University of Toronto – MAT246H1-S – LEC0201/9201

Concepts in Abstract Mathematics

Problem Set n°4

Jean-Baptiste Campesato

Due on March 28th, 2021

You can only use the material covered in class up to lecture 17 (i.e. up to Chapter 6, §4).
Write your solutions concisely but without skipping important steps.
Make sure that your submission is readable on Crowdmark.

Exercise 1.
Prove that $\forall a, b \in \mathbb{N} \setminus \{0\},\ \varphi(ab)\varphi(\gcd(a,b)) = \varphi(a)\varphi(b)\gcd(a,b)$.

Make sure to explain each step.

Exercise 2.
Alice posted her RSA public key on her website: $(n, e) = (4559, 17)$.

1. Eve wants to spy on Alice: help her to find a suitable private key (n, d).
2. Eve intercepts the ciphered message $c = 2741$ that Bob sent to Alice. What is the original message?

You may use a computer to compute modular exponentiations, nonetheless, you need to explain your steps.
You can use the list of prime numbers less than 100 *given in the lecture notes.*

Exercise 3.

1. Let $x \in \mathbb{R}$. Compute $\lim\limits_{n\to+\infty} \dfrac{\sum_{k=1}^{n} \lfloor kx \rfloor}{n^2}$.
2. Use the above question to prove that any real number is the limit of a sequence of rational numbers.

For this question, you can use results about sequences from your first year calculus course.

Exercise 4.
Let $A, B \subset \mathbb{R}$ be such that $\inf(A)$ and $\sup(B)$ exist.

1. Prove that if $\inf(A) = \sup(B)$ then $A \cap B$ contains at most one element.
2. Under the assumption that $\inf(A) = \sup(B)$, is it possible for $A \cap B$ to be empty?
   You need to justify your answer.

Sample solution to Exercise 1.

Method 1:

Let $a, b \in \mathbb{N} \setminus \{0\}$. Write the prime factorization of $\gcd(a, b)$ as

$$\gcd(a, b) = \prod_{i=1}^{r} p_i^{\delta_i}$$

where $r \in \mathbb{N}$, the p_i are pairwise distinct prime numbers and $\delta_i \in \mathbb{N} \setminus \{0\}$. We set $r = 0$ when $\gcd(a, b) = 1$.
Since $\gcd(a, b)|a$, we may write

$$a = \prod_{i=1}^{r} p_i^{\delta_i+\gamma_i} \prod_{j=1}^{s} q_j^{\alpha_j}$$

where $s \in \mathbb{N}$, the q_j are prime numbers such that the p_i, q_j are pairwise distinct, $\gamma_i \in \mathbb{N}$ and $\alpha_j \in \mathbb{N} \setminus \{0\}$. We allow $s = 0$, with the convention that the product is then equal to 1.
Since $\gcd(a, b)|b$, we may write

$$b = \prod_{i=1}^{r} p_i^{\delta_i+\tilde{\gamma}_i} \prod_{k=1}^{t} m_k^{\beta_k}$$

where $t \in \mathbb{N}$, the m_k are prime numbers such that the p_i, m_k are pairwise distinct, $\tilde{\gamma}_i \in \mathbb{N}$ and $\beta_k \in \mathbb{N} \setminus \{0\}$. We allow $t = 0$, with the convention that the product is then equal to 1.
Note that $\{q_1, \dots, q_s\} \cap \{m_1, \dots, m_t\} = \varnothing$ since otherwise a common prime number would divide $\gcd(a, b)$.
Then the prime factorization of ab is

$$ab = \prod_{i=1}^{r} p_i^{\delta_i+\gamma_i+\tilde{\gamma}_i} \prod_{j=1}^{s} q_j^{\alpha_j} \prod_{k=1}^{t} m_k^{\beta_k}$$

where the p_i, q_j, m_k are pairwise distinct prime numbers.
As seen in class, we have

$$\varphi(\gcd(a, b)) = \gcd(a, b) \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

$$\varphi(a) = a \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \prod_{j=1}^{s} \left(1 - \frac{1}{q_j}\right)$$

$$\varphi(b) = b \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \prod_{k=1}^{t} \left(1 - \frac{1}{m_k}\right)$$

$$\varphi(ab) = ab \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \prod_{j=1}^{s} \left(1 - \frac{1}{q_j}\right) \prod_{k=1}^{t} \left(1 - \frac{1}{m_k}\right)$$

