Summary on Lecture 10, March 4, 2019

Recursive definitions. There are many mathematical objects which we can define only *recursively*. We start with well-known example:

(1) **Fibonacci numbers** F_n. We define:

(B) $F_0 = 0,\ F_1 = 1$,

(R) $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$.

Here are the first few values of F_n:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
F_n	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610

We prove that $\sum_{i=1}^{n} F_i^2 = F_n F_{n+1}$ by induction. Indeed, it's true if $n = 1$.

Assume $\sum_{i=1}^{k} F_i^2 = F_k F_{k+1}$. Then

$$\sum_{i=1}^{k+1} F_i^2 = \sum_{i=1}^{k} F_i^2 + F_{k+1}^2 F_k F_{k+1} + F_{k+1}^2 = F_{k+1}(F_k + F_{k+1}) = F_{k+1}F_{k+2}.$$

(2) We define a sequence of numbers a_n as:

(B) $a_0 = 0,\ a_1 = 0,\ a_2 = 1$, and

(R) $a_n = a_{n-1} + a_{n-2}$ for $n \geq 3$.

Here are the first few values of a_n:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a_n	0	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377

We notice that $a_n = F_{n-1}$ for $n \geq 3$. We would like to prove that $a_{n+2} \geq (\sqrt{2})^n$ for all $n \geq 2$. Indeed, it's true if $n = 2, 3$. Assume $a_{k+2} \geq (\sqrt{2})^k$ for all $k = 2, 3, \ldots, n$. We should prove that $a_{n+3} \geq (\sqrt{2})^{n+1}$. We have:

$$\begin{aligned} a_{n+3} = a_{n+2} + a_{n+1} &\geq (\sqrt{2})^n + (\sqrt{2})^{n-1} \\ &= (\sqrt{2})^{n-1}(\sqrt{2}+1) \geq (\sqrt{2})^{n-1} \cdot 2 = (\sqrt{2})^{n+1}. \end{aligned}$$

Here we use that $\sqrt{2} + 1 \geq 2$ and $2 = (\sqrt{2})^2$.

(3) We can define recursively the binomial coefficients $\binom{n}{r}$:

(B) $\binom{n}{0} = 1$, $\binom{n}{r} = 0$ if $r < 0$ and $r > n$.

(R) $\binom{n+1}{r} = \binom{n}{r} + \binom{n}{r-1}$.

(4) We define factorial $\texttt{FAC}(n)$:

(B) $\texttt{FAC}(0) = 1$

(R) $\texttt{FAC}(n) = \texttt{FAC}(n-1) \cdot n$ for $n \geq 1$.

(5) We define the Harmonic numbers H_n:

(B) $H_1 = 1$

(R) $H_n = H_{n-1} + \frac{1}{n}$ for $n \geq 2$.

(6) We define the sequence $\texttt{SEC}(n)$:

(B) $\texttt{SEC}(0) = 1$

(R) $\texttt{SEC}(n+1) = \frac{n+1}{\texttt{SEC}(n)}$.

Exercise. Use induction to prove that the sequence $\texttt{SEC}(n)$ is well-defined.

(7) We define the sequence $T(n)$ as follows:

(B) $T(1) = 1$

(R) $T(n) = 2 \cdot T(\lfloor \frac{n}{2} \rfloor)$ for $n \geq 2$.

We compute a couple of values of $T(n)$:

$$\begin{aligned} T(73) &= 2 \cdot T(36) = 2^2 \cdot T(18) = 2^3 \cdot T(9) = 2^4 \cdot T(4) = 2^5 \cdot T(2) = 2^6 \\ T(2019) &= 2 \cdot T(1009) = 2^2 \cdot T(504) = 2^3 \cdot T(252) = 2^4 \cdot T(126) = 2^5 \cdot T(63) \\ &= 2^6 \cdot T(31) = 2^7 \cdot T(15) = 2^8 \cdot T(7) = 2^9 \cdot T(3) = 2^{10} \end{aligned}$$

Exercise. Use induction to prove that $T(n) = \max\{\ 2^k \mid 2^k \leq n\ \}$.

