UNIVERSITY OF CRETE
DEPARTMENT OF MATHEMATICS AND APPLIED MATHEMATICS
NUMBER THEORY - MEM204 (SPRING SEMESTER 2019-20)
LECTURER: G. KAPETANAKIS

1st exercise set - Answers

Exercise 1. Without using induction, show that for every n, $2 \mid n(n+1)$ and that $6 \mid n(n+1)(n+2)$.

Answer. We have the following cases:

- If n is even, then $2 \mid n \Rightarrow 2 \mid n(n+1)$.
- If n is odd, then $2 \mid n+1 \Rightarrow 2 \mid n(n+1)$.

So, for every $n \in \mathbb{Z}$, $2 \mid n(n+1)$.

The above also implies that $2 \mid n(n+1)(n+2)$, for every $n \in \mathbb{Z}$. Now, take the following cases:

- If n is of the form $n = 3k$, then $3 \mid n \Rightarrow 3 \mid n(n+1)(n+2)$.
- If n is of the form $n = 3k+1$, then $3 \mid n+2 \Rightarrow 3 \mid n(n+1)(n+2)$.
- If n is of the form $n = 3k+2$, then $3 \mid n+1 \Rightarrow 3 \mid n(n+1)(n+2)$.

So, for every $n \in \mathbb{Z}$, $3 \mid n(n+1)(n+2)$. The latter combined with the fact that $2 \mid n(n+1)(n+2)$ yields that, for every $n \in \mathbb{Z}$, $6 \mid n(n+1)(n+2)$. $\square$

Exercise 2. Show that for every $n \in \mathbb{Z}_{\geq 0}$, $7 \mid 3^{2n+1} + 2^{n+2}$.

Answer. We will use induction on n.

- The result is clear when $n = 0$.
- Assume that $7 \mid 3^{2k+1} + 2^{k+2}$, for some $k \geq 0$. This implies
$$3^{2k+1} = 7\ell - 2^{2k+2}, \tag{1}$$
for some $\ell \in \mathbb{Z}$.
- Then:
$$\begin{aligned} 3^{2(k+1)+1} + 2^{(k+1)+2} &= 9 \cdot 3^{2k+1} + 2 \cdot 2^{2k+2} \\ &\overset{(1)}{=} 9(7\ell - 2^{2k+2}) + 2 \cdot 2^{2k+2} \\ &= 7(9\ell - 2^{2k+2}). \end{aligned}$$
$\square$

Exercise 3. Show that for every $n \in \mathbb{Z}_{\geq 1}$, $15 \mid 2^{4n} - 1$.

Answer. We have that
$$2^{4n} - 1 = (2^4)^n - 1 = (2^4 - 1)((2^4)^{n-1} + (2^4)^{n-2} + \cdots + 1) = 15(2^{4n-4} + \cdots + 1).$$

The result follows. $\square$

Exercise 4. Show that for every $\lambda, a_1, \ldots, a_n \in \mathbb{Z}$,

1. $[\lambda a_1, \ldots, \lambda a_n] = |\lambda|[a_1, \ldots, a_n]$ and
2. if $[a_1, \ldots, a_n] = m$, then $\left(\frac{m}{a_1}, \ldots, \frac{m}{a_n}\right) = 1$.

Answer. 1. W.l.o.g. assume that $\lambda > 0$. Now, set $e := [a_1, \ldots, a_n]$ and $m := [\lambda a_1, \ldots, \lambda a_n]$. We have that $\forall i,\ a_i \mid e \Rightarrow \forall i,\ \lambda a_i \mid \lambda e \Rightarrow \underline{m \mid \lambda e}$. Conversely, $\forall i,\ \lambda a_i \mid m \Rightarrow \forall i$, $a_i \mid \frac{m}{\lambda} \Rightarrow e \mid \frac{m}{\lambda} \Rightarrow \underline{\lambda e \mid m}$. We conclude that $\lambda e = m$.

2. Set $d := \left(\frac{m}{a_1}, \ldots, \frac{m}{a_n}\right)$. We have that, $\forall i,\ d \mid \frac{m}{a_i} \Rightarrow \forall i,\ da_i \mid m \Rightarrow [da_1, \ldots, da_n] \mid m$. However, from the previous item, $[da_1, \ldots, da_n] = dm$, so the above relation becomes $dm \mid m \Rightarrow d \mid 1 \Rightarrow d = 1$. ☐

Exercise 5. Find all the integers $a \neq 3$ such that $a - 3 \mid a^3 - 3$.

