

MATH 8, ASSIGNMENT 26: FERMAT'S LITTLE THEOREM

APRIL 26, 2026

CHINESE REMAINDER THEOREM

Theorem (Chinese Remainder Theorem). *Let a, b be relatively prime. Then, for any choice of k, l , the following system of congruences:*

$$\begin{aligned}x &\equiv k \pmod{a} \\x &\equiv l \pmod{b}\end{aligned}$$

has a unique solution mod ab , i.e. it has solutions and any two solutions differ by a multiple of ab . In particular, there exists exactly one solution x such that $0 \leq x < ab$.

FERMAT'S LITTLE THEOREM

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.*

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

This shows that remainders of $a^k \pmod{p}$ will be repeating periodically with period $p - 1$ (or smaller). Note that this only works for prime p .

As a corollary, we get that for any a (including those divisible by p) we have

$$a^p \equiv a \pmod{p}$$

More generally, $a^{k(p-1)+1} \equiv a \pmod{p}$.

Note that the condition that p be prime is important: notice, for example, $3^{(8-1)} \pmod{8}$ is congruent to 3, not 1.

There are many proofs of Fermat's little theorem; one of them is given in problem 8 below.

1. Find all solutions of the system

$$\begin{aligned}x &\equiv 4 \pmod{9} \\x &\equiv 5 \pmod{11}\end{aligned}$$

2. The theory of biorhythms suggests that one's emotional and physical state is subject to periodic changes: 23-day physical cycle and a 28-day emotional cycle. (This is a highly dubious theory, but for this problem, let us accept it.) Assuming that for a certain person January 1st, 2021 was the first day of both cycles, how many days will it take for him to achieve top condition on both cycles (which happens on 6th day of 23-day cycle and 7th day of 28-day cycle)? When will be the next time he achieves top condition in both cycles? (Note: first day is day 1, not day 0!)
3. Find 5^{2021} modulo 11.
4. Prove that $2019^{3000} - 1$ is divisible by 1001. [Hint: you can use Chinese remainder theorem and equality $1001 = 7 * 11 * 13$.]
5. Find the last two digits of 7^{1000} . [Hint: first find what it is mod 2^2 and mod 5^2 .]
6. Show that for any integer a , the number $a^{11} - a$ is a multiple of 66
7. Show that the number 111...1 (16 ones) is divisible by 17. [Hint: can you prove the same about number 999...9?]
8. Let p be a prime number.
 - (a) Show that for any k , $1 \leq k \leq p - 1$, the binomial coefficient ${}_p C_k$ is divisible by p .
 - (b) Without using Fermat's little theorem, deduce from the previous part and the binomial theorem that for any a, b we have $(a + b)^p \equiv a^p + b^p \pmod{p}$
 - (c) Prove that for any a , we have $a^p \equiv a \pmod{p}$. [Hint: $a^p = (1 + 1 + \dots + 1)^p$]