Math 104A, Fall 2018

Number Theory, HW 7

Due Wednesday November 21st by 5PM in Shubham Sinha's box.

From Weissman's book `An illustrated theory of numbers`:

- Exercises (Section 6, pages 170–171):

  4 (see Definition 6.16 on page 160)

- Exercises (Section 7, pages 190–191):

  3, 4, 5, 6, 7, 8, 12, 13(a+b+c)

Problem A. Fix an integer $a > 1$. A composite number $m > 1$ is called a pseudo-prime with respect to a if $\text{GCD}(a, m) = 1$ and $a^{m-1} \equiv 1 \pmod{m}$.

(a) Show that 561 is a pseudo-prime with respect to **any** a which is coprime to 561. (Such numbers are called Carmichael numbers.)

(b) Let $p > 2$ be any prime <u>not</u> dividing $a(a^2 - 1)$ and consider the number

$$m == \frac{a^{2p} - 1}{a^2 - 1} = \frac{a^p - 1}{a - 1} \cdot \frac{a^p + 1}{a + 1}.$$

The following steps will show that m is a pseudo-prime with respect to a.

(1) Use the above factorization (and the assumption that p is odd) to check that m is composite – and coprime to a.

(2) Verify that

$$(a^2 - 1)(m - 1) == a^{2p} - a^2 == a(a^{p-1} - 1)(a^p + a)$$

is divisible by $2p(a^2 - 1)$ and conclude that $2p$ divides $m - 1$.

(3) Note that $a^{2p} = 1 + m(a^2 - 1) \equiv 1 \pmod{m}$ and infer from (2) that

$$a^{m-1} \equiv 1 \pmod{m}$$

which shows m is a pseudo-prime relative to a.

[Letting p vary yields infinitely many pseudo-primes relative to a given a.]