MATH 350, SPRING 2021

HOMEWORK 7, DUE MARCH 20

(1) If $x \equiv [4,8] \pmod{[7,13]}$, find x modulo 91. *Hint: Adding a multiple of* 7 *will change a number modulo* 13 *but not modulo* 7*, and vice versa.*

(2) Prove that if $n > 2$, $\phi(n)$ is even.

(3) Compute $\phi(5880)$.

(4) Find all natural numbers n such that $\phi(n) = 6$.

(5) Let $p = 47$ and $q = 59$, $N = pq = 2773$, and $e = 157$. This key is used in the original paper by Rivest, Shamir, and Adleman (RSA). For this problem, you might wish to use technology. In particular, the Python code `pow(m,e,N)` computes $m^e \pmod{N}$.

  (a) Compute a multiplicative inverse of e modulo $\phi(N)$.

  (b) Every two-letter string (including A-Z and spaces) can be converted to a number-message between 0000 and 2626 by replacing space by 00, A by 01, B by 02, etc. Encrypt the two-letter string HI by converting it to a number m, then the ciphertext m^e modulo n.

  (c) Decrypt 0802-2179-2276-1024.

(6) Suppose that N is the product of two distinct odd primes, $N = pq$. If $N = 8633$ and $\phi(N) = 8448$, what are p and q? (This problem shows why Alice must keep $\phi(N)$ secret as well as p and q.)

(7) *PAR problem #7.* Give a different proof of Euler's Criterion for squareness (Theorem 8.5 in the text) using primitive roots instead of Wilson's Theorem. You may take Proposition 8.3, which states that exactly half of the nonzero congruence classes modulo a prime are quadratic residues, as given.