Problem #1

Use the Euclidean algorithm to calculate the greatest commmon divisor for 24,024 and 7,524. Then use your work to write the gcd as a linear combination of 24,024 and 7,524.

Solution

$$\begin{aligned}
24024 &= (3)7524 + 1542 \\
7524 &= (5)1452 + 264 \\
1452 &= (5)264 + 132 \\
132 &= (2)132
\end{aligned}$$

So the GCD of 24,024 and 7524 is 132. To write the GCD as a linear combination of the two numbers we first solve for the remainders.

$$\begin{aligned}
1452 &= 24042(1) + 7524(-3) \\
264 &= 7524(1) + 1452(-5) \\
132 &= 1452(1) + 264(-5)
\end{aligned}$$

And then we plug in these values to the equations from the first step.

$$\begin{aligned}
132 &= 1452(1) + 264(-5) \\
&= 1452(1) + (7524 + 1452(-5))(-5) \\
&= 1452(1) + 7524(-5) + 1452(25) \\
&= 1452(26) + 7524(-5) \qquad (1) \\
&= (24024 + 7524(-3))(26) + 7524(-5) \\
&= 24024(26) + 7524(-78) + 7524(-5) \\
&= 24024(26) + 7524(-83)
\end{aligned}$$

Problem #2

Suppose R is an equivalence relation on A, S is an equivalence relation on B, and A and B are disjoint. Prove that $R \cup S$ is an equivalence relation on $A \cup B$.

Solution

- Reflexive
  For any $x \in A \cup B$, either
  - Case 1: $x \in A$
    $(x, x) \in R \implies (x, x) \in R \cup S$
  - Case 2: $x \in B$
    $(x, x) \in S \implies (x, x) \in R \cup S$

- Symmetric
  For any $(x, y) \in R \cup S$, either
  - Case 1: $(x, y) \in R$
    $\implies (y, x) \in R \implies (y, x) \in R \cup S$
  - Case 2: $(y, x) \in S$
    $\implies (y, x) \in S \implies (y, x) \in R \cup S$
- Transitive
  Take arbitrary $(x, y), (y, z) \in R \cup S$. y cannot be an element of both A and B because they are disjoint so either
  - Case 1: $(x, y), (y, z) \in R$
    $\implies (x, z) \in R \implies (x, z) \in R \cup S$
  - Case 2: $(x, y), (y, z) \in S$
    $\implies (x, z) \in S \implies (x, z) \in R \cup S$

$R \cup S$ is reflexive, symmetric, and transitive, so $R \cup S$ is an equivalence relation.

Problem #3

Suppose that R is a partial order relation on a set A and that B is a subset of A. The restriction of R to B is defined as follows:

$$\{(x, y) \mid x \in B, y \in B, \text{ and } (x, y) \in R\}$$

In other words, two elements of B are related by the restriction of R to B if, and only if, they are related by R. Prove that the restriction of R to B is a partial order relation on B. (In less formal language, this says that a subset of a partially ordered set is partially ordered.)

Solution

Let $S =$ the restriction of R to B.

- Reflexive
  For any $b \in B$, $(b, b) \in R \implies (b, b) \in S$.
- Antisymmetric
  For any $(x, y) \in S$ such that $x \neq y$:

$$\begin{aligned} (x, y) \in S &\implies (x, y) \in R \\ &\implies (y, x) \notin R \\ &\implies (y, x) \notin S \end{aligned}$$

- Transitive
  For any $(x, y), (y, z) \in S$ it must be the case that $x, y, z \in B$ and:
  $$\begin{aligned}(x, y), (y, z) \in S &\implies (x, y), (y, z) \in R \\ &\implies (x, z) \in R \\ &\implies (x, z) \in S\end{aligned}$$
  So S is transitive.

So the restriction of R to B is a partial order relation.

Problem #4

Suppose R is a partial order on A. Prove that R^{-1} is also a partial order on A.

Solution

- Reflexive
  For all $x \in A$, $(x, x) \in R \implies (x, x) \in R^{-1}$
- Antisymmetric
  For any $x, y \in A$ such that $x \neq y$
  $$(x, y) \in R \implies (y, x) \in R^{-1}$$
  and
  $$\begin{aligned}(x, y) \in R &\implies (y, x) \notin R \\ &\implies (x, y) \notin R^{-1}\end{aligned}$$
- Transitive
  For all $x, y, z \in A$ such that $(x, y), (y, z) \in R^{-1}$.
  $$\begin{aligned}(x, y), (y, z) \in R^{-1} &\implies (y, x), (z, y) \in R \\ &\implies (z, x) \in R \\ &\implies (x, z) \in R^{-1}\end{aligned}$$

So R^{-1} is a partial order on A.

Problem #5

In each case, say whether or not R is a partial order on A. If it is explain why and if not explain why not.

(a) $A =$ the set of all words in English,

$R = \{(x, y) \in A \times A |$ the word y occurs at least as late in alphabetical order as the word $x.\}$

(b) A is the same as above and
$R = \{(x, y) \in A \times A \mid$ The first letter of the word y occurs at least as late in the alphabet as the first letter of the word $x\}$

Solution

Part (a)

The relation is a partial order on A. It is reflexive, antisymmetric, and transitive.

Part (b)

The relation is not a partial order on A. It is reflexive and transitive but not antisymmetric. For example, ("cat", "crab")$\in R$ and ("crab", "cat)$\in R$ and "cat"$\neq$"crab".

Problem #6

For any sets A, B, C, and D, if $A \times B \subseteq C \times D$ then $A \subseteq C$ and $B \subseteq D$. Is the following proof correct? If so, what proof strategies does it use? If not, can it be fixed? Is the theorem correct?

Proof. Suppose $A \times B \subseteq C \times D$. Let a be an arbitrary element of A and let b be an arbitrary element of B. Then $(a, b) \in A \times B$. Since $A \times B \subseteq C \times D$, $(a, b) \in C \times D$. Therefore $a \in C$ and $b \in D$. Since a and b were arbitrary elements of A and B respectively, this shows that $A \subseteq C$ and $B \subseteq D$.

Solution

The proof is not correct. If B and C are empty then $A \times B \subseteq C \times D$ and it is not necessarily the case that $A \subseteq C$. The proof can be made correct by adding the qualification that the sets A, B, C, and D are not empty.

Problem #7

Let $p = 7$ and $q = 13$ and $e = 5$, using RSA Encryption, encrypt the following message and decrypt it to prove you get the same message back. The message is "I♥MATH", use the Caesar cipher for the letters (A=1, B=2,. . . , Z=26) and let ♥ =27. You can use a calculator but you must show where the numbers come from.

Solution

The multiplicative inverse of 5 mod (6)(13) is 29. Then with I=9, ♥=27, M=13, A=1, T=20, and H=8 and using the encryption function encrypt(T) = (T^e) mod pq we have: encrypt(I) = 81, encrypt(♥) = 27, encrypt(M) = 13, encrypt(A) = 1, encrypt(T)=76, and encrypt(H)=8.

Then using the decrpytion function decrypt(C) = C^D mod PQ we have: decrypt(81) = I, encrypt(27) = ♥, encrypt(13) = M, encrypt(1) = A, encrypt(76)=T, and encrypt(8)=H, the original message.