GROUPS IN NUMBER THEORY AND GEOMETRY

VERA SERGANOVA

Euler function.

For every positive integer n let $\varphi(n)$ be the number of positive integers less than n and relatively prime with n. For instance, $\varphi(6) = 2$. The function φ is called the Euler function.

We use the notation (m, n) for the greatest common divisor of m and n. Also recall that $a \cong b(\operatorname{mod} n)$ if n divides $a - b$.

1. Fermat–Euler theorem. If $(a, n) = 1$, then $a^{\varphi(n)} \cong 1(\operatorname{mod} n)$.

2. If $(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.

3. Use the previous problem to prove Euler's product formula

$$\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p}),$$

here the product is taken over all prime p that divide n.

4. Find $\varphi(2013)$.

5. Consider all complex roots of the equation $x^n = 1$. A root ε is called primitive if every other n-th root of 1 is a power of ε. Show that the number of primitive roots equals $\varphi(n)$.

6. Another Euler's formula

$$\sum_{d|n} \varphi(d) = n.$$

7. Let ε be a primitive n-th root of 1. Prove that

$$\varphi(n) = \sum_{k=1}^{n} (k, n)\varepsilon^k.$$

That, in particular, implies the formula

$$\varphi(n) = \sum_{k=1}^{n} (k, n) \cos \frac{2\pi k}{n}.$$

8. If $\varphi(n)$ is a power of 2 then $n = 2^k p_1 \dots p_s$, where $p_1, \dots, p_s$ are distinct Fermat's primes (odd primes of the form $2^a + 1$).

9. If $2^a + 1$ is prime then a is a power of 2. Find first few Fermat's primes.

10. If $2^a - 1$ is prime then a itself is prime.

11. Is $2^{13} - 1$ prime?

12. If p is a prime number that divides $2^q + 1$, then $2q$ divides $p - 1$.

Date: April 2, 2013.

13. A function $f(n)$ defined on the set of positive integers is called multiplicative if $f(nm) = f(n)f(m)$ for relatively prime m and n. Show that if $f(n)$ is multiplicative, then

$$g(n) = \sum_{d|n} f(d)$$

is also multiplicative.

14. The Moebius function $\mu(n)$ is defined uniquely by the properties $\mu(1) = 1$ and for all $n > 1$

$$\sum_{d|n} \mu(d) = 0.$$

Check that μ is multiplicative and find the formula for $\mu(n)$ in terms of prime factorization of n.

15. If $f(n)$ and $g(n)$ are related as in Problem 12, then

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

16. MacMahon's formula. Suppose you have beads of r colors. Let $N(n,r)$ denote the number of necklaces one can make from those beads with total number of beads equal to n. (Two necklaces are the same if one can cut each in one place to obtain identical strings.)

$$N(n,r) = \frac{1}{n} \sum_{d|n} \varphi(d) r^{\frac{n}{d}}.$$

Groups.

A set G with operation of multiplication is called a group if the following three conditions hold

(1) $a(bc) = (ab)c$ for any a, b, c in G;
(2) there is an element 1 such that $1a = a1 = a$ for any a in G;
(3) For every a in G there exists b such that $ab = ba = 1$.

A group is called Abelian if the multiplication is commutative, i.e. $ab = ba$ for all a, b in G.

If a group G is finite we denote by $|G|$ the number of elements in G.

17. Check that the following are groups

(a) The set C_n of all complex roots of $x^n = 1$ with operation of multiplication.

(b) The set S_n of all permutations of $\{1, \dots, n\}$ with operation $(ss')(i) = s(s'(i))$.

(c) The set of rigid motions (transformations which preserve distances) of the plane with operation of composition.

Which of the above groups are Abelian?

18. A subset H of G which is a group with the same operation of multiplication is called a subgroup. Find all subgroups of C_n.

19. Lagrange's theorem. If H is a subgroup of a finite group G, then $|H|$ divides $|G|$. The number $\frac{|G|}{|H|}$ is called the index of H.

20. The order of an element g is the minimal positive integer n such that $g^n = 1$. In a finite group G the order of an element divides $|G|$.

21. Let $s(m)$ be the number of elements of order m in C_n. Prove that $s(m) = \varphi(m)$.

22. Every permutation group S_n has a subgroup A_n of index 2. It is called the *alternating group*. One can define A_n as follows.

(a) A transposition is a permutation that exchanges two numbers and does not move all others. Every permutation is a product of transpositions.

(b) For any permutation s define the number of inversions $l(s)$ as the number of pairs $i < j$ such that $s(i) > s(j)$. Check that for any permutation s and any transposition t, $l(st) - l(s)$ is odd.

(c) Let $t_1 \dots t_k = t'_1 \dots t'_l$ for some transpositions $t_1, \dots, t_k, t'_1, \dots, t'_l$. Show that $k - l$ is even.

(d) Let A_n be the set of all even permutations in S_n. Then A_n is a subgroup of S_n of index 2.

Groups in geometry.

23. Let T denote the group of rigid motions of the plane and G be a finite subgroup of T. Show that G has a fixed point on the plane.

24. The dihedral group D_n is the subgroup of all rigid motions which preserve a regular n-gon. Find the number of elements in D_n and check that C_n is a subgroup of D_n (here we thaink about $\mathbb{C}$ as a plane).

In order to say formally that two groups are *the same* we need the notion of *isomorphism*. Isomorphism is a bijective map $F : G \to G'$ that preserves multiplication, i.e. $F(ab) = F(a)F(b)$. If such F exists we say that G and G' are isomorphic (essentially the same).

25. Prove that D_3 is isomorphic to S_3.

26. Prove that any finite subgroup of T is isomorphic to C_n or D_n.

27. *The group of rotations* $SO(3)$ of the (three dimensional) space is by definition the group of rigid motions which preserve orientation and fix the origin. Show that every element $g \neq 1$ of $SO(3)$ is a rotation about some line passing through the origin.

28. Show that the subgroup of all elements in $SO(3)$ which preserve a regular tetrahedron is isomorphic to A_4.

29. Show that the group of rotations of a cube is isomorphic to S_4.

30. Show that the group of rotations of a dodecahedron is isomorphic to A_5.

31. Any finite subgroup of $SO(3)$ is isomorphic to C_n, D_n, A_4, S_4 or A_5.