

Quiz Section 4: Number Theory

Review

Divisibility: For $d \neq 0$ we write $(d \mid a)$ iff there is an integer k such that $a = kd$.

Division Theorem: For integers a and b with $b > 0$, there are unique integers q and r such that $a = qb + r$ and $0 \leq r < b$. The remainder r is also written as $a \bmod b$.

Mod Predicate $(\bmod m)$: For integer $m > 0$ and integers a and b , we write $a \equiv_m b$ iff $m \mid (a - b)$.

This is equivalent to $(a - b) = km$ for some integer k ; it is also equivalent to $a = b + km$ for some integer k .

Properties of $(\bmod m)$:

- For $m > 0$, $a \equiv_m b$ iff $a \bmod m = b \bmod m$.
- If $a \equiv_m b$ and $b \equiv_m c$ then $a \equiv_m c$.
- If $a \equiv_m b$ and $c \equiv_m d$ then
 - $a + c \equiv_m b + d$
 - $ac \equiv_m bd$

Prime: An integer $n > 1$ is prime iff its only positive divisors are 1 and n .

Unique Factorization Theorem: Every positive integer has a unique representation as a product of prime numbers (assuming that the primes in the product are listed with smaller ones first).

Greatest Common Divisor: $\gcd(a, b)$ is the largest common divisor of a and b .

Properties of gcd: For positive integers a and b , $\gcd(a, 0) = a$ and $\gcd(a, b) = \gcd(b, a \bmod b)$.

Multiplicative Inverse: For $m > 0$ and $0 \leq a < m$, the *multiplicative inverse of a modulo m* is a number b with $0 \leq b < m$ such that $ab \equiv_m 1$. It exists if and only if $\gcd(a, m) = 1$.

Task 1 – Divisibility

a) Circle the statements below that are true. Recall for $a, b \in \mathbb{Z}$: $a \mid b$ if and only if $\exists k \in \mathbb{Z}$ such that $b = ka$.

- (a) $1 \mid 3$
- (b) $3 \mid 1$
- (c) $2 \mid 2018$
- (d) $-2 \mid 12$
- (e) $1 \cdot 2 \cdot 3 \cdot 4 \mid 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$

b) Circle the statements below that are true. Recall for $a, b, m \in \mathbb{Z}$ and $m > 0$: $a \equiv_m b$ if and only if $m \mid (a - b)$.

a) $-3 \equiv_3 3$

b) $0 \equiv_9 9000$

c) $44 \equiv_{77} 13$

d) $-58 \equiv_5 707$

e) $58 \equiv_5 707$

Task 2 – Division of Labor

a) Write a formal proof in cozy of the following claim: if $x \equiv_7 y$, then $y \equiv_7 x$. You can find this on cozy here: <https://tinyurl.com/section42a>. Then, translate it into an English proof.

b) For the domain of integers give an English proof that if $ab = 1$ then $a = 1$ or $a = -1$.

c) Give an English proof of the following claim over the domain of integers: if $a \mid b$, $b \mid a$, and $a \neq 0$, then $a = b$ or $a = -b$.

Task 3 – This is really mod

Let n and m be integers greater than 1, and suppose that $n \mid m$. Give an English proof that for any integers a and b , if $a \equiv_m b$, then $a \equiv_n b$.

Task 4 – Casing the Joint

a) Prove that for all integers n , $n^2 \equiv_4 0$ or $n^2 \equiv_4 1$

b) Prove that for every integer n , $n^2 \equiv_3 0$ or $n^2 \equiv_3 1$.

Task 5 – Planning Your Tiling

Suppose that you had a rectangular room and wanted to tile the entire floor with square tiles of all the same size that are as big as possible (assuming no spacing between tiles and no partial tiles).

a) What is the largest square tile you could use if the room's dimensions are 308 cm by 224 cm?

b) How many tiles will you need?