Exercise. Define a sequence $S(n)$ such that $S(n) = \min\{\ 2^k \mid n \leq 2^k\ \}$.

Exercise. Let p be a prime. Define recursively a sequence $T_p(n)$ such that

$$T(n) = \max\{\ p^k \mid p^k \leq n\ \}.$$

Exercise. Let p be a prime. Define recursively a sequence $S_p(n)$ such that

$$S_p(n) = \min\{\ p^k \mid n \leq p^k\ \}.$$

Exercise. Define recursively what does it mean "well-formed formula", see Ex. 17, p. 220.

• **Division algorithm and prime numbers.** Recall that if $m, n \in \mathbf{Z}$, and $n \neq 0$, we say that n *divides* m or m *is divisible by* n iff $m = n \cdot j$, where $j \in \mathbf{Z}$. We can say also that m is a multiple of n. The notation: $n|m$.

Properties:

(1) $1|m$ and $m|0$ for any $m \in \mathbf{Z}$;

(2) $(n|m) \wedge (m|k) \Longrightarrow n|k$;

(3) $(n|m) \wedge (m|n) \Longrightarrow m = \pm n$;

(4) if $m = c_1 m_1 + \cdots c_s m_s$, and $n|m_i$ for all $i = 1, \ldots, s$, then $n|m$.

Exercise. Prove (3), (4).

Recall that p is a prime number if p has no divisors but 1 and itself. We also recall the following fact (see Lecture 5 for the proof):

Lemma 1. *Let $n \in \mathbf{Z}_+$ be not a prime number. Then there exits a prime p such that $p|n$.*

We use Lemma 1 to prove the following remarkable fact:

Theorem 2. *There is infinite number of primes.*

Proof. Assume there exist only finite number of primes. Let $P = \{p_1, p_2, \ldots, p_k\}$ is the set of all prime numbers, $|P| = k$. Consider the integer: $p_{k+1} = p_1 \cdot p_2 \cdots p_k + 1$. The integer p_{k+1} is either pime or not. If p_{k+1} is not a prime, then by Lemma 1 it has to be divisible by some prime p_j, $j = 1, \ldots, k$, but it is not since the remainder will be 1. Thus p_{k+1} is a prime, and $p_{k+1} \in P$. Then $|P| = k + 1$, not $|P| = k$. This two properties cannot hold together. Contradiction. □

• **Division Algorithm.** First we prove the existence result.

Theorem 2. *Let $m, n \in \mathbf{Z}$, and $n \neq 0$. Then there exist unique integers $q \in \mathbf{Z}$ and $r \in \{0, 1, \ldots, n-1\}$ such that $m = n \cdot q + r$.*

Proof. We consider only the case when $m > 0$ and $n > 0$, leaving the remaining cases to you. If $n|m$, then $m = n \cdot q$ for some $q \in \mathbf{Z}$. If $m = n \cdot q'$, then $n \cdot q - n \cdot q' = 0$, or $n(q - q') = 0$, which implies $q = q'$.

Let $n \not| m$ and $n < m$. Then we consider the set

$$S = \{\ m - t \cdot n \mid m - t \cdot n > 0\ \}.$$

We notice that $S \neq \emptyset$ since $m > n$, i.e., $m - 1 \cdot n > 0$. Also, by definition, all elements of S are positive. By the Well-Ordering Principle, there exists a minimal element of S. We denote it by r. We have $m = q \cdot n + r$. We notice that $n > r \geq 0$: indeed, if $r \geq n$, then there is an element $(r - n) = m - (q + 1) \cdot n$ in S. □

Exercise. Prove uniquness of q and r in the case when $m > n > 0$.

• **The Euclidian Algorithm: warm-up.** Recall: let $m, n \in \mathbf{Z}$, and $n \neq 0$. Then there exist unique integers $q \in \mathbf{Z}$ and $r \in \{0, 1, \ldots, n - 1\}$ such that $m = n \cdot q + r$.

We look at the division:

$$m = q \cdot n + r, \quad 0 \leq r < n.$$

The following fact is very important for us: it gives a key to compute $\gcd(m, n)$ for arbitrary integers m and n. Euclid has discovered this property around 2,300 years ago.

