

Math 406 – Fall 2009 – Harry Tamvakis
PROBLEM SET 8 – Due November 5, 2009

Reading for this week: Section 10.

Problems

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

A1) Prove each of the following statements below:

- (a) If $\text{ord}_n(a) = hk$, then $\text{ord}_n(a^h) = k$.
- (b) If p is an odd prime and $\text{ord}_p(a) = 2k$, then $a^k \equiv -1 \pmod{p}$.
- (c) If $\text{ord}_n(a) = n - 1$, then n is a prime number.

A2) Prove that $\phi(2^n - 1)$ is a multiple of n for any $n > 1$. [Hint: The integer 2 has order n modulo $2^n - 1$.]

A3) Assume that $\text{ord}_n(a) = h$ and $\text{ord}_n(b) = k$. Show that $\text{ord}_n(ab)$ divides hk , and deduce that if $(h, k) = 1$, then $\text{ord}_n(ab) = hk$.

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 r is a primitive root of p , then the sum is congruent modulo p to

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

Extra Credit Problems.

EC1) 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 $a \not\equiv 0 \pmod{p}$.]

EC2) Consider the sequence $\{F_n\}$ of Fibonacci numbers, with $F_0 = 0$, $F_1 = F_2 = 1$, and $F_{n+2} = F_{n+1} + F_n$ for all $n > 0$. Choose a modulus N

and consider the sequence $\{F_n \bmod N\}$ as $n = 0, 1, 2, \dots$. For example, for $N = 7$ the sequence of $\{F_n \bmod 7\}$ looks like

$$0, 1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, 1, 1, 2, 3, 5, \dots$$

while for $N = 8$ the sequence of $\{F_n \bmod 8\}$ is

$$0, 1, 1, 2, 3, 5, 0, 5, 5, 2, 7, 1, 0, 1, 1, 2, 3, 5, 0, 5, 5, 2, 7, 1, \dots$$

Prove that for any fixed $N > 0$, this sequence is *periodic*. That is, there exists a number $t > 0$ (which will depend on N) such that

$$F_{n+t} \equiv F_n \bmod N$$

for all $n \geq 0$.