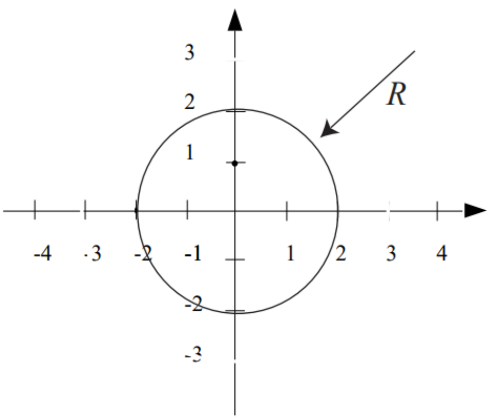
Task 2 Note you will need the Whiteboard to answer this and you can add lines and shapes easily to it.

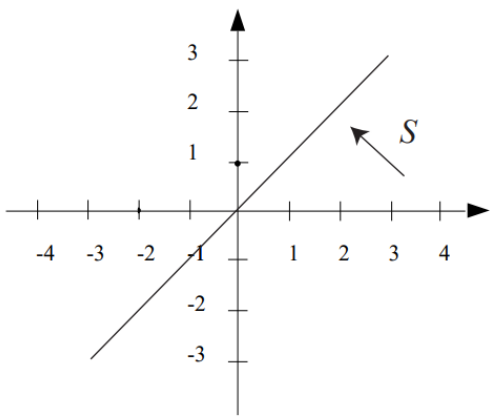
Define relations R and S on $\mathbf{R}$ as follows:

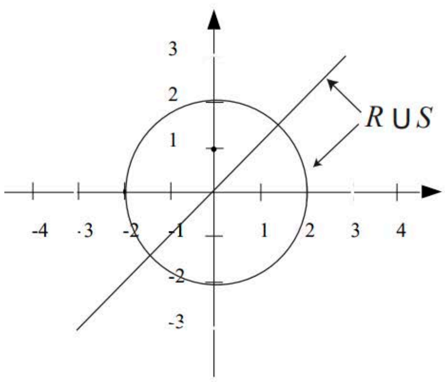
$$R = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid x^2 + y^2 = 4\} \quad \text{and}$$
$$S = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid x = y\}.$$

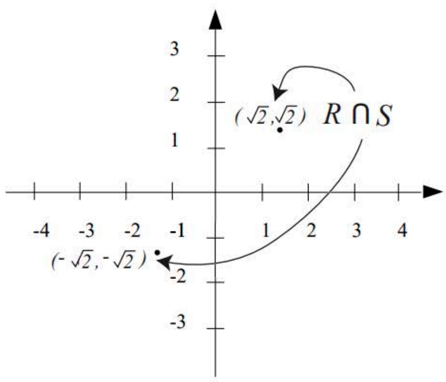
Graph R, S, $R \cup S$, and $R \cap S$ in the Cartesian plane.

Answer







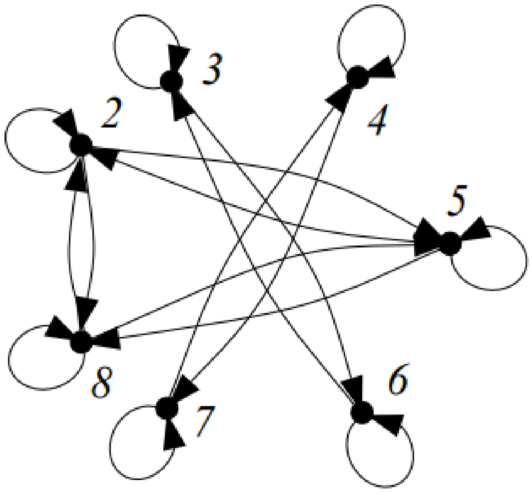


Task 3

Draw a directed graph of this relation

Let $A = \{2, 3, 4, 5, 6, 7, 8\}$ and define a relation T on A as follows: For every $x, y \in A$,

$$x\,T\,y \quad \Leftrightarrow \quad 3 \mid (x - y).$$



Discuss what properties of the relation you can see on the graph?

Ans: You can see all of reflective, symmetric and transitive relations are satisfied.

Task 4

Recall that a prime number is an integer that is greater than 1 and has no positive integer divisors other than 1 and itself. (In particular, 1 is not prime.) A relation P is defined on $\mathbf{Z}$ as follows: For every $m, n \in \mathbf{Z}$, $m\,P\,n \Leftrightarrow \exists$ a prime number p such that $p \mid m$ and $p \mid n$.

Determine if this relation is reflexive. symmetric, transitive or none of these and justify your answer.

P is not reflexive: P is reflexive $\Leftrightarrow$ for every integer n, $n\ P\ n$. By definition of P this means that for every integer n, $\exists$ a prime number p such that $p \mid n$ and $p \mid n$. This is false. As a counterexample, take $n = 1$. There is no prime number that divides 1.

