

## SOLUTION

### MATH 115, SUMMER 2012 QUIZ 3

JAMES MCIVOR

There are problems on the back of this page, 20 points total. Write clearly and in complete sentences. If you need extra paper, ask me.

- (1) (8 points) Find all solutions to the congruence  $x^3 + 8x - 5 \equiv 0 \pmod{5^3}$ .

Let  $f(x) = x^3 + 8x - 5$

$$f(x) \equiv 0 \pmod{5} \iff x \equiv 0$$

$$f'(x) = 3x^2 + 8, f'(0) = 3, \text{ so } 0 \text{ is a non-singular root.}$$

$$f'(0)^{-1} = 2. \text{ Set } a = a_1 = 0$$

$$a_2 = 0 - f(0) \cdot 2 = -(-5) \cdot 2 = 10 \pmod{25}$$

$$a_3 = 10 - f(10) \cdot 2 = 10 - (1075) \cdot 2 \pmod{125}$$

$$\equiv 10 - (-50) \cdot 2 = \boxed{110}$$

- (2) (3 points) Let  $a$  be a unit in the ring  $\mathbb{Z}/18$ . What are all the possible values of the order of  $a$ ?

$$\text{ord}(a) / \phi(18) = \phi(2)\phi(9) = 1 \cdot 6 = 6$$

$$\text{So } \boxed{\text{ord}(a) = 1 \text{ or } 2 \text{ or } 3 \text{ or } 6}$$

- (3) (2 points) If  $g$  is a primitive root mod 11, what is the order of  $g^4 \pmod{11}$ ?

$$\text{ord}(g) = \phi(11) = 10. \text{ Look at } g^4, (g^4)^2, (g^4)^3, (g^4)^4, \dots$$

$$\text{So } (g^4)^5 = 1, \text{ hence } \boxed{\text{ord}(g^4) = 5} = g^4, g^8, g^2, g^6, g^{10} = 1$$

- (4) (2 points) Find the order of the element 7 in  $\mathbb{Z}/9$ .

Look at powers of 7 mod 9.  $7^1 = 7$

$$7^2 = 49 \equiv 4$$

$$7^3 = 7^2 \cdot 7 \equiv 4 \cdot 7 \equiv 1$$

$$\text{So } \boxed{\text{ord}(7) = 3}$$

(5) (1 point each) True or False. No justification necessary.

$$\phi(13) = 12$$

(a) If  $a^6 \equiv -1 \pmod{13}$ , then  $a$  is a primitive root mod 13.

**False:**  $a^6 \equiv -1 \Rightarrow a^{12} \equiv 1$ , but could be lower powers that work, too.  $a=5$  has  $a^2 \equiv -1$ , but  $\text{ord}(a)=4$ .

(b) If  $f(x) \equiv 0 \pmod{p}$  has exactly three solutions, then  $f(x) \equiv 0 \pmod{p^2}$  has at least three solutions.

**False:** If one of the 3 solns is singular, it may not lift!

(c) If  $m > 1$  is odd, then every congruence  $f(x) \equiv 0 \pmod{m}$  has at least one solution mod  $m$ .

**False** Take  $f(x) = 1 \pmod{m}$  has no solns unless  $m=1$

(d) If  $g$  is a primitive root mod  $p$ , then  $g^{(p-1)(p-2)/2} \equiv -1 \pmod{p}$ :

**True** If  $p=2$ , then  $g=1=g^k=-1 \forall k$ . If  $p>2$ ,  $g^{p-1} \equiv 1$ , so  $(g^{p-1})^{p-2} = (-1)^{p-2} = -1$ .

(e) There are  $\phi(11)$  primitive roots mod 12.

**False**  $\phi(11) = 10$ , but there are only  $\phi(12) = 4$  elements in  $(\mathbb{Z}/12)^\times$ .