbf{19} &= 39 - 20 \\
\mathbf{1} &= 20 - 19
\end{aligned}$$

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

$$\begin{aligned}
\mathbf{1} &= 20 - \mathbf{19} \\
&= 20 - (39 - 20) = \mathbf{20} \times 2 - 39 \\
&= (59 - 39) \times 2 - 39 = 59 \times 2 - \mathbf{39} \times 3 \\
&= 59 \times 2 - (98 - 59) \times 3 = \mathbf{59} \times 5 - 98 \times 3 \\
&= (255 - 98 \times 2) \times 5 - 98 \times 3 = 255 \times 5 - \mathbf{98} \times 13 \\
&= 255 \times 5 - (353 - 255) \times 13 = \mathbf{255} \times 18 - 353 \times 13 \\
&= (2020 - 353 \times 5) \times 18 - 353 \times 13 = 2020 \times 18 - 353 \times 103
\end{aligned}$$

So we can take $u = 18$, $v = -103$.

Exercise 3 *An "obvious" factorisation*

1. 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. Factor $N = 9999$ into primes. Make sure to prove that the factors you find are prime.

Solution 3

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 4 *(In)variable gcd's*

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

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

Solution 4

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 5 *Another algorithm for the gcd*

1. Let $a, b \in \mathbb{Z}$ be integers. Prove that $\gcd(a, b) = \gcd(b, a-b)$.

2. 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 5

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).

Exercise 6 *Product of coprimes*

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 6

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.

And here is a third proof, in terms of prime factorisations this time: Since a and b are coprime, the primes in the factorisation of b are all distinct from those in the factorisation of a. Similarly, the primes in the factorisation of c are all distinct from those in the factorisation of a. Now, the prime factorisation of bc is obtained by merging that of b with that of c (which could involve regrouping some primes b and c have in common, since b and c may not be coprime); as a result, it still does not involve any prime that appears in the factorissation of a. This shows that a and bc are coprime (think of how you can read the factorisation of the gcd of two integers off their respective factorisations).

Exercise 7 *Valuations*

1. Let $m = \prod_i p_i^{a_i}$, $n = \prod_i p_i^{b_i}$ be two integers, where the p_i are pairwise distinct primes. Prove that $m \mid n$ iff. $a_i \leqslant b_i$ for each i.

   Hint: If $n = km$, consider the prime factorisation of k.

2. In what follows, let $p \in \mathbb{N}$ be prime. Recall that for nonzero $n \in \mathbb{Z}$, we define $v_p(n)$ as the exponent of p in n. Prove that for all nonzero $n \in \mathbb{Z}$, $v_p(n)$ is the largest integer v such that $p^v \mid n$.

3. Recall that we set $v_p(0) = +\infty$ by convention. In view of the previous question, does this convention seem appropriate?

4. Let $m, n \in \mathbb{Z}$, both nonzero. Prove that $v_p(mn) = v_p(m) + v_p(n)$. What happens if m or n is zero?

5. Let $m, n \in \mathbb{Z}$, both nonzero. Prove that $v_p(m+n) \geqslant \min(v_p(m), v_p(n))$. What happens if m or n is zero?

6. Let $m, n \in \mathbb{Z}$. Prove that if $v_p(m) \neq v_p(n)$, then $v_p(m+n) = \min(v_p(m), v_p(n))$.

7. Give an example where $v_p(m+n) > \min(v_p(m), v_p(n))$.

Solution 7

1. If $m \mid n$, we have $n = km$ for some integer k. Possibly after extending[1] the set of primes p_i, we may factor $k = \prod_i p_i^{c_i}$, where the c_i are non-negative integers. Then

   $$\prod_i p_i^{b_i} = n = km = \prod_i p_i^{c_i} \prod_i p_i^{a_i} = \prod_i p_i^{a_i + c_i}.$$

   The uniqueness statement of the fundamental theorem of arithmetic shows that necessarily, $b_i = a_i + c_i$ for all i; in particular $b_i \geqslant a_i$ for all i since the c_i are nonnegative.

   Conversely, if $b_i \geqslant a_i$ for all i, define $c_i = b_i - a_i$ (which is thus nonnegative), and

   $$k = \prod_i p_i^{c_i},$$

   which is an integer since the c_i are nonnegative. The same computation as above shows that $n = km$, which proves that $m \nmid n$.

