

## MATH 102: IDEAS OF MATH

### WORKSHEET 4

#### 1. Modular Arithmetic

*Question 1.* What is *congruent modulo*? Discuss about ways of representing this concept?

*Question 2.* Let  $a, b, c, d$  and  $m$  be integers so that  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ . Prove that

- (1)  $a + c \equiv b + d \pmod{m}$
- (2)  $a + c \equiv b + d \pmod{m}$
- (3)  $a \cdot c \equiv b \cdot d \pmod{m}$

*Question 3.* Give definition of prime and composite numbers.

*Question 4.* Let  $a, b, c$  be integers and  $p$  be a prime number. Prove the following

- (1) If  $p \nmid a$ , then  $\gcd(p, a) = 1$
- (2) If  $a \mid bc$  and  $\gcd(a, b) = 1$ , then  $a \mid c$
- (3) If  $p \mid bc$ , then  $p \mid b$  or  $p \mid c$

*Question 5* (Modular cancellation law). Let  $a, b, k$  and  $m$  be integers. Prove that if  $ak \equiv bk \pmod{m}$  and  $\gcd(k, m) = 1$ , then

$$a \equiv b \pmod{m}.$$

*Question 6.* Discuss about Fermat's little theorem:

If  $a$  is an integer and  $p$  is a prime so that  $p \nmid a$ . Then,

$$a^{p-1} \equiv 1 \pmod{p}.$$