MATH CLUB: NUMBER THEORY: FERMAT'S THEOREM AND EULER FUNCTION

OCT 25, 2020

The following two results are frequently useful in doing number theory problems:

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

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

It is known that Euler's function $\varphi(n)$ is multiplicative:

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

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.*

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

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. Show that equation

$$a^2 + b^2 - 8c = 6$$

has no integer solutions.

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

3. Find 5^{2092} modulo 11. What about the same number, but modulo 11^2?

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

5. FInd at least one n such that 2013^n ends in 001 (i.e. the rightmost three digits of 2013^n are 001). Can you find the smallest such n?

6. Find the last three digits of 7^{1000}. [Hint: first find what it is mod 2^3 and mod 5^3.]

***7.** This is not so much a problem as a mini research topic.

The number 76 had the property that $76^2 = 5776$ ends again in 76. Can you continue this and get a three-digit number $a76$ so that its square again ends in $a76$? Do you think it can be continued to 4-digit number, 5-digit number, ...? And are there other numbers with the same property?

Hint: last k digits are the same as remainder of a number mod 10^k. What if you ask similar question, but in about last digits in base 2? in base 5?

8. And now for something completely different...

(a) Jake has a bag with 20 pieces of red candy and 30 pieces of green candy. Every day he pulls out a candy and eats it; then he continues pulling out candies and eating them as long as they are the same color as the first candy of the day. Once he gets a candy of different color, he eats it and stops for the day. Next day he begins anew.
What is the probability that the last candy he eats will be red?

(b) Same as previous, but with an importnat difference: once Jake gets a candy of different color, he doesnt eat it but instead **retirns it to the bag** and stops for the day.
Again, what is the probability that last candy he eats s red?

Hints to the last problem are on reverse.

Hints for last problem: Part a: who cares when one day ends and the next one begin
Part b: who cares how many candy of each color there are as long as this number is nonzero