[1] Actually that won't be necessary, since the primes dividing k also divide $n = km$.

2. Since the prime factorisation of p^v is simply p^v, the previous question shows that $p^v \mid n$ iff. $v \leqslant v_p(n)$, whence the result.

3. We have $m \mid 0$ for all $m \in \mathbb{N}$; in particular $p^v \mid 0$ for all $v \in \mathbb{Z}_{\geqslant 0}$. As a result, there is no largest integer v such that $p^v \mid 0$, but this also explains the convention $v_p(0) = +\infty$.

4. Suppose first that $m, n \neq 0$. We can write the prime factorisation of m as $p^v \times$ powers of other primes, where $v = v_p(m)$ by definition; similarly $n = p^{v_p(n)} \times$ powers of other primes. Then

   $$mn = p^{v_p(m)} \times \text{ powers of other primes} p^{v_p(n)} \times \text{ powers of other primes} = p^{v_p(m)+v_p(n)} \times \text{ powers}$$

   which shows that $v_p(mn) = v_p(m) + v_p(n)$.

   If now exactly one of m and n, say m, is 0, then $mn = 0$, so the identity to prove becomes

   $$+\infty = +\infty + v_p(n),$$

   which holds if we make the convention that $+\infty + v = +\infty$ for all $v \in \mathbb{Z}$, which is reasonable.

   Finally, in the case $m = n = 0$, the identity still holds provided that we agree that $+\infty + +\infty = +\infty$, which is also reasonable.

5. Suppose first that $m, n \neq 0$, and let $v = \min(v_p(m), v_p(n))$. Then $v \leqslant v_p(m)$, so $p^v \mid m$ by question 2.; similarly $p^v \mid n$. Therefore $p^v \mid (m + n)$, whence $v \leqslant v_p(m + n)$ again by question 2.

   If now exactly one of m and n, say m, is 0, then we have

   $$v_p(m + n) = v_p(n) = \min(v_p(m), v_p(n))$$

   under the reasonable convention that $\min(+\infty, v) = v$ for all $v \in \mathbb{Z}$.

   Finally, if $m = n = 0$, we still have

   $$v_p(m + n) \geqslant \min(v_p(m), v_p(n))$$

   if we make the reasonable convention that $\min(+\infty, +\infty) = +\infty$.

6. Without loss of generality, we may assume that $v_p(m) > v_p(n)$. By question 2., this implies $p^{v_p(n)+1} \mid m$. Therefore, if we have $p^{v_p(n)+1} \mid (m + n)$, we would have that $p^{v_p(n)+1} \mid ((m + n) - m) = n$, contradicting question 2. about $v_p(n)$. Therefore $v_p(m + n) \leqslant v_p(n)$. But by the previous question, we also have $v_p(m + n) \geqslant \min(v_p(m), v_p(n)) = v_p(n)$, whence the result.

7. The previous question shows that this can happen only when $v_p(m) = v_p(n)$. We can take for instance $p = 3$, $m = 6$, $n = 12$, so that $m + n = 18$ and

   $$v_3(m + n) = 2 > \min(v_3(m), v_3(n)) = 1.$$

Exercise 8 *$\sqrt{n}$ 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 8

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.

Exercise 9 *Divisors*

1. Factor 2020 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 2020, and the sum of these divisors.

3. Do the same computations with 6000 instead of 2020.

Solution 9

1. Obviously, $2020 = 20 \times 101 = 2^2 \times 5 \times 101$. 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, so $2020 = 2^2 \times 5^1 \times 101^1$ is the full factorisation.

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

   $$\sigma_0(2020) = (1+2)\times(1+1)\times(1+1) = 12,$$

   and that

   $$\sigma_1(2020) = \frac{2^3-1}{2-1}\times\frac{5^2-1}{5-1}\times\frac{101^1-1}{101-1} = 7\times(5+1)\times(101+1) = 4284.$$

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 10 *Divisors again*

1. Find all integers $M \in \mathbb{N}$ of the form $3^a 5^b$ such that the sum of the positive divisors of M is 33883.

   Hint: $33883 = 31\times 1093$, *and both factors are prime.*

2. Find all integers $L \in \mathbb{N}$ of the form $2^a 3^b$ such that the **product** of the divisors of L is 12^{15}.

   Hint: What are the divisors of L? Can you arrange them in a 2-dimensional array? Count the number of 2's, and deduce that the 2-adic valuation the product of all these divisors is $(b+1)(1+2+3+\cdots+a)$. *What about the 3-adic valuation?*

Solution 10

1. Clearly, finding M is equivalent to finding a and b. So we are looking for integers $a, b \geq 0$ such that

   $$(1+3+\cdots+3^a)(1+5+\cdots+5^b) = 31\times 1093.$$

   Since 13 and 1093 are prime, either one of the factors is 31 and the other is 1093, or one is 1 and the other is 33883.

