Aurélien SAGNIER asagnie1@jhu.edu Dept.of Mathematics, John Hopkins University

Problem set 3 - Arithmetics

DUE : 27^{th} SEPTEMBER 2019

Remark 0.1. You should consider the results of 1.1, 1.2, 1.3, 1.5, 1.6, 3.2, 3.4 as results seen in class and therefore must learn them.

Definition 0.2. We say that a number $p \in \mathbb{N}\backslash\{0;1\}$ is a prime number if p is divisible only by ± 1 and $\pm p$. We denote $\mathbb{P}$ the set of prime numbers.

Exercise 1. *Around prime numbers*

1. *(Gauss' lemma)* Let $a, b, c \in \mathbb{Z}$ such that $a|(bc)$ and $a \wedge b = 1$. Prove that $a|c$.
   (*Hint :* use Bezout theorem).

2. *(Euclid's lemma)* Let $p \in \mathbb{P}$ and $a, b \in \mathbb{Z}$, prove that $[p|(ab)] \Rightarrow [(p|a) \vee (p|b)]$.

3. *(Euclid's theorem)* Prove that $\mathbb{P}$ is infinite.
   (*Hint :* assume by absurd that $\mathbb{P}$ is finite of cardinal $r \in \mathbb{N}^\star$ and consider $N = 1 + \prod_{i=1}^{r} p_i$)

4. *(very weak form of Dirichlet's theorem)* Let us denote $\mathbb{P}_{3,4}$ the set of elements of $\mathbb{P}$ congruent to 3 modulo 4. Show that $\mathbb{P}_{3,4}$ is infinite.
   (*Hint :*assume by absurd that $\mathbb{P}_{3,4}$ is finite of cardinal $r \in \mathbb{N}^\star$ and consider $N = -1 + 4\prod_{i=1}^{r} p_i$)

5. *(Fundamental theorem of arithmetics)* Let $a \in \mathbb{Z}\backslash\{0,1\}$, prove that there exists an unique $d \in \mathbb{N}^\star$, an unique $(p_1, \dots, p_d) \in \mathbb{P}^d$ and an unique $(n_1, \dots, n_d) \in (\mathbb{N}^\star)^d$ such that $a = \mathrm{sgn}(a)\prod_{i=1}^{d} p_i^{n_i}$ where $\mathrm{sgn}(a) = \frac{a}{|a|}$.
   (*Hint :* do the existence part with strong induction on $|a|$, use Euclid's lemma for the uniqueness part)

6. For $(a, b) \in (\mathbb{Z}\backslash\{0\})^2$, we call the least common multiple of a and b (and denote it $a \vee b$) the smallest positive integer such that $a|(a \vee b)$ and $b|(a \vee b)$. Show that $a \vee b$ always exists. Then show that it is always possible to write $a = \mathrm{sgn}(a)\prod_{i=1}^{d} p_i^{n_i(a)}$ and $b = \mathrm{sgn}(b)\prod_{i=1}^{d} p_i^{n_i(b)}$ with $d \in \mathbb{N}^\star$, $(n_1(a), \dots, n_d(a)) \in \mathbb{N}^d$ and $(n_1(b), \dots, n_d(b)) \in \mathbb{N}^d$. Finally show that $a \vee b = \prod_{i=1}^{d} p_i^{\max(n_i(a), n_i(b))}$ and that $a \wedge b = \prod_{i=1}^{d} p_i^{\min(n_i(a), n_i(b))}$.

