Homework 8

Aleck Zhao

April 20, 2017

1. Let $p, x, n \in \mathbb{Z}$ with p prime and $n > 0$.
   (a) Prove that if $p \mid x^n$ then $p \mid x$.
   (b) Show that the statement need not be true if p is not prime.
2. Use the Fundamental Theorem of Arithmetic (FTA) to show that $\log_{21} 143$ is irrational.
3. Let $a, b, c, n \in \mathbb{Z}$ with $n > 1$.
   (a) Prove that if $\gcd(c, n) = 1$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$.
   (b) Show that the statement in part (a) need not be true if c and n are not relatively prime.
4. Let $a, b, c, d, n \in \mathbb{Z}$ with $n > 1$. Prove that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then
   (a) $a + c \equiv b + d \pmod{n}$
   (b) $ac \equiv bd \pmod{n}$
5. In this problem we will use direct proof to prove the following statement: Let $a, p \in \mathbb{Z}$. If p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$.
   (a) We are given that $a, p \in \mathbb{Z}, p$ is prime, and $p \nmid a$. Explain why this mean $a \neq 0$.
   (b) Let $S = \{a, 2a, 3, \cdots, (p-1)a\}$. Let $x, y \in S$ with $x \neq y$. Prove $x \not\equiv y \pmod{p}$.
   (c) Let $T = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ and let $f : S \to T$ be given by the rule $f(s) = s \mod p$. Prove f is a bijection.
   (d) Explain why
   $$\prod_{s \in S} s \equiv \prod_{t \in T} t \pmod{p}$$
   (e) Explain why p and $(p-1)!$ are relatively prime.
   (f) Based on your work in parts (d) and (e), conclude that $a^{p-1} \equiv 1 \pmod{p}$.
6. In a transposition cipher we use permutations to help encode text. First we select a positive integer m. Let $M = \{ x \in \mathbb{N} \mid 1 \leq x \leq m \}$. Next, we create a permutation $f : M \to M$. we then take the text message and split its letters into blocks of size m. We encode the block $b_1 b_2 \cdots b_m$ as $c_1 c_2 \cdots c_m$ where $c_i = b_{f(i)}$.
   (a) Suppose $m = 4$ and $f(1) = 3, f(2) = 1, f(3) = 4, f(4) = 2$. Use the transposition cipher to encode PIRATE ATTACK.
   (b) We decrypt an encoded transposition cipher message by using $f \inf$. For the function provided in part (a), what is f^{-1}?
   (c) Using the decryption function you obtained in part (b), decode SWUETRAEOEHS.

- Suppose $n = 713 = 23 \times 31$.
   (a) Let $e = 43$. Bob's encryption function is $E(M) = M^e \mod n$. what is his decryption function?
   (b) Encrypt the word I using Bob's encryption function.
   (c) Let $d = 43$. Sue's decryption function is $D(N) = N^d \mod n$. What is Sue's encryption function?