MATH 8
ASSIGNMENT 13: CHINESE REMAINDER THEOREM

JAN 14TH, 2018

In two weeks we are going to start Geometry. Please buy: "The Art of Problem Solving, Volume 1: The Basics" by Sandor Lehoczky and Richard Rusczyk, ISBN-13: 978-0-9773045-6-1. Please do not get the solution manual (or hide it for emergencies). It is important that you try the problems on your own.

Reminders: LCM

Theorem. *If a, b are relatively prime, then any common multiple of a, b is a multiple of ab. In particular,* $\gcd(a, b) = ab$.

If $\gcd(a, b) = d$, *then* $\text{lcm}(a, b) = ab/d$.

Theorem. *Any positive integer $m > 1$ can be written in the form*

$$m = p_1^{k_1} \dots p_l^{k_l}$$

where p_i are distinct prime numbers. Moreover, such a decomposition is unique (except for for reordering factors)

Chinese Remainder Theorem

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

$$x \equiv k \mod a$$
$$x \equiv l \mod b$$

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

Proof. First, we prove existence of a solution. Write $x = k + ta$; then the first congruence is satisfied. To satisfy the second one, we need $k + ta \equiv l \mod b$, or

$$ta \equiv l - k \mod b$$

Since a, b are relatively prime, a has an inverse modulo b; multiplying both sides by this inverse, we get the t. This shows existence of a solution.

If x, x' are two different solutions, then $x - x'$ satisfies

$$x - x' \equiv 0 \mod a$$
$$x - x' \equiv 0 \mod b$$

Thus, $x - x'$ is a common multiple of a, b, so it is a multiple of ab.

□

Problems

When doing this homework, be careful that you only use the material we had proved or discussed so far — in particular, please do not use the prime factorization. And I ask that you only use integer numbers — no fractions or real numbers.

1. Find all solutions of the system

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

2. Find all solutions of the system

$$\begin{aligned} x &\equiv 5 \mod 7 \\ x &\equiv 9 \mod 30 \end{aligned}$$

3. The standard 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 yesterday, Feb 1st, 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!)

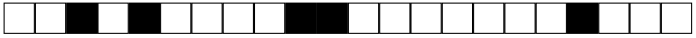
4. (a) Find the remainder upon the division of 19^{2014} by 7.
(b) Find the remainder upon the division of 19^{2014} by 70. [Hint: use $70 = 7 \times 10$ and Chinese remainder theorem.]

5. Prove that a number a is relatively prime with the product ab if and only if it is relatively prime with a and also relatively prime with b.

6. Let $\varphi(n)$ be the number of remainders mod n which are relatively prime to n.
(The function $\varphi(n)$ is called the Euler function and plays a key role in number theory.)
(a) Compute $\varphi(10)$; $\varphi(25)$; $\varphi(125)$; $\varphi(3^7)$
(b) Prove that $\varphi(n)$ is multiplicative: if m, n are relatively prime, then $\varphi(mn) = \varphi(m)\varphi(n)$.
(c) Compute $\varphi(12)$; $\varphi(2^3 3^7)$; $\varphi(10000)$;
(d) Let $n = p_1^{k_1} \dots p_l^{k_l}$ where p_i are distinct prime numbers. What is $\varphi(n)$?

***7.** Prove that $\sqrt{2}$ is irrational: assume $\sqrt{2} = p/q$, where p, q are relatively prime, and get a contradiction.
[Hint: rewrite it in the form $p^2 = 2q^2$. Are p, q even or odd?]

***8.** Consider all numbers with at most six digits: 000001 – 999999. How many of them have the sum of digits equal to 17?
[Hint: does the figure below help?]



214073