Exercise 2. *Pirates and arithmetics*
A group of 17 pirates has recently stolen a chest of gold pieces from a spanish gallion. They decide to share those gold pieces equally among them and give the rest to the cook accompanying them on their boat. In this configuration the cook would then receive 3 gold pieces. However before this sharing is made, the pirates have a party to celebrate their newly aquired treasure. Some pirates drink too much during this party, they start to quarrel and 6 pirates are killed during this dispute. The remaining pirates decide to share equally among them the treasure of spanish gallion and still give the remainder to the cook. In this new situation, the cook would get 4 pieces. However the captain of the pirates is still drunk from the party and doesn't see the reefs. As a result the pirate ship sinks before the pirates were able to share the spanish treasure. In the end only 6 pirates, the cook and the treasure are safe and land on an unknown island. The remaining pirates decide to share the reasure equally among them and give the remaining gold pieces to the cook. Now the cook would get 5 pieces. Find the minimal number of gold pieces the chest was containing in the first place and so how much the cook will get when he decides to poison the remaining pirates.
(*Hint :* the cook has taken a class on the Chinese remainder theorem)

Exercise 3. *RSA cryptosystem*

1. Let $p \in \mathbb{P}$, show that $\forall k \in [\![1, p-1]\!], p | \binom{p}{k}$, where $\binom{p}{k} = \frac{p!}{k!(p-k)!}$.

2. *(Frobenius)* Show that $\forall p \in \mathbb{P}, \forall (a,b) \in \mathbb{N}^2, (a+b)^p \equiv a^p + b^p \,(p)$.

3. Show that $\forall p \in \mathbb{P}, \forall a \in \mathbb{N}, a^p \equiv a (p)$. (*Hint :* for fixed $p \in \mathbb{P}$, do an induction on a)

4. *(Fermat's little theorem)* Show that $\forall p \in \mathbb{P}, \forall a \in \mathbb{N}, ((a \not\equiv 0\,(p)) \Rightarrow (a^{p-1} \equiv 1\,(p)))$.
(*Hint :* use Bezout theorem on a and p)

5. Romeo wants to send love messages to Juliet but desires that only Juliet would be able to read those messages. To achieve this, Romeo and Juliet ask their friends Ron Rivest, Adi Shamir and Leonard Adleman from MIT to help them. Here is Rivest, Shamir, Adleman advice :

   - Juliet should choose two distinct "big" prime numbers p and q.
   - Juliet should then choose an integer e coprime with $(p-1)(q-1)$.
   - Juliet should then find an positive integer d such that $de \equiv 1\,[(p-1)(q-1)]$.
   - Juliet should keep her choice of p, q, d secret and make public the couple (n, e). This couple of integers is called Juliet's *public key*.
   - Romeo, who wants to send his message in the form of an integer m modulo n, computes the value $M := m^e\,(n)$ and sends this M to Juliet.
   - Juliet gets the integer M from Romeo and computes M^d modulo n and so recovers m.

   Show that this method (RSA) works, in other words that $M^d \equiv m\,(n)$ where $M \equiv m^e\,(n)$.
   (*Hint :* you may first prove that $m^{ed} \equiv m\,(p)$ and then $m^{ed} \equiv m\,(q)$ and use Chinese remainder theorem to conclude)
   Remark : what makes this method secret is the fact when p and q are "big" prime numbers with $n = pq$, it is very hard (in practise) to find back those p and q when you just know n. This method was invented by Ron Rivest, Adi Shamir and Leonard Adleman in 1977.

6. *Application* Juliet chooses $p = 3$, $q = 11$ and $e = 7$.

   (a) Find which integer between 1 and 10 Juliet can choose for d.

   (b) Romeo wants to send the message "love you" to Juliet. He encodes every letter by its number in the alphabet and the space by 0 (so l by 12, o by 15, v by 22, e by 5, y by 25, u by 21). And sends a message to Juliet for each character (letter or space). Compute the series of messages Romeo sends to Juliet.
   Bonus question : at the time of Juliet and Romeo, no machine could assist you in computations (one of the first machines, the "Pascaline", was invented by Blaise Pascal around 1645). Try to figure out how to compute by hand the messages Romeo has to send (*Hint :* There is something better than brute force that you could try. The computations would still take some time but would be faster than brute force by hand, try to look at what happens for the letter l).

   (c) Juliet receives the messages of Romeo. Compute how Juliet decodes the series of messages sent by Romeo.