MATH 8
ASSIGNMENT 28: EULER FUNCTION
MAY 16, 2021

Theorem (Fermat's Little theorem). *For any prime p and any number a not divisible by p, we have $a^{p-1}-1$ is divisible by p, i.e.*

$$a^{p-1} \equiv 1 \mod p.$$

This shows that remainders of a^k mod p will be repeating periodically with period $p-1$ (or smaller).

A similar statement holds for remainders modulo n, where n is not a prime. However, in this case $p-1$ must be replaced by a more complicated number: the Euler function of n.

Definition. For any positive integer n, Euler's function $\varphi(n)$ is defined by

$$\varphi(n) = \text{ number of integers } a,\ 1 \le a \le n-1, \text{ which are relatively prime with } n$$

Note that by previously proved results, "relatively prime with n" is equivalent to "is invertible mod n".

For example, if $n = p$ is prime, then any non-zero remainder mod n is relatively prime with n, so in this case $\varphi(p) = p - 1$ Some properties of Euler's function are given in problems below.

Theorem (Euler's theorem). *For any integer $n > 1$ and any number a which is relatively prime with n, we have $a^{\varphi(n)} - 1$ is divisible by n, i.e.*

$$a^{\varphi(n)} \equiv 1 \mod n.$$

In the example when $n = p$ is prime, we get $\varphi(p) = p - 1$, , soin this case Euler's theorem becomes Fermat's little theorem.

For example, $\varphi(10) = 4$. This means that for any number a which is relativley prime with 10, remainders of a^k modulo 10 (i.e., the last digit of a^k) repeat periodically with period 4.

1. Compute $\varphi(25)$; $\varphi(125)$; $\varphi(100)$.

2. Let p be prime. Compute $\varphi(p)$; $\varphi(p^2)$; $\varphi(p^k)$

3. Use Chineses remainder theorem to show that if m, n are relatively prime, then a number a is invertible modulo mn if and only if it is invertible mod n and inviertible mod n. Deduce from this that

$$\varphi(mn) = \varphi(m)\varphi(n) \qquad \text{if } \gcd(m,n) = 1$$

4. Find the last two digits of $14^{14^{14}}$.

***5.** (a) Show that if a is not divisible by 7 or 11, then $a^{60} \equiv a \mod 77$

(b) Show that for any a, we have $a^{61} \equiv a^{121} \equiv \cdots \equiv a \mod 77$

(c) Given a number a between 1 and 77, Alice computes $b = a^{13} \mod 77$ and shows the answer to Bob. Show that then Bob can find a by using $a = b^d$ for some d. [Hint: it suffices to find d such that $13d \equiv 1 \mod 60$]