   By trying the values $b = 0, 1, \cdots, 7$ (or better, by using $1+5+\cdots+5^b = (5^{b+1}-1)/4$ to find b), we see that 33883 is not of the form $1+5+\cdots+5^b$, and similarly we see that 33883 is not of the form $1+3+\cdots+3^a$ either.

   So we must have either $1+3+\cdots+3^a = 31$ and $1+5+\cdots+5^b = 1093$, or the other way round. In the first case, we find again no solution; in the second case, we find the unique solution $a = 6$, $b = 2$.

   As a conclusion, the only solution is $M = 3^6 5^2$.

2. Again, we have to find a and b. The divisors of L are the $2^x 3^y$ for $0 \leq x \leq a$ and $0 \leq y \leq b$. Let us multiply all of them, by order of increasing x.

   - For $x = 0$, we are multiplying the $b+1$ divisors $1, 3, \cdots, 3^b$; these contribute no power of 2.
   - For $x = 1$, we are multiplying the $b+1$ divisors $2, 2 \cdot 3, \cdots, 2 \cdot 3^b$; each contributes one factor 2, so in total they contribute $b+1$ factors 2.
   - For $x = 2$, we are multiplying the divisors $2^2, 2^2 \cdot 3, \cdots, 2^2 \cdot 3^b$; each contributes two factors 2, so in total they contribute $2(b+1)$ factors 2.
   - $\vdots$
   - For $x = a$, we are multiplying the $b+1$ divisors divisors $2^a, 2^a \cdot 3, \cdots, 2^a \cdot 3^b$; each contributes a factors 2, so in total they contribute $a(b+1)$ factors 2.

   So in total we have $0 + (b+1) + 2(b+1) + \cdots + a(b+1) = (b+1)(1+2+\cdots+a)$ factors 2.

   Similarly, in total we have $(a+1)(1+2+\cdots+b)$ factors 3, so the product of the divisors of L is
$$2^{(b+1)(1+2+\cdots+a)} 3^{(a+1)(1+2+\cdots+b)}.$$

   We want this to be $12^{15} = 2^{30} 3^{15}$, so by unicity of the factorization we must solve the system
$$\left\{ \begin{array}{l} (b+1)(1+2+\cdots+a) = 30, \\ (a+1)(1+2+\cdots+b) = 15. \end{array} \right.$$

   Since $15 = 3 \cdot 5$ and 3 and 5 are prime, the second equation tells us that $a+1$ is either 1, 3, 5, or 15. Let us examine these cases separately.

   - If $a+1 = 1$, then $a = 0$ and $1+2+\cdots+b = 15$, so $b = 5$, but then $(b+1)(1+2+\cdots+a) = 6 \neq 30$, so this does not work.
   - If $a+1 = 3$, then $1+2+\cdots+b = 5$, but there is no such b.
   - If $a+1 = 5$, then $a = 4$ and $1+2+\cdots+b = 3$, so $b = 2$, and then indeed $(b+1)(1+2+\cdots+a) = 30$, so we have a solution.
   - Finally, If $a+1 = 15$, then $a = 14$; but then $(b+1)(1+2+\cdots+a)$ will obviously be much more than 30, so this does no work either.

   As a conclusion, the only such L is $L = 2^4 3^2$.

Exercise 11 *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 11

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 12 *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. Let $q \in \mathbb{N}$. Prove that if $2^q - 1$ is prime, then q is also prime.

   Hint: $x^m - 1 = (x - 1)(x^{m-1} + x^{m-2} + \cdots + x + 1)$.

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

Solution 12

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 Gauss'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 distinct 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. Suppose q is composite. Then we can write $q = kl$ with $k, l > 1$ integers. But then
$$2^q - 1 = (2^k)^l - 1 = (2^k - 1)(2^{k(l-1)} + 2^{k(l-2)} + \cdots + 2^k + 1).$$
Since k and l are > 1, non of the factors of the RHS can be 1, so we have a genuine factorisation of $2^q - 1$, which is thus composite. By contraposition, if $2^q - 1$ is prime, then so is q.