Answer. Let p be a prime divisor of $a - 3$. We have that

$$p \mid a - 3 \overset{a-3 \mid a^3-3}{\Longrightarrow} p \mid a^3 - 3 \overset{p \mid a-3}{\Longrightarrow} p \mid a^3 - a = a(a-1)(a+1) \overset{p \in \mathbb{P}}{\Longrightarrow} p \mid a \text{ or } p \mid a \pm 1.$$

We take the following cases:

- $p \mid a \overset{p \mid a-3}{\Longrightarrow} p \mid 3 \overset{p \in \mathbb{P}}{\Longrightarrow} p = 3$.
- $p \mid a \pm 1 \overset{p \mid a-3}{\Longrightarrow} p \mid 2 \text{ or } 4 \overset{p \in \mathbb{P}}{\Longrightarrow} p = 2$.

In other words, the only primes that may divide $a - 3$ are 2 and 3, i.e.,

$$a - 3 = \pm 2^\kappa 3^\lambda \iff a = 3 \pm 2^\kappa 3^\lambda, \tag{2}$$

for some $\kappa, \lambda \geq 0$. It follows that

$$\begin{aligned} a^3 - 3 &= 3^3 \pm 3 \cdot 3^2 2^\kappa 3^\lambda + 3 \cdot 3 \cdot 2^{2\kappa} 3^{2\lambda} \pm 2^{3\kappa} 3^{3\lambda} - 3 \\ &= 24 \pm 2^\kappa 3^{\lambda+3} + 2^{2\kappa} 3^{2\lambda+2} \pm 2^{3\kappa} 3^{3\lambda}. \end{aligned}$$

It is clear that $2^\kappa 3^\lambda$ divides the LHS of the above, as well as the last three terms of the RHS, so it also divides the first term. In other words,

$$2^\kappa 3^\lambda \mid 24 = 2^3 3.$$

It follows that $0 \leq \kappa \leq 3$ and $0 \leq \lambda \leq 1$. In accordance with (2), we conclude that

$$a = 3 \pm 2^\kappa 3^\lambda,$$

where $0 \leq \kappa \leq 3$ and $0 \leq \lambda \leq 1$ (16 numbers in total). ☐

Exercise 6. Find all the integers a such that both 624 and 301 leave a remainder of 16 when divided by a.

Answer. We have that

$$\left.\begin{array}{l} a \mid 624-16=608 \\ a \mid 301-16=285 \end{array}\right\} \Rightarrow a \mid (608,285)=19 \Rightarrow a=1 \text{ or } 19.$$

Since a division with 1 always leaves remainder 0, we conclude that $a=19$. □

Exercise 7. If $n>1$, show that n^4+4 is composite.

Answer. We have that

$$n^4+4=n^4+4n^2+4-4n^2=(n^2+2)^2-(2n)^2=(n^2-2n+2)(n^2+2n+2).$$

Since $n>1$, both of the factors above are non-trivial, thus we have a non-trivial factorization of n^4+4. □

Exercise 8. Without using Dirichlet's theorem, show that there are infinitely many primes of the forms $4k+3$ and $6\ell+5$.

Answer. Assume that there is only a finite number of such primes. Let

$$3, p_1, \dots, p_n$$

be these primes (i.e. $p_1=7$). Now, take the number

$$A := 4p_1 \cdots p_n + 3.$$

Clearly A is of the form $4k+3$. However, $A \neq 3$ and $A > p_i$ for all i, that is A is not a prime. Now, since A is even, 2 does not appear in the prime factorization of A. Also, $3 \nmid A$, since that would imply $3 \mid 4p_1 \cdots p_n$, a contradiction. Moreover, it is easy to check that the product of two numbers of the form $4k+1$ is another number of the form $4k+1$. It follows that A has at least one prime factor of the form $4k+3$, i.e., $p_i \mid A$ for some i.

