Math 261 — Exercise sheet 2

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

Version: September 27, 2018

Answers are due for Wednesday 26 September, 11AM.

The use of calculators is allowed.

Exercise 2.1: $ax + by$ (20 pts)

1. (10 pts) When $I, J \subset \mathbb{Z}$ are two subsets of $\mathbb{Z}$, we denote by

$$I + J = \{i + j \mid i \in I, j \in J\}$$

the set of integers that can be written as the sum of an element of I and of an element of J.

Prove that if I and J are ideals of $\mathbb{Z}$, then $I + J$ is also an ideal of $\mathbb{Z}$.

Hint: $i + j + i' + j' = i + i' + j + j'$.

2. (10 pts) Let now $a, b \in \mathbb{N}$. By the previous question, $a\mathbb{Z} + b\mathbb{Z}$ is an ideal, so it is of the form $c\mathbb{Z}$ for some $c \in \mathbb{N}$. Express c in terms of a and b. What is the name of the theorem that we thus recover?

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

Solution 2.1:

1. 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 $n \in \mathbb{Z}$. Again, we have $x = i + j$ with $i \in I$ and $j \in J$, and then $nx = ni + nj \in I + J$ since $ni \in I$ (because I is an ideal) and $nj \in J$ (because J is an ideal).

2. $a\mathbb{Z}$ 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.

Exercise 2.2: Min-max (40 pts)

Let $a, b \in \mathbb{N}$. We may write

$$a = \prod_{i=1}^{r} p_i^{v_i}, \quad b = \prod_{i=1}^{r} p_i^{w_i}$$

with the same (pairwise distinct) primes p_i, by allowing $v_i, w_i \geq 0$.

1. (10 pts) Express $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ in terms of the p_i, v_i, and w_i.
2. (10 pts) Let v, w be two numbers. Prove carefully that $\min(v, w) + \max(v, w) = v + w$ (including the case $v = w$).
3. (10 pts) Deduce from the previous questions a proof of the formula

$$\gcd(a, b) \operatorname{lcm}(a, b) = ab.$$

4. (10 pts) Find $\operatorname{lcm}(543, 210)$ (you may use results from last week's exercise sheet).

Solution 2.2:

1. Let $g = \gcd(a, b)$. We know that $v_p(g) = \min\big(v_p(a), v_p(b)\big)$ for all p, which is $\min(v_i, w_i)$ if p is one of the p_i, and 0 else. Since we also know that g is a positive number, we can conclude that

$$\gcd(a, b) = + \prod_{p \text{ prime}} p^{v_p(g)} = \prod_{i=1}^{r} p_i^{\min(v_i, w_i)}.$$

   Similarly, we find that

$$\operatorname{lcm}(a, b) = + \prod_{p \text{ prime}} p^{v_p(g)} = \prod_{i=1}^{r} p_i^{\max(v_i, w_i)}.$$

2. Let us define $m = \min(v, w)$ and $M = \max(v, w)$. We distinguish 3 cases:
   - If $v < w$, then $m = v$, $M = w$, so $m + M = v + w$.
   - If $v > w$, then $m = w$, $M = v$, so again $m + M = v + w$.
   - Finally, if $v = w$, then $m = M = v = w$, so again $m + M = v + w$.

   Either way, we have $m + M = v + w$.

3. We have

$$\begin{aligned}
\gcd(a, b) \operatorname{lcm}(a, b) &= \left(\prod_{i=1}^{r} p_i^{\min(v_i, w_i)}\right) \left(\prod_{i=1}^{r} p_i^{\max(v_i, w_i)}\right) \\
&= \prod_{i=1}^{r} p_i^{\min(v_i, w_i) + \max(v_i, w_i)} \\
&= \prod_{i=1}^{r} p_i^{v_i + w_i} \text{ by the previous question} \\
&= \left(\prod_{i=1}^{r} p_i^{v_i}\right) \left(\prod_{i=1}^{r} p_i^{w_i}\right) = ab.
\end{aligned}$$

Exercise 2.3: Divisors (40 pts)

The three questions of this exercise are independent of each other. The last one is difficult.

1. (15 pts) Let $N = 1200$. Find the number of positive divisors of N, the sum of these divisors, and the sum of the squares of these divisors.

2. (20 pts) Find an integer M 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.*

3. (5 pts) Find an integer L 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 2.3:

1. The factorization of N is $N = 2^4 3^1 5^2$, so

   - $\sigma_0(N) = (1+4)(1+1)(1+2) = 30$,
   - $\sigma_1(N) = (1+2+2^2+2^3+2^4)(1+3)(1+5+5^2) = 3844$,
   - and $\sigma_2(N) = (1+2^2+2^4+2^6+2^8)(1+3^2)(1+5^2+5^4) = 2219910$.

2. (20 pts) 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 $M = 3^6 5^2$.

3. 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

$$\begin{cases} (b+1)(1+2+\cdots+a) = 30, \\ (a+1)(1+2+\cdots+b) = 15. \end{cases}$$

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 $L = 2^4 3^2$.

The exercise below has been added for practice. It is not mandatory, and not worth any points. The solution will be made available with the solutions to the other exercises.

Exercise 2.4: $\sqrt{n}$ 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 2.4:

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.