Lemma 1. $\gcd(m, n) = \gcd(n, r)$.

Proof. We will show that every common divisor of m and n is also a common divisor of n and r, and that every common divisor of n and r is also a common divisor of m and n.

Indeed, let $d|m$ and $d|n$. Then, since $r = m - q \cdot n$, $d|r$. Thus d is a common divisor of n and r.

Let $d|n$ and $d|r$. Then, since $m = q \cdot n + r$, $d|m$. Thus d is a common divisor of m and n.

Now, since the common divisors of the pairs (m, n) and (n, r) coincide, the greatest common divisor is the same, i.e., $\gcd(m, n) = \gcd(n, r)$. □

Examples. We compute few examples:

$$\begin{aligned}&\gcd(27,5)=\gcd(5,2)=\gcd(2,1)=1\\&\gcd(183,15)=\gcd(15,3)=\gcd(3,0)=3\\&\gcd(2014,323)=\gcd(323,76)=\gcd(76,19)=\gcd(19,0)=19.\end{aligned}$$

We introduce the notations: $(m \ \mathsf{DIV}\ n) := q$, and $(m \ \mathsf{MOD}\ n) := r$. Thus we can write:

$$m = (m \ \mathsf{DIV}\ n)\cdot n + (m \ \mathsf{MOD}\ n).$$

We fix $n > 0$ and then we say that m and m' are equal **mod** n iff $(m - m' \ \mathsf{MOD}\ n) = 0$, i.e. that $m - m'$ is divisible by n.

Example. Let $n = 5$. Then there are only possible remainders are $0,1,2,3,4$. Thus we can put together all integers in 5 different classes:

$$\mathbf{0} := \{0, \pm 5, \pm 2\cdot 5, \ldots\},\quad \mathbf{1} := \{1, 1\pm 5, 1\pm 2\cdot 5, \ldots\},\quad \mathbf{2} := \{2, 2\pm 5, 2\pm 2\cdot 5, \ldots\},$$
$$\mathbf{3} := \{3, 3\pm 5, 3\pm 2\cdot 5, \ldots\},\quad \mathbf{4} := \{4, 4\pm 5, 4\pm 2\cdot 5, \ldots\}.$$

Now we can add the classes: say, let $4 + 5j \in \mathbf{4}$, and $1 + 5i \in \mathbf{1}$. Then

$$4 + 5j + 1 + 5i = 5(1 + i + j) \in \mathbf{0},$$

and we choose different numbers in $\mathbf{4}$ and $\mathbf{1}$, the result will be the same. Thus we have that $\mathbf{4}+\mathbf{1} = \mathbf{0}$. Similarly, we can multiply. Say, let $2 + 5j \in \mathbf{2}$, and $3 + 5i \in \mathbf{3}$. Then

$$(2 + 5j)(3 + 5i) = 6 + 5\cdot 3i + 5\cdot 2j + 5\cdot 5ji = 1 + 5(3i + 2j + 5ji) \in \mathbf{1}.$$

Thus $\mathbf{2}\cdot\mathbf{3} = \mathbf{1}$. Here are the addition and multiplication tables **mod** 5:

+	**0**	**1**	**2**	**3**	**4**
0	**0**	**1**	**2**	**3**	**3**
1	**1**	**2**	**3**	**4**	**0**
2	**2**	**3**	**4**	**0**	**1**
3	**3**	**4**	**0**	**1**	**2**
4	**4**	**0**	**1**	**2**	**3**

×	**0**	**1**	**2**	**3**	**4**
0	**0**	**0**	**0**	**0**	**0**
1	**0**	**1**	**2**	**3**	**4**
2	**0**	**2**	**4**	**1**	**3**
3	**0**	**3**	**1**	**4**	**2**
4	**0**	**4**	**3**	**2**	**1**

