Math 406 – Fall 2025 – Harry Tamvakis
PROBLEM SET 8 – Due November 6, 2025

Reading for this week: Section 10.

Problems

From Section 10, #2, 4, 8, 9, 10, 20. In addition, do the following problems:

A1) Suppose that $\gcd(a,n)=1$. Prove each of the statements below.

(a) If $\mathrm{ord}_n(a)=hk$, then $\mathrm{ord}_n(a^h)=k$.

(b) If p is an odd prime and $\mathrm{ord}_p(a)=2k$, then $a^k \equiv -1 \pmod{p}$.

(c) If $\mathrm{ord}_n(a)=n-1$, then n is a prime number.

A2) Assume that $\mathrm{ord}_n(a)=h$ and $\mathrm{ord}_n(b)=k$.

(a) Show that $\mathrm{ord}_n(ab)$ divides hk.

(b) Deduce that if $(h,k)=1$, then $\mathrm{ord}_n(ab)=hk$.

A3) Prove that $\phi(2^n-1)$ is a multiple of n for any $n>1$. [Hint: The integer 2 has order n modulo 2^n-1.]

A4) For an odd prime p, prove that

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

[Hint: If $(p-1)\nmid n$, and a is a primitive root of p, then the sum is congruent modulo p to

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

Extra Credit Problem.

EC) Let p be a prime and n a natural number with $(n,p-1)=1$. Prove that for any integer a, the equation $x^n \equiv a \pmod{p}$ has exactly one solution in x. [Hint: Consider first the case that $a\equiv 0 \pmod{p}$; then use primitive roots when $a \not\equiv 0 \pmod{p}$.]