

HOMEWORK ASSIGNMENT 6
AMAT326 (S09)

Due: April 28 (Tuesday)

- (1) Find the smallest nonnegative solution for system of congruences

$$x \equiv 2 \pmod{7},$$

$$x \equiv 4 \pmod{8},$$

$$x \equiv 3 \pmod{9}.$$

- (2) Recall that $\mathbb{F}_9 = \{a + bi : a, b \in \mathbb{Z}/3\mathbb{Z}\}$ and the Frobenius map $f_3(x) = x^3$ for some $x \in \mathbb{F}_9$. Note that $i^2 = -1$.

(a) Verify that $f_3(1 + 2i) + f_3(2 + 2i) = f_3(1 + 2i + 2 + 2i)$.

(b) Show that $f_3(a + bi) = a - bi$.

(c) Find F_0 , where $F_0 := \{x \in \mathbb{F}_9 : f_3(x) = x\}$.

(d) Show that $f_3 \circ f_3$ is the identity homomorphism on \mathbb{F}_9 .

- (3) Find a primitive root modulo 47.

- (4) Show that U_{25} is cyclic. Find a generator of U_{25} . Find the generators of each of the subgroups of U_{25} .

- (5) Show that U_{28} is not cyclic. What is its order? What is its exponent?

- (6) Find a primitive element of U_{81} by the method of Theorem 3 on page 359 (2^{nd} edition).

- (7) **Extra** (10pt) Prove that $\phi(p^k) = p^{k-1}(p - 1)$.

- (8) **Extra** (10pt) Prove Wilson's theorem:

If p is an odd prime, then $(p - 1)! \equiv -1 \pmod{p}$.

Hint: Look at the hint in E10 on page 350 at the end of section 23A (2^{nd} edition).

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY AT ALBANY, ALBANY, NY 12222