8. 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. By the previous question, we know that we can restrict our search to values of a such that $a+1$ is prime. 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 $a = 4$, 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 $2^q - 1$ are called Mersenne primes *after Marin Mersenne (French, 17th century). Not all numbers of the form $2^q - 1$ with q prime are prime, as the counter-example $2^{11} - 1 = 23 \times 89$ shows. In fact, as of today, only 49 primes q such that $2^q - 1$ 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!*

Exercise 13 *Ideals of $\mathbb{Z}$*

In this exercise, we define an *ideal* of $\mathbb{Z}$ to be a subset $I \subseteq \mathbb{Z}$ such that

- I is not empty,
- whenever $i \in I$ and $j \in J$, we also have $i + j \in I$,
- whenever $x \in \mathbb{Z}$ and $i \in I$, we also have $xi \in I$.

1. Let $n \in \mathbb{Z}$. Prove that $n\mathbb{Z} = \{nx,\ x \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$.
2. For which $m, n \in \mathbb{Z}$ do we have $m\mathbb{Z} = n\mathbb{Z}$?
3. Let $I \subset \mathbb{Z}$ be an ideal. Prove that whenever $i \in I$ and $j \in J$, we also have $-i \in I$, $i - j \in I$, and $0 \in I$.
4. Let $I \subset \mathbb{Z}$ be an ideal. Prove that there exists $n \in \mathbb{Z}$ such that $I = n\mathbb{Z}$.

   Hint: If $I \neq \{0\}$, let n be the smallest positive element of I, and consider the Euclidean division of the elements of i by n.
5. Prove that if I and J are ideals of $\mathbb{Z}$, then
   $$I + J = \{i + j \mid i \in I, j \in J\}$$
   is also an ideal of $\mathbb{Z}$.

   Hint: $i + j + i' + j' = i + i' + j + j'$.
6. Let now $a, b \in \mathbb{Z}$. By the previous question, $a\mathbb{Z} + b\mathbb{Z}$ is an ideal, so it is of the form $c\mathbb{Z}$ for some $c \in \mathbb{Z}$. Express c in terms of a and b.

   Hint: If you are lost, write an English sentence describing the set $a\mathbb{Z} + b\mathbb{Z}$.

7. Prove that if I and J are ideals of $\mathbb{Z}$, then so is their intersection $I \cap J$.

8. Let now $a, b \in \mathbb{Z}$. By the previous question, $a\mathbb{Z} \cap b\mathbb{Z}$ is an ideal, so it is of the form $c\mathbb{Z}$ for some $c \in \mathbb{Z}$. Express c in terms of a and b.

Solution 13

1. We have to check that $n\mathbb{Z}$ has the 3 properties required to be an ideal.

   - We have $0 = 0n \in n\mathbb{Z}$, so $n\mathbb{Z}$ is not empty.
   - Let $i, j \in n\mathbb{Z}$. By definition of $n\mathbb{Z}$, we have $i = nx$, $j = ny$ for some integers $x, y \in \mathbb{Z}$. Then $i + j = nx + ny = n(x + y) \in n\mathbb{Z}$ since $x + y \in \mathbb{Z}$.
   - Finally, let $x \in \mathbb{Z}$ and $i \in \mathbb{Z}$. Again we have $i = ny$ for some $y \in \mathbb{Z}$; then $xn = xny = n(xy) \in n\mathbb{Z}$ since $xy \in \mathbb{Z}$.

2. By definition $n = n1 \in n\mathbb{Z}$. So if $m\mathbb{Z} = n\mathbb{Z}$, we have $m \in m\mathbb{Z} = n\mathbb{Z}$, so $m = nx$ for some $x \in \mathbb{Z}$. Similarly, $n = my$ for some $y \in \mathbb{Z}$. Thus $m = nx = myx$, so $m(1 - xy) = 0$. If $m = 0$, then $m\mathbb{Z} = 0\mathbb{Z} = \{0x,\ x \in \mathbb{Z}\} = \{0\} \ni n$ so $n = 0$ as well. If $m \neq 0$, then $xy = 1$; as $x, y \in \mathbb{Z}$, this forces $x = y = \pm 1$, whence $n = \pm m$; conversely it is clear that if $m = \pm n$, then $m\mathbb{Z} = n\mathbb{Z}$. So in conclusion, $m\mathbb{Z} = n\mathbb{Z}$ iff. $m = \pm n$.

