MATH 10
ASSIGNMENT 24: EULER'S FUNCTION
APR 22, 2023

Summary of previous results

We will be using some basic results from number theory which we had discussed 2 years ago. Most important of them is the following:

Theorem. *If two integers a, b, are relatively prime, then there exist $x, y \in \mathbb{Z}$ such that*

$$ax + by = 1.$$

Corollary: if a is relatively prime with a positive integer $n > 1$, then a is invertible modulo n: there exists an integer x such that $ax \equiv 1 \mod n$.

Using this, we have proved last time the following result:

Theorem 1. *The set $\mathbb{Z}_n^\times$ of all remainders modulo n relatively prime with n is a group with respect to multiplication.*

The order of this group is denoted by $\varphi(n)$ and is called the Euler function:

$$\varphi(n) = \text{number of remainders modulo } n \text{ which are relatively prime to } n.$$

For example, if $n = p$ is prime, then $\mathbb{Z}_p^\times = \{1, 2, \dots, p-1\}$, so that $\varphi(p) = p - 1$.

Combining this with the results about the order of an element, we got Euler's theorem:

Theorem 2. *If a is relatively prime to n, then $a^{\varphi(n)} \equiv 1 \mod n$. In particular, for prime p, we have $a^{p-1} \equiv 1 \mod p$ for any a not divisible by p.*

1. Use Euclid's algorithm to find x, y such that $211x + 103y = 1$.

2. Find the following inverses
  (a) Inverse of 5 modulo 22
  (b) Inverse of 10 mod 17
  (c) Inverse of 103 modulo 211

3. Prove that for a prime p, one has $\varphi(p^k) = p^k - p^{k-1}$. Compute $\varphi(128)$; $\varphi(125)$.

4. Prove that if p, q are different primes, then $\varphi(pq) = (p-1)(q-1)$. Can you guess the general formula for $\varphi(n)$ if prime factorization of n is $n = p_1^{k_1} \dots p_m^{k_m}$?

5. Compute $\varphi(10)$; $\varphi(100)$; $\varphi(72)$

6. Let p, q be two different primes, and let a be relatively prime to p, q. Sow that then $a^d \equiv a \mod pq$ for any d which satisfeis $d \equiv 1 \mod (p-1)(q-1)$. Is the same true without the assumption that a is not divisible by p, q?

7. Compute the last digit of 2003^{280}

8. Compute the last digit of $7^{(7^7)}$

9. Consider the group $\mathbb{Z}_{11}^\times$. Does it have an element of order 10? Is the group cyclic (i.e., is it true that there is an element x such that $\mathbb{Z}_{11}^\times = \{1, x, x^2, \dots\}$) ?