Assignment 12.

This homework is due *Thursday* April 19.

There are total 35 points in this assignment. 31 points is considered 100%. If you go over 31 points, you will get over 100% for this homework (up to 115%) and it will count towards your course grade.

Collaboration is welcome. If you do collaborate, make sure to write/type your own paper *and give credit to your collaborators in your pledge.* Your solutions should contain full proofs. Bare answers will not earn you much.

(1) (8.1.1ab) Find the order of integers $2, 3, 5$:
  (a) [2pt] modulo 17,
  (b) [2pt] modulo 19.

(2) Let p be an odd prime. Prove the following.
  (a) [2pt] (8.1.2b) Prove that if $\mathrm{ord}_p a = 2k$, then $a^k \equiv -1 \pmod{p}$. (*Hint:* What's the order of a^k?)
  (b) [2pt] (8.2.6a) If r is a primitive root of p, then $r^{(p-1)/2} \equiv -1 \pmod{p}$.
  (c) [2pt] (9.1.5a) Prove that a primitive root of p is never a quadratic residue of p.

(3) (8.1.11)
  (a) [2pt] Find two primitive roots of 10.
  (b) [3pt] Use the information that 3 is a primitive root of 17 to obtain all eight primitive roots of 17.

(4) Using the information that 2 is a primitive root of 19, solve the congruences:
  (a) [3pt] $x^3 \equiv 1 \pmod{19}$.
  (b) [3pt] $x^3 \equiv 13 \pmod{19}$. (*Hint:* $13 \equiv 2^5 \pmod{19}$.)
  (c) [3pt] $x^3 \equiv 7 \pmod{19}$. (*Hint:* $7 \equiv 2^6 \pmod{19}$.)

(5) [3pt] Let an integer $k > 0$ and a prime p be such that $\gcd(k, p-1)=1$. Prove that the only solution of the congruence $x^k \equiv 1 \pmod{p}$ is $x \equiv 1 \pmod{p}$.

(6) [4pt] (8.2.9) Use the fact that each prime p has a primitive root to give a different proof of Wilson's theorem. (*Hint:* Show first that if p has a primitive root r, then $(p-1)! \equiv r^{1+2+\ldots+(p-1)} \pmod{p}$.)

(7) [4pt] For an odd prime p, prove that the sum

$$1^n + 2^n + 3^n + \ldots + (p-1)^n \equiv \begin{cases} 0 \pmod{p} & \text{if } (p-1) \nmid n, \\ -1 \pmod{p} & \text{if } (p-1) \mid n. \end{cases}$$

[*Hint:* Show that if $(p-1) \nmid n$, and r is a primitive root of p, then this sum is congruent mod p to

$$1 + r^n + r^{2n} + \ldots + r^{(p-2)n} = \frac{r^{(p-1)n} - 1}{r^n - 1}.]$$