Therefore

$$\begin{aligned}
\varphi(ab)\varphi(\gcd(a, b)) &= ab \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \prod_{j=1}^{s} \left(1 - \frac{1}{q_j}\right) \prod_{k=1}^{t} \left(1 - \frac{1}{m_k}\right) \gcd(a, b) \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \\
&= \left(a \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \prod_{j=1}^{s} \left(1 - \frac{1}{q_j}\right) \right) \left(b \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \prod_{k=1}^{t} \left(1 - \frac{1}{m_k}\right) \right) \gcd(a, b) \\
&= \varphi(a)\varphi(b) \gcd(a, b)
\end{aligned}$$

Method 2:
Let $a, b \in \mathbb{N} \setminus \{0\}$. Given a prime divisor p of ab, by Euclid's lemma, exactly one of the following occurs:

- Either p divides a but not b,
- Or p divides b but not a,
- Or p divides both a and b, i.e. $p | \gcd(a, b)$.

According to the lecture notes,

$$\varphi(ab) = ab \prod_{\substack{p \text{ prime,} \\ p|ab}} \left(1 - \frac{1}{p}\right)$$

$$\varphi(a) = a \prod_{\substack{p \text{ prime,} \\ p|a}} \left(1 - \frac{1}{p}\right)$$

$$\varphi(b) = b \prod_{\substack{p \text{ prime,} \\ p|b}} \left(1 - \frac{1}{p}\right)$$

$$\varphi(\gcd(a, b)) = \gcd(a, b) \prod_{\substack{p \text{ prime,} \\ p|a \text{ and } p|b}} \left(1 - \frac{1}{p}\right)$$

Therefore

$$\begin{aligned}
\varphi(ab) &= ab \prod_{\substack{p \text{ prime,} \\ p|ab}} \left(1 - \frac{1}{p}\right) \\
&= ab \prod_{\substack{p \text{ prime,} \\ p|a \text{ and } p\nmid b}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \text{ prime,} \\ p\nmid a \text{ and } p|b}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \text{ prime,} \\ p|a \text{ and } p|b}} \left(1 - \frac{1}{p}\right) \\
&= \frac{\left(a \prod_{\substack{p \text{ prime,} \\ p|a \text{ and } p\nmid b}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \text{ prime,} \\ p|a \text{ and } p|b}} \left(1 - \frac{1}{p}\right)\right)\left(b \prod_{\substack{p \text{ prime,} \\ p\nmid a \text{ and } p|b}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \text{ prime,} \\ p|a \text{ and } p|b}} \left(1 - \frac{1}{p}\right)\right)}{\prod_{\substack{p \text{ prime,} \\ p|a \text{ and } p|b}} \left(1 - \frac{1}{p}\right)} \\
&= \frac{\left(a \prod_{\substack{p \text{ prime,} \\ p|a}} \left(1 - \frac{1}{p}\right)\right)\left(b \prod_{\substack{p \text{ prime,} \\ p|b}} \left(1 - \frac{1}{p}\right)\right)}{\prod_{\substack{p \text{ prime,} \\ p|a \text{ and } p|b}} \left(1 - \frac{1}{p}\right)} \\
&= \gcd(a, b) \frac{\varphi(a)\varphi(b)}{\varphi(\gcd(a, b))}
\end{aligned}$$

Sample solution to Exercise 2.

