Computational Number Theory - Homework 3

Philip Warton

February 15, 2021

Problem 17

Show that if n is a positive integer and $n \equiv 2 \mod 4$, then $8^n + 9^n$ is divisible by 5.

Proof. Since $n \equiv 2 \mod 4$ of course we have some $k \in \mathbb{Z}$ such that $n = 4k + 2$. Then we write

$$8^n + 9^n = 8^{4k+2} + 9^{4k+2} = 8^2 8^{4k} + 9^2 9^{4k}$$

Observe the following facts modulo 5,

$$8^2 \equiv 64 \equiv 4 \tag{1}$$
$$9^2 \equiv 81 \equiv 1 \tag{2}$$
$$\tag{3}$$
$$8^4 \equiv 4^2 \equiv 16 \equiv 1 \tag{4}$$
$$9^4 \equiv 1^2 \equiv 1 \tag{5}$$

So then we can say

$$8^n + 9^n \equiv (4)1^k + (1)1^k \equiv 4 + 1 \equiv 0 \mod 5 \tag{6}$$

□

Problem 18

Show that if $p \geqslant 5$ is prime and $a, b \in \mathbb{Z}$, then $ab^p - a^p b$ is divisible by $6p$.

Proof. Assume that $p \geqslant 5$ is some prime number, and let a, b be integers. We want to show that $ab^p - a^p b$ is divisible by $6p$. We write

$$ab^p - a^p b = (ab)(b^{p-1} - a^{p-1})$$

Then if a number is divisible by $6p$ it must be divisible by 6 and by p. We know that $p \nmid 6$ it follows that this proof may involve Fermat's Little Theorem. So we know that $6^{p-1} \equiv 1 \mod p$. We can write $6p = (2)(3)(p)$. Possibly we can invoke Fermat's Little Theorem to say that $b^{p-1} - a^{p-1}$ must be equivalent to 0 mod 2, mod 3, or mod p. If both a and b are divisible by $2, 3$ and p then trivially the term $ab^p - a^p b$ is divisible by $6p$. If both are not divisible by 2, 3, or p then of course $b^{p-1} - a^{p-1} \equiv 0 \mod p$ and therefore the number $ab^p - a^p b$ is divisible by p and therefore $6p$. Of course if we have any other combinations of a and b's prime factors that covers $6p$ it follows that ab will be divisible by $6p$. □

Problem 19

Let $n \geqslant 1$ and let $m = 2^n - 1$. Show that (a.) if m is prime then n is prime, and that (b.) if n is prime then m is either prime or base 2 psuedo-prime.

(a)

(b)

Problem 20

Problem 21

Problem 22