**Math 4707 Fall 2017 (Darij Grinberg): homework set 3 [corrected 23 Oct 2017]**

due date: Wednesday 25 Oct 2017 at the beginning of class, or before that by email or moodle

Please solve **at most 4** of the 7 exercises!

Two integers $a$ and $b$ are said to be *coprime* if their greatest common divisor is 1. (Note that $\gcd(a,0) = |a|$ for any integer $a$.)

The *Euler totient function* $\phi : \{1,2,3,\ldots\} \to \mathbb{N}$ is defined by

$$\begin{aligned}\phi(n) &= (\text{the number of all } m \in [n] \text{ that are coprime to } n) \\ &= |\{m \in [n] \mid m \text{ is coprime to } n\}|.\end{aligned}$$

More about greatest common divisors and about this function can be found in Lehman/Leighton/Meyer (Chapter 9). That said, you won't need anything but the definitions in this homework set.

**Exercise 1.** Let $n$ be a positive integer.

**(a)** Prove that if $m$ is an integer coprime to $n$, then $n - m$ is also an integer coprime to $n$.

**(b)** Prove that $\phi(n)$ is even if $n > 2$.

[**Hint:** If you haven't used the $n > 2$ requirement, then you must have missed something. $\phi(2) = 1$, which is not even!]

**Exercise 2.** A preprint recently posted on the arXiv says (in a proof) that "

$$1 - \sum_{i=2}^{d} (i-1) \binom{d}{i} \left(\frac{1}{d-1}\right)^i = 0,$$

the final equality being verified by the computer algebra system Maple (which itself employs an algorithm of Zeilberger)". Here, $d$ is assumed to be an integer $\geq 2$.

Prove this equality by hand (but feel free to use a computer to write up your proof...). More generally, find and prove a sum-less expression for

$$\sum_{i=2}^{d} (i-1) \binom{d}{i} q^i$$

where $q$ is an arbitrary rational number (and $d$ is still an integer $\geq 2$).

**Exercise 3.** Let $n \in \mathbb{N}$. Consider $n$ people standing in a circle. Each of them looks down at someone else's feet (i.e., at the feet of one of the other $n-1$ persons). A bell sounds, and every person (simultaneously) looks up at the eyes of the person whose feet they have been ogling. If two people make eye contact, they scream. Show that the probability that no one screams is

$$\sum_{k=0}^{n} (-1)^k \frac{n(n-1)\cdots(n-2k+1)}{(n-1)^{2k} \cdot 2^k \cdot k!}.$$

Combinatorial restatement (feel free to solve this instead): A pair $(i,j)$ of elements of $[n]$ is said to *scream* at a map $f : [n] \to [n]$ if it satisfies $f(i) = j$ and $f(j) = i$. A map $f : [n] \to [n]$ is *silent* if no pair $(i,j) \in [n] \times [n]$ screams at $f$. Prove that the number of all silent maps $f : [n] \to [n]$ is

$$\sum_{k=0}^{n} (-1)^k \frac{n(n-1)\cdots(n-2k+1)}{2^k \cdot k!} (n-1)^{n-2k}.$$

**Exercise 4.** Let $i$ and $j$ be positive integers. Prove that

$$\sum_{k=\max\{i,j\}}^{i+j} (-1)^k \frac{(k-1)!}{(k-i)!\,(k-j)!\,(i+j-k)!} = 0.$$

[**Hint:** Assume that $i \geq j$, and rewrite $\dfrac{(k-1)!}{(k-i)!\,(k-j)!\,(i+j-k)!}$ as a constant (independent of $k$) times a product of two binomial coefficients, one of which is $\dbinom{i}{k-j}$.]

**Exercise 5.** Let $N \in \mathbb{N}$. Let $(a_0, a_1, \ldots, a_N)$ be a list of rational numbers. Define a second list $(b_0, b_1, \ldots, b_N)$ of rational numbers by setting

$$b_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} a_i \qquad \text{for each } n \in \{0,1,\ldots,N\}.$$

Prove that

$$a_n = \sum_{i=0}^{n} (-1)^i \binom{n}{i} b_i \qquad \text{for each } n \in \{0,1,\ldots,N\}.$$

Now, recall some of the notations for finite differences:

Per se, the words "map", "mapping", "function", "transformation" and "operator" are synonyms in mathematics (they all mean assignments of values from one set to the elements of another set). But it is common to use some of these words selectively for certain kinds of maps. We shall follow the following rules:

- The word "map" can mean any kind of map.
- The word "function" shall mean a map from $\mathbb{Q}$ to $\mathbb{Q}$. Thus, the set of all functions is $\mathbb{Q}^{\mathbb{Q}}$.
- The word "operator" shall mean a map from $\mathbb{Q}^{\mathbb{Q}}$ to $\mathbb{Q}^{\mathbb{Q}}$. Thus, an operator is a map sending functions to functions.

For example, the map

$$\mathbb{Q} \to \mathbb{Q}, \qquad x \mapsto x^2$$

is a function, whereas the map

$$\mathbb{Q}^{\mathbb{Q}} \to \mathbb{Q}^{\mathbb{Q}}, \qquad f \mapsto f \circ f$$

("apply a function twice") is an operator.