Now, we have:

$$p_i \mid A = 4p_1 \cdots p_n + 3 \overset{p_i \mid 4p_1 \cdots p_n}{\Longrightarrow} p_i \mid 3 \overset{p_i \in \mathbb{P}}{\Longrightarrow} p_i = 3,$$

a contradiction.

The question regarding $6\ell+5$ is similar. □

Exercise 9. Find all $a, b \in \mathbb{Z}_{>0}$, such that $ab=480$ and $[a,b]=240$.

Answer. We have that $480=2^5 \cdot 3 \cdot 5$ and $240=2^4 \cdot 3 \cdot 5$. It follows that

$$a=2^{a_2}3^{a_3}5^{a_5} \text{ and } b=2^{b_2}3^{b_3}5^{b_5},$$

where $a_i, b_i \geq 0$, such that

$$\begin{aligned} a_2+b_2=5 \quad &, \quad \max(a_2,b_2)=4, \\ a_3+b_3=1 \quad &, \quad \max(a_3,b_3)=1, \\ a_5+b_5=1 \quad &, \quad \max(a_5,b_5)=1. \end{aligned}$$

It follows that $\{a_2,b_2\}=\{1,4\}$, $\{a_3,b_3\}=\{0,1\}$ and $\{a_5,b_5\}=\{0,1\}$. We conclude that we have 8 choices for the pair a, b. □

Exercise 10. Let $a = a_m \cdots a_0$ be the decimal expression a, i.e., $a = \sum_{i=0}^{m} 10^i a_i$. Show that:

(a) $2 \mid a \iff 2 \mid a_0$.
(b) $3 \mid a \iff 3 \mid \sum_{i=0}^{n} a_i$.
(c) $4 \mid a \iff 4 \mid 10a_1 + a_0$.
(d) $5 \mid a \iff 5 \mid a_0$.
(e) $7 \mid a \iff 7 \mid 2a_0 - \frac{a-a_0}{10}$.
(f) $9 \mid a \iff 9 \mid \sum_{i=0}^{n} a_i$.
(g) $11 \mid a \iff 11 \mid \sum_{i=0}^{n}(-1)^i a_i$.
(h) $25 \mid a \iff 25 \mid 10a_1 + a_0$.

Answer. (a) We have that $a = \sum_{i=0}^{m} 10^i a_i = a_0 + 2 \cdot 5 \cdot \sum_{i=1}^{n} a_i 10^{i-1}$. It follows that $2 \mid a \iff 2 \mid a_0$. Item (d) is similar.

(b) First, we will inductively prove that $10^i = 3k_i + 1$, for some k_i. The result is trivial for $i = 0$. Assume that $10^j = 3k_j + 1$. Then $10^{j+1} = 10 \cdot 10^j = 10(3k_j + 1) = 3(10k_j + 3) + 1$. This assures our claim. Now, we have that

$$a = \sum_{i=0}^{m} 10^i a_i = \sum_{i=0}^{m} (3k_i + 1)a_i = 3\left(\sum_{i=0}^{n} k_i a_i\right) + \sum_{i=0}^{n} a_i.$$

The latter implies $3 \mid a \iff 3 \mid \sum_{i=0}^{n} a_i$. Item (f) is similar.

(c) We have that $a = \sum_{i=0}^{m} 10^i a_i = a_0 + 10a_1 + 4 \cdot 25 \cdot \sum_{i=2}^{n} a_i 10^{i-2}$. It follows that $4 \mid a \iff 4 \mid a_0 + 10a_1$. Item (h) is similar.

(e) First notice that $a - a_0 = 10\left(\sum_{i=1}^{n} a_i 10^{i-1}\right)$, that is, $\frac{a-a_0}{10}$ is an integer, i.e., $2a_0 - \frac{a-a_0}{10}$ is an integer. Furthermore, note that

$$2a_0 - \frac{a - a_0}{10} = \frac{21a_0 - a}{10}.$$

It follows that

$$7 \mid 2a_0 - \frac{a - a_0}{10} \iff 7 \mid \frac{21a_0 - a}{10} \overset{(7,10)=1}{\iff} 7 \mid 21a_0 - a \overset{7|21}{\iff} 7 \mid a.$$