1. Note that $n = 4559 = 47 \times 97$ where 47 and 97 are prime numbers (see Example 3 of Chapter 3).
   Therefore $\varphi(n) = (47-1)(97-1) = 46 \times 96 = 4416$.
   Let's find a Bézout's identity for $\varphi(n) = 4416$ and $e = 17$:

$$\begin{aligned} 4416 &= 17 \times 259 + 13 \\ 17 &= 13 \times 1 + 4 \\ 13 &= 4 \times 3 + 1 \end{aligned}$$

   Therefore

$$1 = 13-4\times3 = 13-(17-13)\times3 = 17\times(-3)+13\times4 = 17\times(-3)+(4416-17\times259)\times4 = 17\times(-1039)+4416\times4$$

   Thus, if we set $d = -1039 + 4416 = 3377$ then $d > 0$ and $ed \equiv 1 \pmod{\varphi(n)}$:

$$ed = 17 \times (-1039 + 4416) \equiv 17 \times (-1039) + 4416 \times 4 \pmod{4416} \equiv 1 \pmod{4416}$$

   Thus $(n, d) = (4459, 3377)$ is a suitable private key.

2. $c^e = 2741^{3377} \equiv 2718 \pmod{4559}$, then $m = 2718$ is the original message since $m \in \{0, 1, \dots, 4558\}$.

Sample solution to Exercise 3.

1. Since $\forall k \in \mathbb{N},\ \lfloor kx \rfloor \leq kx < \lfloor kx \rfloor + 1$, we get

$$\frac{\sum_{k=1}^{n} \lfloor kx \rfloor}{n^2} \leq \frac{\sum_{k=1}^{n} kx}{n^2} = x\frac{n(n+1)}{2n^2} = x\frac{n+1}{2n}$$

   and

$$\frac{\sum_{k=1}^{n} \lfloor kx \rfloor}{n^2} > \frac{\sum_{k=1}^{n} (kx-1)}{n^2} = x\frac{n+1}{2n} - \frac{1}{n}$$

   Therefore

$$x\frac{n+1}{2n} - \frac{1}{n} < \frac{\sum_{k=1}^{n} \lfloor kx \rfloor}{n^2} \leq x\frac{n+1}{2n}$$

   Since $\lim\limits_{n\to+\infty} x\frac{n+1}{2n} - \frac{1}{n} = \lim\limits_{n\to+\infty} x\frac{n+1}{2n} = \frac{x}{2}$, we get from the Squeeze Theorem that

$$\lim_{n\to+\infty} \frac{\sum_{k=1}^{n} \lfloor kx \rfloor}{n^2} = \frac{x}{2}$$

2. Let $x \in \mathbb{R}$. For $n \in \mathbb{N} \setminus \{0\}$, set $u_n = 2\frac{\sum_{k=1}^{n} \lfloor kx \rfloor}{n^2}$.
   Then $\forall n \in \mathbb{N} \setminus \{0\}$, $u_n \in \mathbb{Q}$ and $x = \lim\limits_{n\to+\infty} u_n$ from the previous question.

Sample solution to Exercise 4.

1. Let $A, B \subset \mathbb{R}$ be such that $\inf(A)$ and $\sup(B)$ exist.
   We are going to prove the contrapositive: if $A \cap B$ contains at least two elements then $\inf(A) \neq \sup(B)$.
   Assume that there exist $x, y \in A \cap B$ such that $x < y$.
   Then, since $\sup(B)$ is an upper bound of B and $y \in B$, we have $y \leq \sup(B)$.
   Since $\inf(A)$ is a lower bound of A and $x \in A$, we have $\inf(A) \leq x$.
   Therefore $\inf(A) \leq x < y \leq \sup(B)$, so $\inf(A) \neq \sup(B)$.

2. Let $A = (0, 42)$ and $B = (-\pi, 0)$. Then $\inf(A) = \sup(B) = 0$ and $A \cap B = \emptyset$.