If $f$ and $g$ are functions, then $f+g$ denotes the pointwise sum of $f$ and $g$ (that is, the function $\mathbb{Q} \to \mathbb{Q}$, $x \mapsto f(x) + g(x)$), and $fg$ denotes the pointwise product of $f$ and $g$ (that is, the function $\mathbb{Q} \to \mathbb{Q}$, $x \mapsto f(x)\, g(x)$). We can also write $f \cdot g$ for $fg$.

If $f$ is a function and $\lambda \in \mathbb{Q}$, then $\lambda f$ denotes the pointwise product of $\lambda$ with $f$ (that is, the function $\mathbb{Q} \to \mathbb{Q}$, $x \mapsto \lambda f(x)$). Thus, the functions form a $\mathbb{Q}$-vector space (and better yet, a commutative $\mathbb{Q}$-algebra, because of the multiplication).

The following three operators are particularly important:

- The identity operator $\mathrm{id} : \mathbb{Q}^{\mathbb{Q}} \to \mathbb{Q}^{\mathbb{Q}}$. It sends each function $f$ to $f$ itself.
- The shift operator $S : \mathbb{Q}^{\mathbb{Q}} \to \mathbb{Q}^{\mathbb{Q}}$. It sends each function $f$ to the function $S(f)$ defined by $(S(f))(x) = f(x+1)$ for all $x \in \mathbb{Q}$. Speaking in terms of function plots, the operator $S$ shifts a function by 1 to the left.
- The difference operator $\Delta : \mathbb{Q}^{\mathbb{Q}} \to \mathbb{Q}^{\mathbb{Q}}$. It sends each function $f$ to the function $\Delta(f)$ defined by $(\Delta(f))(x) = f(x+1) - f(x)$ for all $x \in \mathbb{Q}$. Speaking in terms of function plots, the operator $\Delta$ shifts a function by 1 to the left and subtracts the original function back from it. Note that $\Delta(f) = S(f) - f$ for each $f \in \mathbb{Q}^{\mathbb{Q}}$.

If our functions were $C^\infty$-functions $\mathbb{R} \to \mathbb{R}$ instead of maps $\mathbb{Q} \to \mathbb{Q}$, then $\dfrac{d}{dx}$ would be another operator (sending each function $f$ to its derivative).

**Exercise 6.** **(a)** Prove that $S(fg) = S(f) \cdot S(g)$ for any two functions $f$ and $g$.
**(b)** Prove that $\Delta(fg) = S(f)\,\Delta(g) + \Delta(f)\,g$ for any two functions $f$ and $g$.
**(c)** Prove that $\Delta(fg) = f\Delta(g) + \Delta(f)\,S(g)$ for any two functions $f$ and $g$.
**(d)** Prove that $\Delta \circ S = S \circ \Delta$.

And finally, let's take our tale of periodic tuples and necklaces to its (temporary) conclusion:[1]

**Exercise 7.** This exercise is a continuation of Exercise 7 on homework set #2 and of Exercise 6 on midterm #1.

Let $p$ be a **prime** number. Let $X$ be a set.

**(a)** Let $\mathbf{x} \in X^p$ be a $p$-tuple. Prove that:

[1] To remind: You are allowed to use the exercises from previous problem sets even if you did not solve them.

- if all entries of $\mathbf{x}$ are equal (that is, if $\mathbf{x}$ has the form $\left(\underbrace{x, x, \ldots, x}_{p \text{ times}}\right)$ for some $x \in X$), then $|[\mathbf{x}]_\sim| = 1$;
- otherwise, we have $|[\mathbf{x}]_\sim| = p$.

[*Example:* If $p = 3$, then the 3-tuple $\mathbf{x} = (5,5,5)$ satisfies $|[\mathbf{x}]_\sim| = 1$, while the 3-tuple $\mathbf{x} = (1,3,1)$ satisfies $|[\mathbf{x}]_\sim| = 3$.]

A $p$-necklace $[\mathbf{x}]_\sim$ is said to be *aperiodic* if $|[\mathbf{x}]_\sim| = p$.

**(b)** Assume that the set $X$ is finite. Prove that the number of all aperiodic $p$-necklaces (over $X$) is $\dfrac{|X|^p - |X|}{p}$.

[*Example:* If $p = 3$ and $X = \{1,2,3\}$, then the aperiodic $p$-necklaces over $X$ are

$$[(1,1,2)]_\sim,\ [(1,1,3)]_\sim,\ [(1,2,2)]_\sim,\ [(1,2,3)]_\sim,$$
$$[(1,3,2)]_\sim,\ [(1,3,3)]_\sim,\ [(2,2,3)]_\sim,\ [(2,3,3)]_\sim.$$

You can, of course, write them differently: e.g., $[(1,2,3)]_\sim$ is also known as $[(2,3,1)]_\sim$ (but $[(1,3,2)]_\sim$ is different). The $p$-necklaces that are not aperiodic are $[(1,1,1)]_\sim$, $[(2,2,2)]_\sim$ and $[(3,3,3)]_\sim$.]

**(c)** Prove *Fermat's Little Theorem*, which states that $p \mid a^p - a$ for every integer $a$. [**Note:** $a$ might be negative.]

**(d)** Assume that the set $X$ is finite. Prove that the number of all $p$-necklaces (over $X$) is $\dfrac{|X|^p + (p-1)\,|X|}{p}$.

We have thus counted $p$-necklaces for a prime number $p$. Counting $n$-necklaces for $n$ composite is harder; we will learn about this later.