P is symmetric: *[We must show that for all integers m and n, if $m\ P\ n$ then $n\ P\ m$.]* Suppose m and n are integers such that $m\ P\ n$. By definition of P this means that there exists a prime number p such that $p \mid m$ and $p \mid n$. But to say that "$p \mid m$ and $p \mid n$" is logically equivalent to saying that "$p \mid n$ and $p \mid m$." Hence there exists a prime number p such that $p \mid n$ and $p \mid m$, and so by definition of P, $n\ P\ m$.

P is not transitive: P is transitive $\Leftrightarrow$ for all integers m, n, and p, if $m\ P\ n$ and $n\ P\ p$ then $m\ P\ p$. This is false. As a counterexample, take $m = 2$, $n = 6$, and $p = 9$. Then $m\ P\ n$ because the prime number 2 divides both 2 and 6 and $n\ P\ p$ because the prime number 3 divides both 6 and 9, but m is not related to p by P because the numbers 2 and 9 have no common prime factor.

Task 5

a) Use the RSA cipher from Examples 8.4.9 and 8.4.10 to encrypt this word

HELLO b) Now decrypt 13 20 20 09

a)

The letters in HELLO translate numerically into 08, 05, 12, 12, and 15. By Example 8.4.9, the H is encrypted as 17. To encrypt E, we compute 5^3 *mod* $55 = 15$. To encrypt L, we compute 12^3 *mod* $55 = 23$. And to encrypt O, we compute 15^3 *mod* $55 = 20$. Thus the ciphertext is 17 15 23 23 20. (In practice, individual letters of the alphabet are grouped together in blocks during encryption so that deciphering cannot be accomplished through knowledge of frequency patterns of letters or words.)

b)

By Example 8.4.10, the decryption key is 27. Thus the residues modulo 55 for 13^{27}, 20^{27}, and 9^{27} must be found and then translated into letters of the alphabet.

Because $27 = 16 + 8 + 2 + 1$, we first perform the following computations:

$13^1 \equiv 13 \pmod{55}$	$20^1 \equiv 20 \pmod{55}$	$9^1 \equiv 9 \pmod{55}$
$13^2 \equiv 4 \pmod{55}$	$20^2 \equiv 15 \pmod{55}$	$9^2 \equiv 26 \pmod{55}$
$13^4 \equiv 4^2 \equiv 16 \pmod{55}$	$20^4 \equiv 15^2 \equiv 5 \pmod{55}$	$9^4 \equiv 26^2 \equiv 16 \pmod{55}$
$13^8 \equiv 16^2 \equiv 36 \pmod{55}$	$20^8 \equiv 25^2 \equiv 5 \pmod{55}$	$9^8 \equiv 16^2 \equiv 36 \pmod{55}$
$13^{16} \equiv 36^2 \equiv 31 \pmod{55}$	$20^{16} \equiv 25^2 \equiv 20 \pmod{55}$	$9^{16} \equiv 36^2 \equiv 31 \pmod{55}$

Then we compute

13^{27} *mod* $55 = (31 \cdot 36 \cdot 4 \cdot 13)$ *mod* $55 = 7$,

20^{27} *mod* $55 = (20 \cdot 25 \cdot 15 \cdot 20)$ *mod* $55 = 15$,

9^{27} *mod* $55 = (31 \cdot 36 \cdot 26 \cdot 9)$ *mod* $55 = 4$.

Finally, because 7, 15, and 4 translate into letters as G, O, and D, we see that the message is GOOD.

Task 6

Use Theorem 8.4.5 to prove that for all integers a, b, and c, if $\gcd(a, b) = 1$ and $a \mid c$ and $b \mid c$, then $ab \mid c$.

. Proof: Suppose a, b, and c are integers such that $\gcd(a,b) = 1$, $a \mid c$, and $b \mid c$. We will show that $ab \mid c$.

By Corollary 8.4.6 (or by Theorem 8.4.5), there exist integers s and t such that $as + bt = 1$.

Also, by definition of divisibility, $c = au = bv$, for some integers u and v. Hence, by substitution,

$$c = asc + btc = as(bv) + bt(au) = ab(sv + tu).$$

But $sv + tu$ is an integer, and so, by definition of divisibility, $ab \mid c$ *[as was to be shown]*.

Task 7

According to Fermat's Little Theorem, if p is a prime number and a and p are relatively prime, then $a^{p-1} \equiv 1\ (mod\ p)$. Verify that this theorem gives correct results for the following:

a) $a = 15$ and $p = 7$ b) $a = 8$ and $p = 11$

a. When $a = 15$ and $p = 7$,

$$a^{p-1} = 15^6 = 11390625 \equiv 1 \pmod 7 \text{ because } 11390625 - 1 = 7 \cdot 1627232.$$

b. When $a = 8$ and $p = 11$,

$$a^{p-1} = 8^{10} = 1073741824 \equiv 1 (\text{mod}\, 11) \text{ because } 1073741824 - 1 = 11 \cdot 97612893.$$