MAS 4301 - Abstract Algebra I

Chapter 0 - Preliminaries

Properties of Integers

The Well-Ordering Principle Every ____.

The Division Algorithm Theorem

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there __________________________ such that

_____________________________________.

Example

(i) $a = 13$, $b = 5$.

(ii) $a = -13$, $b = 5$.

Sketch of Proof of Theorem

Let $S = \{a - bk : k \in \mathbb{Z} \text{ and } a - bk \geq 0\}$.

Case 1 $0 \in S$. Then

Case 2 $0 \notin S$. Then S is a ____________.

Show S is nonempty.

By ____ S has ________.

Let r be the ________.

Then $r =$ ____________.

Show $r < b$. Show uniqueness.

Definition Let $a, b \in \mathbb{Z}$. We say a divides b and write _____ if

____

for ________.

We say a is a divisor of b.

Example $8 \mid 24$ since ____________.

Definition Let $a, b \in \mathbb{Z}$ not both zero. Then the greatest common divisor denoted by ____ is ________________.

NOTE : In Number Theory $\gcd(a,b)$ is denoted by ____.

Example $\gcd(8, 60) =$ ____.

Theorem Let $a, b \in \mathbb{Z}$ not both zero. Then

$\gcd(a,b) = \underline{\underline{MIN}}\{$____________________$\}$

Sketch of Proof

Let $S = \{ as+bt : s, t \in \mathbb{Z} \ \& \ as+bt > 0 \}$.

S is nonempty since ________ $\in S$.

So S is a nonempty set of ________.

By the __________, S has a ________ element d. We show $d = \gcd(a, b)$.

So $d =$ ________

For __________. By the Division Algorithm,

$a =$ ________ for some ________

where ________.

$$r = a - dq$$

$$= a(\_\_\_\_) + b(\_\_\_\_).$$

Since d is the ____________

it follows that $r =$

Hence $a = dq$ & ______.

Similarly ______ so that d is a ________ of a, b. Suppose g is a common divisor of a, b then

& so $d =$ ________. $\square$

Example Let $a = 8$, $b = 15$.
Then

$$\gcd(a,b) = \_\_\_\_ = 8s + 15t \_\_$$

where $s = \_\_\_$ & $t = \_\_\_$.

Definition: We say a, b are **relatively prime** if __________.

Corollary Let $a, b \in \mathbb{Z}$, a, b not both zero.
Then a, b are relatively prime if and only if
____
for ________.

MODULAR ARITHMETIC

Let $a, m \in \mathbb{Z}$ where $m \geq 1$.
By the Division Algorithm

$$a = \_\_\_\_\_\_ \quad \& \quad \_\_\_\_$$

for some ____ integers q, r.
We write $a \pmod{m} = r$.

Example $13 \pmod 5 = \_\_\_$,
$-13 \pmod 5 = \_\_\_$.

NOTE
(1) In Number Theory, r is called the __________
__________.

(2) In Number Theory, we write

$$a \equiv b \pmod{m} \qquad \text{(a is congruent to b mod m)}$$

if __________.

(3) Proposition Let $a, b, m \in \mathbb{Z}$ with $m \geq 1$. Then $a \equiv b \pmod{m}$ if & only if ______________.

PROOF:

($\Longrightarrow$) Suppose $a \equiv b \pmod{m}$. Then $m \mid (a-b)$.
By the division Alg, there are integers q_1, r_1, q_2, r_2 such that

$$a = \qquad\qquad , \qquad b =$$

where $0 \leq r_1 <$ ___ and $0 \leq r_2 <$ ___.
We may assume without loss of generality that

$$0 \leq r_1 \leq r_2.$$

Then

$$b - a = m(\qquad) + (\qquad)$$

and

$$0 \leq \qquad \leq \qquad < .$$

By the Division Alg, $r_2 - r_1 =$ ___
Using ______.
Hence ______, and

$$a \pmod{m} = \qquad = \qquad = b \pmod{m}.$$

($\Longleftarrow$) (EX).

EQUIVALENCE RELATIONS

Definition An equivalence relation on a set S is a relation on a set S satisfying the 3 properties below.

Let $R = \{(a,b) \in S \times S : a \text{ is related to } b\}$.

(i) [REFLEXIVE] ________________________

(ii) [SYMMETRIC] ________________________.

(iii) [TRANSITIVE] ________________________.

Theorem Let m be a positive integer. Congruence mod m is an equivalence relation on the set of integers $\mathbb{Z}$. Let

$$R = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} : a \equiv b \pmod{m}\}.$$

PROOF

(i) Let $a \in \mathbb{Z}$. Then

(ii) Suppose $a, b \in \mathbb{Z}$ & $(a,b) \in R$; ie ________

(iii) Suppose $a, b, c \in \mathbb{Z}$ & $(a,b) \in R$ & $(b,c) \in R$; ie ________________

Equivalence Classes

Definition: Let R be an equivalence relation on a set S. Let $a \in S$. The equivalence class of S containing a is the ___________________

and is denoted by ____.

So

$$[a] = \{ \qquad \qquad \qquad \}.$$

Example Let $m = 2$ & consider congruence mod 2 on $\mathbb{Z}$. Given any $a \in \mathbb{Z}$,

$$a = 2q + r$$

where $q \in \mathbb{Z}$ and $r =$ ____ by the Division Algorithm. So

$$a \equiv \_\_\_ \text{ or } \_\_\_ \pmod 2.$$

$[0] =$

$[1] =$

NOTE: $[0] \cup [1] =$ ____ and $[0] \cap [1] =$ ____

We say $[0], [1]$ is a partition of $\mathbb{Z}$.

Theorem Let $m \in \mathbb{Z}$, $m \geq 1$.
There are exactly ___ different equivalence classes mod m on $\mathbb{Z}$, namely
$[r]$, where ________.

~~Theorem~~
Definition a **partition** of a set S is a collection of nonempty disjoint subsets of S whose union is S.

Theorem
(i) The equivalence classes of an equivalence relation on a set S constitute a ______ of S.
(ii) Conversely, for any partition P of S there is ~~a~~ an ________ on S whose equivalence classes are the ________.

PROOF: Let S be a nonempty set.
(i) Suppose $\sim$ is an equivalence relation on S.
Any equivalence class has the form
$$[a] = \{ \qquad \qquad \qquad \}.$$
Since $\sim$ is _____, $a \sim$ and ____ for all $a \in S$
Hence
$$S =$$
and the union of equivalence classes is ___.
We need to show that distinct equivalence classes are disjoint. Suppose $a, b \in S$ & $[a] \neq [b]$.

We claim that

$$[a] \cap [b] = \_\_\_\_.$$

Suppose by way of contradiction that

(iii) Suppose $\mathcal{P}$ is a partition of S, and so

$$S = \bigcup_{C \in \mathcal{P}} C \qquad \text{(disjoint)}.$$

For $a, b \in S$ we define $a \sim b$ if & only if ________________.

EX: Show $\sim$ is an equivalence relation on S.