EULER'S THEOREM CONTINUED

MAY 1, 2022

Summary of previous results

Theorem (Chinese Remainder 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. In particular, x is divisible by both m and n if and only if x is divisible by mn.

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

Theorem (Euler's theorem)**.** *If a is relatively prime to n, then $a^{\varphi(n)} \equiv 1 \mod n$.*

Here $\varphi(n)$ is Euler's function:

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

To compute Euler's function, one can use the following result.

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

Problems

1. Does there exist a power of 3 which ends in 0001?

2. Prove that if p is prime, then for any number a, $a \equiv a^p \equiv a^{1+2(p-1)} \mod p$. More generally, if $k \equiv q \mod (p-1)$, then $a^k \equiv a$

3. Prove that for any a, $a^{11} - a$ is a multiple of 66.

4. Prove that $7^{120} - 1$ is a multiple of 143.

5. Let p, q be different primes. Prove that then, if $k \equiv 1 \mod (p-1)(q-1)$, then $a^k \equiv a \mod pq$.

6. Prove that the number $111\dots1$ (16 ones) is divisible by 17. [Hint: what about $99\dots9$?]

***7.** Let p be a prime number. Let us write $1/p$ as an infinite decimal. Show that the digits (after some point) will be periodically repeating with period which divides $p-1$. [Hint: try to formulate the rule how each next digit is obtained from the previous one]

Test it for $p = 7$; for $p = 13$; $p = 17$