MODULAR ARITHMETICS
(MA2316, THIRD WEEK)

VLADIMIR DOTSENKO

Let us recall some standard results of modular arithmetics for integers. Recall that for a prime number p the ring $\mathbb{Z}/p\mathbb{Z}$ is a field, that is all nonzero residues modulo p are invertible.

Theorem 1 (Fermat's Little Theorem)**.** *Let p be a prime, and let a be an integer coprime to p. Then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. The simplest proof is based on the Lagrange's theorem from group theory: consider the group $G = (\mathbb{Z}/p\mathbb{Z})^{\times}$. Its order is $p-1$, so the order of each element divides $p-1$, so $(a+p\mathbb{Z})^{p-1} = 1+p\mathbb{Z}$, that is $a^{p-1} \equiv 1 \pmod{p}$. □

In fact, this result generalises for composite numbers as follows. Define the *Euler's totient function* $\phi(n)$ to be equal to the number of positive integers that are smaller than or equal to n and coprime to n.

Theorem 2 (Euler's Theorem)**.** *Let n be an integer, and let a be an integer coprime to n. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Proof. Similarly, use the Lagrange's theorem: consider the group $G = (\mathbb{Z}/n\mathbb{Z})^{\times}$. Its order is $\phi(n)$, so the order of each element divides $\phi(n)$, so $(a+n\mathbb{Z})^{\phi(n)} = 1+p\mathbb{Z}$, that is $a^{\phi(n)} \equiv 1 \pmod{p}$. □

Remark. *Let us give a yet another proof of Fermat's Little Theorem which will be useful later on. If we consider all numbers modulo p, we have $\{1, 2, \ldots, p-1\} = \{a, 2a, \ldots, (p-1)a\}$, since $ia \equiv ja \pmod{p}$ only for $i \equiv j \pmod{p}$, so*

$$1 \cdot 2 \cdots (p-1) \equiv a \cdot 2a \cdots (p-1)a \pmod{p},$$

and consequently $1 \equiv a^{p-1} \pmod{p}$.

Let us also remark that another way to formulate Fermat's Little Theorem so that it works for all choices of a is to say that $a^p \equiv a \pmod{p}$. Let us mention here a yet another generalisation of this form of the statement.

Theorem 3. *Let A be a square $n \times n$-matrix with integer entries, and let p be a prime. Then $\mathrm{tr}(A^p) \equiv \mathrm{tr}(A) \pmod{p}$.*

Proof. We may assume that all entries of A are positive, since the result only cares about their values modulo p. We shall interpret the traces combinatorially. Let us consider n distinct points that we label $1, 2, \ldots, n$, and connect them by arrows so that there are a_{ij} arrows directed from the point i to the point j. Then

$$\mathrm{tr}(A^p) = \sum_{j_1, j_2, \ldots, j_p = 1}^{n} a_{j_1 j_2} a_{j_2 j_3} \cdots a_{j_p j_1}$$

counts "closed walks" of length p moving along the arrows, that is the number of ways to pick a point, and walk from it along the arrows, returning back after p steps. A closed walk has an associated closed path, where we forget at which vertex we started. Usually, there are p different ways to reconstruct a closed walk from a closed path, since choosing one of the p points along the

path as the starting point leads to different walks. There is only one situation where it fails, that is for walks that are repetitions of the same "loop" arrow from some vertex i to itself p times. (Indeed, we can view our walk as an infinite p-periodic walk, and if it there are less than p different ways to reconstruct the walk from its associated path, this means that it is periodic with a smaller period, which for prime p implies that it has period 1), Thus the number of all p-periodic walks, that is $\operatorname{tr}(A^p)$, is congruent modulo p to the number of 1-periodic walks, that is $\operatorname{tr}(A)$. □

Theorem 4 (Wilson's Theorem)**.** *Let p be a prime. Then $(p-1)! \equiv -1 \pmod{p}$.*

Proof. We have

$$1 \cdot 2 \cdots (p-1) \equiv 1 \cdot (p-1) \pmod{p},$$

since modulo p the elements that are equal to their inverses are 1 and $-1 = p-1$, and all other elements in the product will cancel with their inverses. □

Theorem 5. *Let p be a prime. Then the group $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.*

Proof. Let us show that if $d \mid (p-1)$, then the congruence $x^d \equiv 1 \pmod{p}$ has d solutions modulo p. Indeed, since $\mathbb{Z}/p\mathbb{Z}$ is a field, this congruence has at most d solutions (a polynomial of degree d over a field has at most d roots), and if their number is less than d, then the polynomial $\frac{x^{p-1}-1}{x^d-1}$ of degree $p-1-d$ would have too many roots (as by Fermat's Little Theorem the polynomial $x^{p-1}-1$ has $p-1$ roots).

Let us denote by $\alpha(d)$ the number of elements of order exactly d in the group $(\mathbb{Z}/p\mathbb{Z})^\times$. Then, our result can be formulated as $\sum_{c|d} \alpha(c) = d$ (since by Lagrange's theorem, the order of an element of a group G divides the number of elements of G). But we also have $\sum_{c|d} \phi(c) = d$, since if we look at fractions $\frac{1}{d}, \frac{2}{d}, \ldots, \frac{d}{d}$, and bring each of them to the lowest terms, exactly $\phi(c)$ of them will have c as a denominator (the numerators will be precisely all integers smaller than or equal to c that are coprime to c). From these two facts, it is easy to see by induction that $\alpha(c) = \phi(c)$ for all $c \mid p-1$. In particular, $\alpha(p-1) = \phi(p-1) \geq 1$ so there exists an element of order $p-1$, and the group is cyclic. □