

1. (15) Let A be a set and R a relation on A . That is, $R \subseteq A \times A$.

a. Define what it means to say that R is an equivalence relation.

R is an equivalence relation if it satisfies the following three conditions:

reflexive: $\forall a \in A (a, a) \in R$

symmetric: if $(a, b) \in R$ then $(b, a) \in R$

transitive: if (a, b) and (b, c) are both in R , then $(a, c) \in R$.

b. Assume that R is an equivalence relation, and let $[a]$ denote the equivalence class generated by a . Show that the set of equivalence classes forms a partition of the set A .

We need to show that the union of all of the equivalence classes is A and any two equivalence classes are either exactly the same or they are disjoint.

Let $a \in A$, since R is reflexive we know $(a, a) \in R$. That is, $a \in [a]$, and therefore a belongs to the union of the equivalence classes.

Suppose the equivalence classes $[a_1]$ and $[a_2]$ are not disjoint. That is, there is an element x which belongs to A and $x \in [a_1] \cap [a_2]$. Suppose now that $z \in [a_1]$, then transitivity of R tells us that z is related to x , and since x is related to a_2 transitivity tells us that z is also related to a_2 . That is, $z \in [a_2]$. Thus, $[a_1] \subset [a_2]$. An identical argument shows the reverse inclusion, and we may conclude that $[a_1] = [a_2]$.

2. (10) Define the relation R on the integers $Z = \{\dots, -2, -1, 0, 1, \dots\}$ by

$$(m, n) \in R \text{ if } |m - n| \leq 1.$$

a. Find all integers related to 2. That is, find all m such that $(m, 2) \in R$.

We need to find those integers m such that $|m - 2| \leq 1$, but this is equivalent to

$$-1 \leq m - 2 \leq 1$$

$$1 \leq m \leq 3.$$

That is $m = 1, 2$, or 3 .

b. Is R an equivalence relation?

While R is reflexive and symmetric it is not transitive: $(1, 2) \in R$ and $(2, 3) \in R$, but $(1, 3) \notin R$.

3. (25) Let a , b , and n be integers with $n > 0$.

a. Define what $a \equiv b \pmod{n}$ means.

This means that n divides $a - b$.

b. Show that if $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$ then

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{n}.$$

There are integers k_1 and k_2 such that $a_1 - b_1 = k_1n$ and $a_2 - b_2 = k_2n$.
Thus,

$$(a_1 + a_2) - (b_1 + b_2) = (k_1 + k_2)n,$$

which means that $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$.

c. If the equation $5x \equiv 7 \pmod{127}$ has a solution find it. If the equation does not have a solution explain why.

The greatest common divisor of 5 and 127 is 1. The Euclidean algorithm is used to write 1 as a linear combination of 5 and 127:

$$1 = 51 \cdot 5 - 2 \cdot 127$$

$$7 = 357 \cdot 5 - 14 \cdot 127.$$

Thus, $x = 357$ works as does any $x \in [357]$ modulo 127. Note

$$[357] = \{\dots, 484, 357, 230, 103, -24, \dots\}$$

4. (30) Let A be a set with n elements and B a set with m elements.

a. How many different functions are there from A to B ?

Think of a function from A to B as an n -slotted beast; each slot representing one of the elements in A . There are m items from B we can put into any slot. The number of different choices is

$$m^n = |B|^{|A|}.$$

b. If we assume $n \leq m$, how many one-to-one functions from A to B are there?

Again think of a function from A to B as an n -slotted thing. There are m ways to fill the first slot, and since the function is supposed to be one-to-one, there are only $m - 1$ ways to fill the second, etc. Thus, the number of one-to-one functions from A to B is

$$m(m-1)(m-2)\cdots(m-n+1) = \frac{m!}{(m-n)!} = P(m, n).$$

c. If we assume $n > m$, how many one-to-one functions from A to B are there?

The pigeon hole principle tells us that there cannot be such functions.

5. (20) Determine whether each of the following is true or false. If it is true, prove it, and if it's false, give a counter example.

a. Let A, B , etc., denote sets contained in a universal set U . Then

$$\forall A \subseteq U, \forall B \subseteq U, \exists C \subseteq U, \text{ such that } A \cap B = A \cup C.$$

This is false. Let A be any nonempty set and set $B = \emptyset$. Then no matter what C is we will not have equality.

b. If $d_1 = \gcd(a_1, b_1)$ and $d_2 = \gcd(a_2, b_2)$, then

$$d_1 d_2 = \gcd(a_1 a_2, b_1 b_2).$$

This is false. One counter example is given by $a_1 = 2, b_1 = 4, a_2 = 6$, and $b_2 = 1$. Then we have

$$2 = d_1 d_2 \text{ and } \gcd(12, 4) = 4.$$