MATH 9
ASSIGNMENT 24: EULER'S FUNCTION

APRIL 24, 2022

Summary of previous results

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

$$ax + by = 1.$$

Corollary: an congruence class $[a] \in \mathbb{Z}_n$ is invertible if and only if a is relatively prime with n.

Chinese Remainder Theorem:

Theorem. *Let m, n be relatively prime. Then for any k, l, the system of congruences*

$$x \equiv k \mod m$$
$$x \equiv l \mod n$$

has a solution, and any two solutions differ by a multiple of mn.

Fermat's little theorem

Let us take a number and start computing its powers modulo some prime p. For example, computing powers of 2 mod 5, we get:

$$2,\ 2^2 = 4,\ 2^3 = 8 = 3,\ 2^4 = 3 \cdot 26 = 1,\ 2^5 = 2,$$

and after this, the values will be repeating periodically, with period 4 (since $2^4 \equiv 1$, we get $2^{k+4} \equiv 2^k \cdot 2^4 \equiv 2^k$).

It turns out that this is a general phenomenon: powers will always begin repeating periodically, and we can even say what the period is

Theorem (Fermat's little theorem)**.** *Let p be a prime number and let a be a number which is not divisible by p. Then $a^{p-1} \equiv 1 \mod p$.*

Equivalently, using the language of congruence classes discussed before, we can rewrite this result as follows: for any $[a] \in \mathbb{Z}^p$, $[a] \neq [0]$, we have $[a]^{p-1} = [1]$.

Note that the theorem doesn't claim that $k = p - 1$ is the smallest power of a which is congruent to 1. For example, for $p = 7$, Fermat's little theorem claims that $a^6 \equiv 1$, but one easily sees that for $a = 2$, we have $2^3 \equiv 1$. Still the theorem is true: 2^6 is also congruent to 1.

Euler's function

If n is not prime, it is not true that $a^{n-1} \equiv 1 \mod n$ for any a not divisible by n. Instead, the result needs to be modified.

Definition. Euler's function of n is defined by

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

For example, if $n = p$ is prime, then any nonzero remainder mod p is relatively prime to p, so $\varphi(p) = p - 1$.

Generalization of Fermat's little theorem to this case is called Euler's theorem:

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

To compute Euler's function, one can use the following result, proved in the previous homework.

Theorem. *If m, n are relatively prime, then $\varphi(mn) = \varphi(m)\varphi(n)$.*

Homework

1. Prove that for a prime p, one has $\varphi(p^k) = p^k - p^{k-1}$. Compute $\varphi(128)$; $\varphi(125)$; $\varphi(10)$; $\varphi(12)$.

2. Use results of the previous problem and $\varphi(mn) = \varphi(m)\varphi(n)$ to write a general formula for $\varphi(n)$, where $n = p_1^{k_1} \dots p_m^{k_m}$. Find $\varphi(15)$; $\varphi(100)$; $\varphi(1001)$; $\varphi(240)$; $\varphi(30000)$; $\varphi(96)$.

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

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

5. Compute the last two digits of 2011^{970}.

6. The goal of this problem is to prove Fermat's little theorem. Let p be prime; denote by $\mathbb{Z}_p^\times$ the set of non-zero remainders mod p. Let $[a] \in \mathbb{Z}_p^\times$.

(a) Show that $[x] \mapsto [ax]$ is a bijection $\mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$; in other words, every element $[y] \in \mathbb{Z}_p^\times$ can be uniquely written in the form $[y] = [a][x]$ for some $x \in \mathbb{Z}_p^\times$.

(b) Show that $[a]$, $[2a]$, ..., $[a(p-1)]$ is the same set as $[1]$, $[2]$, ..., $[p-1]$ (but in different order).

(c) Prove

$$[a] \cdot [2a] \cdot \dots \cdot [a(p-1)] = [1][2] \dots [(p-1)]$$

as an element in $\mathbb{Z}_p^\times$

(d) Deduce from this Fermat's little theorem.

***7.** Can you modify the arguments above to prove Euler's theorem?