Question on Hmk.: $S = \{(a,b) \in \mathbb{Z}^2 : 1 \leq a < 5,\ b^2 = (a-1)^2\}$ is a relation on $\mathbb{Z}$.

$b^2 = (a-1)^2 \Leftrightarrow b = \pm(a-1)$

Draw corresponding directed graph.

$S = \{(1,0), (2,1), (2,-1), (3,2), (3,-2), (4,3), (4,-3)\}$

Applications of Equivalence Relations.

① Image processing — i.e. identifying shapes.

We want to say that two shapes are equivalent if

① • The two shapes can be rotated so that they coincide

or ② • One shape can be rescaled so that it matches the other.

or ③ • One shape can be translated (moved without rotating) so that it coincides with the other

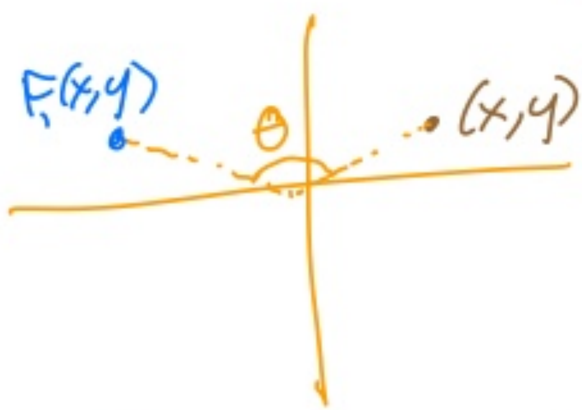
or • Some combination of those 3 things.

example

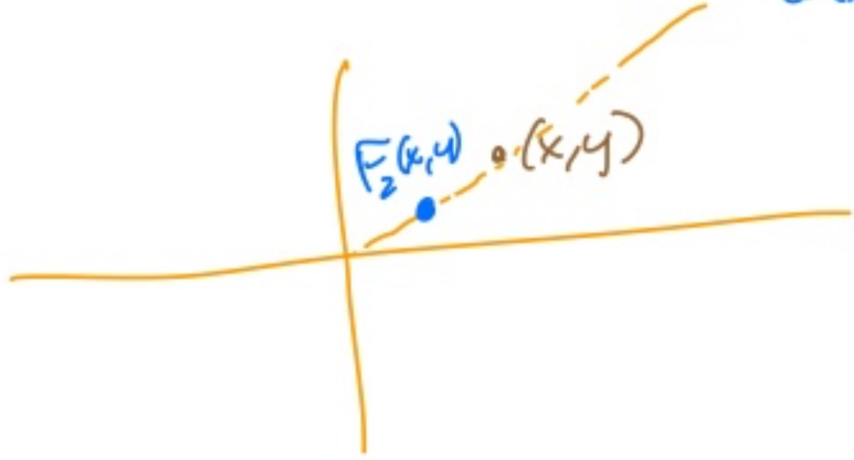
These should be considered equivalent.

We can say that one set is a set in $\mathbb{R}^2$, and the 3 kinds of operations on the sets are

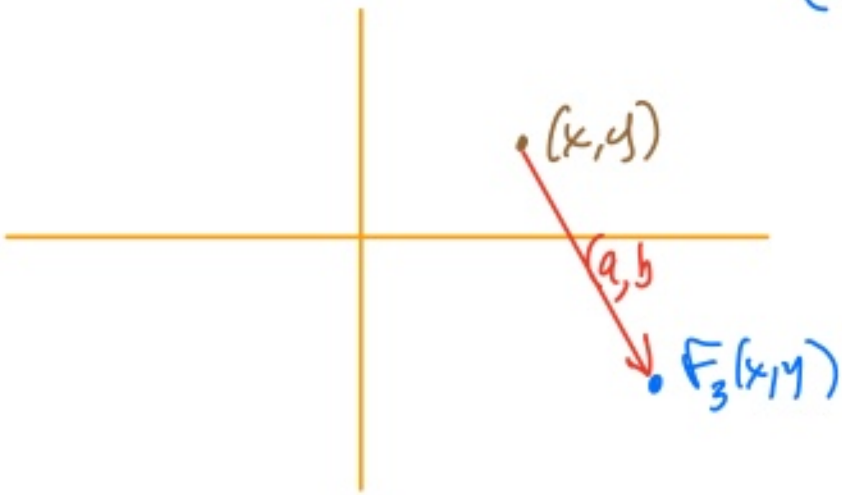
① $F_1(x,y) = (x\cos\theta - y\sin\theta, x\sin\theta + y\cos\theta)$



② $F_2(x,y) = (cx, cy)$ for some constant $c > 0$



(3) $F_3(x,y) = (x+a, y+b)$ for some $(a,b) \in \mathbb{R}^2$



Application 2 Modular Arithmetic → Encryption RSA algorithm.

Euler's Theorem Let $\varphi(n)$ = # of positive integers $< n$ that are relatively prime to n. Then for any positive integer k that is relatively prime to n, $\underbrace{k^{\varphi(n)} \equiv 1 \bmod n}$.

(ie $k^{\varphi(n)} - 1$ has a factor of n)

Eg: If $n = 28$, the pos. integers relatively prime to n are

$$\{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\}$$

$$\varphi(n) = 12$$

Let pick $k = 5$

Let's calculate $5^{12} \bmod 28$

$$5^2 = 25 = -3 \bmod 28$$

$$5^4 = (-3)^2 = 9 \bmod 28$$

$$5^{12} = 5^4 \cdot 5^4 \cdot 5^4 = 9 \cdot 9 \cdot 9 \bmod 28$$

$$= 81 \cdot 9 \bmod 28 = (-3) \cdot 9 \bmod 28$$

$$28 \cdot 3 = 84$$

$$= -27 \bmod 28$$

$$= 1 \bmod 28. \checkmark$$

<u>Proof of Euler's Theorem:</u> Let $\{a_1, \dots, a_{\varphi(n)}\}$ be the positive integers relatively prime to n. If you multiply any of them together, you get another integer in this set (at least mod n). Let x be one of these integers. Then note that

$$x a_j = x a_k \mod n$$

$$\Rightarrow x(a_j - a_k) \equiv 0 \mod n$$

$\Rightarrow (a_j - a_k) \equiv 0 \mod n$ (since x is relatively prime to n.)

$\Rightarrow a_j \equiv a_k \mod n$

$\Rightarrow j = k.$

Thus $\{x a_j\}_{1 \le j \le 28} = \{a_j\}_{1 \le j \le 28}$

Then the product

$$(x a_1)(x a_2) \cdots (x a_{\varphi(n)}) = a_1 a_2 \cdots a_{\varphi(n)} \mod n$$

$$\Rightarrow x^{\varphi(n)} \underbrace{a_1 a_2 \cdots a_{\varphi(n)}}_{\text{relatively prime to } n} = \underbrace{a_1 a_2 \cdots a_{\varphi(n)}}_{} \mod n$$

$$\Rightarrow \left(x^{\varphi(n)} - 1\right)\left(a_1 a_2 \cdots a_{\varphi(n)}\right) \equiv 0 \mod (n)$$

$\Rightarrow x^{\varphi(n)} - 1$ is a multiple of n

$$\Rightarrow x^{\varphi(n)} \equiv 1 \mod n. \quad \blacksquare$$