Example. Let $n = 6$. Then there are only possible remainders are $0,1,2,3,4,5$. Thus we can put together all integers in 6 different classes:

$$\mathbf{0} := \{0, \pm 6, \pm 2\cdot 6, \ldots\},\quad \mathbf{1} := \{1, 1\pm 6, 1\pm 2\cdot 6, \ldots\},\quad \mathbf{2} := \{2, 2\pm 6, 2\pm 2\cdot 6, \ldots\},$$
$$\mathbf{3} := \{3, 3\pm 6, 3\pm 2\cdot 6, \ldots\},\quad \mathbf{4} := \{4, 4\pm 6, 4\pm 2\cdot 6, \ldots\},\quad \mathbf{5} := \{5, 5\pm 6, 5\pm 2\cdot 6, \ldots\}.$$

Similarly, we can add and multiply. Here are the addition and multiplication tables **mod** 6:

+	**0**	**1**	**2**	**3**	**4**	**5**
0	**0**	**1**	**2**	**3**	**4**	**5**
1	**1**	**2**	**3**	**4**	**5**	**0**
2	**2**	**3**	**4**	**5**	**0**	**1**
3	**3**	**4**	**5**	**0**	**1**	**2**
4	**4**	**5**	**0**	**1**	**2**	**3**
5	**5**	**0**	**1**	**2**	**3**	**4**

×	**0**	**1**	**2**	**3**	**4**	**5**
0	**0**	**0**	**0**	**0**	**0**	**0**
1	**0**	**1**	**2**	**3**	**4**	**5**
2	**0**	**2**	**4**	**0**	**2**	**4**
3	**0**	**3**	**0**	**3**	**0**	**3**
4	**0**	**4**	**2**	**0**	**4**	**2**
5	**0**	**5**	**4**	**3**	**2**	**1**

We notice that $\mathbf{2}\cdot\mathbf{3}=\mathbf{0}$, $\mathbf{4}\cdot\mathbf{3}=\mathbf{0}$, and $\mathbf{3}\cdot\mathbf{3}=\mathbf{3}$.

Exercise. Write the addition and multiplication tables for $n=10$ and $n=11$.

Example. Compute last three digits of the following integer: 2019^{79}.

In other words, we have to compute 2019^{79} **mod** 1000. To warm-up, we compute 2019^{2^k} **mod** 1000 for several values of k:

$$\begin{array}{lllll}
2019^1 & = & 19 & = & 19 \ \mathbf{mod}\ 1000\ , \\
2019^2 & = & 19^2 & = & 361 \ \mathbf{mod}\ 1000\ , \\
2019^{2^2} & = & 361^2 & = & 321 \ \mathbf{mod}\ 1000\ , \\
2019^{2^3} & = & 321^2 & = & 41 \ \mathbf{mod}\ 1000\ , \\
2019^{2^4} & = & 41^2 & = & 681 \ \mathbf{mod}\ 1000\ , \\
2019^{2^5} & = & 681^2 & = & 761 \ \mathbf{mod}\ 1000\ , \\
2019^{2^6} & = & 761^2 & = & 121 \ \mathbf{mod}\ 1000\ .
\end{array}$$

Now we find a binary decomposition of 79: We have: $79=1+2+4+8+64=1+2+2^2+2^3+2^6$. Then we have:

$$\begin{array}{lll}
2019^{79} & = & 2019^1\cdot 2019^2\cdot 2019^{2^2}\cdot 2019^{2^3}\cdot 2019^{2^6} \\
 & = & 19\cdot 361\cdot 321\cdot 41\cdot 121 \qquad \mathbf{mod}\ 1000 \\
 & = & (19\cdot 361)\cdot(321\cdot 41)\cdot 121 \qquad \mathbf{mod}\ 1000 \\
 & = & 859\cdot 161\cdot 121 \qquad \mathbf{mod}\ 1000 \\
 & = & 859\cdot(161\cdot 121) \qquad \mathbf{mod}\ 1000 \\
 & = & 859\cdot 481 \qquad \mathbf{mod}\ 1000 \\
 & = & 179 \qquad \mathbf{mod}\ 1000
\end{array}$$

The answer: $2019^{79}=179$ **mod** 1000.

Exercise. Compute last two digits of the integer 2019^{2019}.