(g) First, we will inductively prove that $10^i = 11\ell_i + (-1)^i$, for some ℓ_i. The result is trivial for $i = 0$. Assume that $10^j = 11\ell_j + (-1)^j$. Then $10^{j+1} = 10 \cdot 10^j = (11 - 1)(11\ell_j + (-1)^j) = 11(11\ell_j + (-1)^j - \ell_j) + (-1)^{j+1}$. This assures our claim. Now, we have that

$$a = \sum_{i=0}^{m} 10^i a_i = \sum_{i=0}^{m} (11\ell_i + (-1)^i)a_i = 11\left(\sum_{i=0}^{n} \ell_i a_i\right) + \sum_{i=0}^{n} (-1)^i a_i.$$

The latter implies $11 \mid a \iff 11 \mid \sum_{i=0}^{n}(-1)^i a_i$. $\square$

Exercise 11. Find all $x \in \mathbb{Q}$, such that $A = 3x^2 - 5x \in \mathbb{Z}$.

Answer. Clearly, if $x \in \mathbb{Z}$, then $A \in \mathbb{Z}$. Now, assume that $x \notin \mathbb{Z}$. Then w.l.o.g., we may assume that $x = \frac{a}{b}$, where $(a, b) = 1$ and $b > 1$. Now, we get that $A = \frac{a(3a-5b)}{b^2} \in \mathbb{Z}$. It follows that

$$b^2 \mid a(3a - 5b) \Rightarrow b \mid a(3a - 5b) \overset{(a,b)=1}{\Rightarrow} b \mid 3a - 5b \overset{b|5b}{\Rightarrow} b \mid 3a \overset{(a,b)=1}{\Rightarrow} b \mid 3 \overset{b>1}{\Rightarrow} b = 3.$$

It remains to check for which values of a, with $(a,3)=1$, $x=\frac{a}{3}$, yields $A\in\mathbb{Z}$. In particular, we have $A=3x^2-5x=\frac{a(a-5)}{3}$, that is (since $(a,3)=1$, a must satisfy $3\mid a-5$, that is $a=3k+2$ for some k.

All in all, $A\in\mathbb{Z}\iff x\in\mathbb{Z}$ or $x=k+\frac{2}{3}$, for some $k\in\mathbb{Z}$. □

Exercise 12. Show that if 2^n-1 is a prime, then n is a prime.

Answer. Suppose that n is not a prime, that is, $n=st$, for some $s,t>1$. Then $2^n-1=2^{st}-1=(2^s-1)((2^s)^{t-1}+\cdots+1)$, where both factors are >1, a contradiction. □

Exercise 13. The *Fibonacci sequence* $1,1,2,3,\ldots$ is defined recursively as $a_{n+1}=a_n+a_{n-1}$, for $n\geq 2$, and $a_1=a_2=1$. Show that $(a_n,a_{n+1})=1$ for every $n\geq 1$

Answer. First, we prove that for any a,b, we have that

$$(a+b,a)=(a,b). \tag{3}$$

Set $d_1=(a+b,a)$ and $d_2=(a,b)$. Now, note that $d_1\mid a+b\overset{d_1|a}{\Rightarrow}d_1\mid b\overset{d_1|a}{\Rightarrow}\underline{d_1\mid d_2}$. Additionally, we have that $d_2\mid b\overset{d_2|a}{\Rightarrow}d_2\mid a+b\overset{d_2|a}{\Rightarrow}\underline{d_2\mid d_1}$. It follows that $d_1=d_2$ this concludes the proof of our claim.

Now, we will prove that $(a_n,a_{n+1})=1$, using induction on n.

- The result is trivial for $n=1$ and $n=2$.
- Assume that $(a_k,a_{k+1})=1$ for some $k\geq 2$ (I.H.).
- We have that $(a_{k+1},a_{k+2})=(a_{k+1},a_k+a_{k+1})\overset{(3)}{=}(a_{k+1},a_k)\overset{\text{I.H.}}{=}1$. □

Exercise 14. Suppose that $a,b>1$ and $(a,b)=1$. Then:

1. There exists some $x,y>0$ such that $ax-by=1$.
2. If $x^a=y^b$, then $x=n^b$ and $y=n^a$ for some n.
3. For every $n>ab$, there exist some $x,y>0$ such that $n=ax+by$.
4. There are no $x,y>0$ such that $ab=ax+by$.