3. As $i \in I$, we have $(-1)i \in I$ since $-1 \in \mathbb{Z}$; similarly $-j \in I$. Thus $i - j = i + (-j) \in I$. Finally, since $I \neq \emptyset$, we can find $i \in$, and then $0 = i - i \in I$.

4. If $I = \{0\}$, we have $I = 0\mathbb{Z}$. Suppose now that $I \neq \{0\}$. Since $I \neq \emptyset$, we can find a nonzero $i \in I$. As $-i \in I$ as well by the previous question, we can suppose that $i > 0$. Thus
$$\{i \in I \mid i > 0\}$$
is a non-empty subset of $\mathbb{N}$, so it has a smallest element. Call this element n. Then $n \in I$, so $nx \in I$ for all $x \in \mathbb{Z}$ since I is an ideal; thus $n\mathbb{Z} \subseteq I$.

   We now prove that actually $I = n\mathbb{Z}$. Let $i \in I$. As $n \neq 0$, we may consider the Euclidean division of i by n: $i = nq + r$, where $q, r \in \mathbb{Z}$, $0 \leqslant r < n$. Then $nq \in I$ since $n \in I$, so $r = i - nq \in I$ as well. But since $0 \leqslant r < n$,and since $n = \min\{i \in I \mid i > 0\}$, we necessarily have $r = 0$; thus $i = nq + 0 = nq \in n\mathbb{Z}$. Since i was arbitrary, this proves that $I \subseteq n\mathbb{Z}$, whence finally $I = n\mathbb{Z}$.

5. We have to check that $I + J$ has the 3 properties required to be an ideal.

   - Since I and J are ideals, they are not empty, so we can find $i \in I$ and $j \in J$. Then $i + j \in I + J$, so $I + J$ is not empty.
   - Let $x, y \in I + J$. By definition of $I + J$, we can write $x = i + j$ and $y = i' + j'$, with $i, i' \in I$ and $j, j' \in J$. Then $x + y = i + j + i' + j' = (i + i') + (j + j') \in I + J$ since $i + i' \in I$ (because I is an ideal) and $j + j' \in J$ (because J is an ideal).
   - Finally, let $x \in I + J$ and $y \in \mathbb{Z}$. Again, we have $x = i + j$ with $i \in I$ and $j \in J$, and then $yx = yi + yj \in I + J$ since $yi \in I$ (because I is an ideal) and $yj \in J$ (because J is an ideal).

6. $a\mathbb{Z}$ is the set of numbers of the form ax ($x \in \mathbb{Z}$), and $b\mathbb{Z}$ is the set of numbers of the form by ($y \in \mathbb{Z}$), so $a\mathbb{Z} + b\mathbb{Z}$ is the set of numbers of the form $ax + by$, and Bézout tells us that these numbers are exactly the multiples of $\gcd(a, b)$. So we have
$$a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z},$$
and this identity is exactly (the strong version of) Bézout's theorem.

7. We have to check that $I \cap J$ has the 3 properties required to be an ideal.

   - Since I and J are ideals, they contain 0 by question 3., so $0 \in I \cap J$, which is thus nonempty.
   - Let $i, j \in I \cap J$. Then $i, j \in I$, so $i + j \in I$ as I in an ideal; similarly, $i, j \in J$, so $i + j \in J$. Thus $i + j \in I \cap J$.
   - Finally, let $i \in I \cap J$ and $x \in \mathbb{Z}$. Then $i \in I$ so $xi \in I$ as I is an ideal; similarly $i \in J$ so $xi \in J$ because J i an ideal. Thus $xi \in I \cap J$.

8. $a\mathbb{Z}$ is the set of multiples of a, and $b\mathbb{Z}$ is the set of multiples of b, so $a\mathbb{Z} \cap b\mathbb{Z}$ is the set of common multiples of a and b. We have seen in class that these are precisely the multiples of $\operatorname{lcm}(a, b)$, so
$$a\mathbb{Z} \cap b\mathbb{Z} = \operatorname{lcm}(a, b)\mathbb{Z}.$$