MATH CLUB: NUMBER THEORY: CHINESE REMAINDER THEOREM

NOV 1, 2020

As before, all numbers used in this assignment are integers.

Theorem (Chinese Remainder Theorem)**.** *Let m, n be relatively prime. Then for any a_1, a_2 the system of congruences*

$$x \equiv a_1 \mod m$$
$$x \equiv a_2 \mod n$$

has a solution, and the solution is unique up to adding a multiple of mn.

For small numbers, a solution can be found by trial and error. For larger numbers, write $x = a_1 + km$; plugging this into the second congruence gives $km \equiv (a_2 - a_1) \mod n$, which is easy to solve if we can find the inverse of m mod n.

As a practical corollary, we can use this theorem to solve, e.g., problems where one is required to find remainder of a number mod 100: if we can find $x \mod 25$ and $x \mod 4$, then by CRT, this uniquely defines $x \mod 100$.

1. Find all prime numbers p such that $29^p + 1$ is a multiple of p. [Hint: show first that p can not be equal to 29.]
2. Find $2^{98} \mod 33$.
3. Find last two digits of 1032^{1032}
4. Calculate the last three digits of
$$2005^{11} + 2005^{12} + \cdots + 2005^{2006}$$
5. Let $a_n = 6^n + 8^n$. Find a_{83} mod 7; mod 49.
6. This problem is a basically a review of RSA method of public key cryptography.
   (a) Let $n = 11 \cdot 13$. Prove that then for any a, we have $a^{121} \equiv a \mod n$; more generally, $a^{120k+1} \equiv a \mod n$. [Note: we are not assuming that a is relatively prime with n.]
   (b) Consider the function (on the set of all remainders mod n) given by
   $$f(x) = x^{43}.$$
   Show that we can invert this operation: if $y = x^{43}$, then $x = y^{67}$. (The number 43 was chosen randomly; can you guess how we came up with number 67?)
   (c) Can you explain how we could generalize this if 11 and 13 are replaced by arbirary pair of primes p, q, so that $n = pq$: if we have a function $f(x) = x^e$ on the set of all remainders mod n, how can we invert this function?