Answer.

1. Since $(a,b)=1$, there exist some x',y', such that $ax'+by'=1$. Next, notice that $x',y'\neq 0$, since that would imply $a\mid 1$ or $b\mid 1$. Moreover, notice that, since $a,b>1$, exactly one of x',y' is positive and the other is negative. If $x'>0$ and $y'<0$ the result is immediate, so we only need to focus on the case $x'<0$ and $y'>0$.

   So, assume that $x'<0$ and $y'>0$ and for any $n>0$, set $x_n=x'+bn$ and $y_n=y'-an$. For every $n\in\mathbb{Z}$, we have that

   $$ax_n+by_n=a(x'+bn)+b(y'-an)=ax'+by'=1.$$

   Also, note that $\lim_{n\to\infty}x_n=\infty$ and $\lim_{n\to\infty}y_n=-\infty$, that is, there exists some m, such that $x:=x_m>0$ and $y:=y_m<0$. The desired result follows.

2. From item 1, there exist some $k, \ell > 0$, such that
$$ak - b\ell = 1. \tag{4}$$
We have that
$$x^a = y^b \Rightarrow x^{a\ell} = y^{b\ell} \overset{(4)}{\Rightarrow} x^{a\ell} = y^{ak-1} \Rightarrow y^{1/a} = \frac{y^k}{x^\ell} \in \mathbb{Q}.$$
However, we know[1] that a rational power of an integer is either an integer or an irrational number. This means that $y^{1/a} = n$, for some $n \in \mathbb{Z}$. It follows that $\underline{y = n^a}$. Also, we have that
$$x^a = y^b \Rightarrow x^a = n^{ab} \Rightarrow \underline{x = n^b}.$$

3. Fix some $n > ab$. Set
$$S := \{n - ib \;:\; 1 \le i \le a\}.$$
We claim that any two distinct elements of S, leave a different remainder, when divided by a. In order to prove that, assume that there exist some $1 \le i < j \le a$, such that $n - ib = k_i a + r$ and $n - jb = k_j a + r$. It follows that $a \mid b(j-i) \overset{(a,b)=1}{\Rightarrow} a \mid j - i$, impossible, since $0 < j - i < a$. Our claim is now proven.

   The above combined with the fact that $|S| = a$, yields that the set S includes elements that leave every possible remainder when divided by a, including one that leaves remainder zero, i.e., is divided by a. In other words, there exists some k, such that $k = n - yb$, for some $1 \le y \le a$ and $k = ax$, for some $x \le 1$. The result follows.

4. Let $x, y > 0$ be such that
$$ab = ax + by. \tag{5}$$
We have that $a \mid ab$ and $a \mid ax$, so (5) implies that $a \mid by \overset{(a,b)=1}{\Longrightarrow} a \mid y \Rightarrow y = ay'$. In a similar way, one obtains $x = bx'$. Now, (5) becomes
$$ab = ab(x' + y'),$$
which is impossible. □

Exercise 15. If $a > 1$, then $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

Answer. If $m = n$ the result is clear, so we focus on the case $m \ne n$ and w.l.o.g. we may further assume that $m > n$.

Now, if $m = qn + r$ is the Euclidean division of m and n, we have that
$$\begin{aligned} a^m - 1 &= a^{qn+r} - 1 \\ &= a^r(a^{qn} - 1) + (a^r - 1) \\ &= \underbrace{a^r(a^{q-1} + a^{q-2} + \cdots + 1)}_{A}(a^n - 1) + (a^r - 1) \\ &= A(a^n - 1) + (a^r - 1), \end{aligned}$$

[1]If you don't know that, prove it!

where in the last equation, we note that clearly, $0 \leq a^r - 1 < a^n - 1$. In other words $a^r - 1$ is the remainder of the Euclidean division between $a^m - 1$ and $a^n - 1$. This implies that the Euclidean division between $a^m - 1$ and $a^n - 1$ is dictated by the corresponding Euclidean division between m and n. It follows that the Euclidean algorithm will follow the same steps in both cases and that the last non-trivial remainder (i.e. the gcd) of the Euclidean algorithm for $a^m - 1$ and $a^n - 1$ will be $a^{(m,n)} - 1$. $\square$