

## Chapter 4: Euclid's Algorithm

**Exercise 4.4** Prove that, for any odd square number  $x$ , there is an even square number  $y$  such that  $x + y$  is a square number.

*Proof.* Since  $x$  is square and odd, there must be an  $n \in \mathbb{N}$  such that  $x = (2n + 1)^2$ . Let  $y$  be some even square number. Thus, there must be an  $m \in \mathbb{N}$  such that  $y = (2m)^2$ . It follows that

$$\begin{aligned}x + y &= (2n + 1)^2 + (2m)^2 \\ &= 4(n^2 + m^2) + 4n + 1\end{aligned}$$

We must define  $m$  as a function of  $n$  in such a way that this number conforms a square. In order to do this, let's see what happens for some small cases:

- If  $n = 1$ , then  $x = 9$ . If we set  $m = 2$ ,  $y = 16$  and  $x + y = 25$ , which is a square.
- If  $n = 2$ , then  $x = 25$ . Taking  $m = 6$ ,  $y = 144$  and  $x + y = 169$ , which is a square (since  $13^2 = 169$ ).
- If  $n = 3$ , then  $x = 49$ . Now,  $m$  can be 12, and then  $y = 576$  and  $x + y = 625 = 25^2$ .

A careful analysis of these cases reveals a pattern:  $m = n^2 + n$ . Substituting this in the equation shown before,

$$\begin{aligned}x + y &= 4(n^2 + m^2) + 4n + 1 \\ &= 4(n^2 + (n^2 + n)^2) + 4n + 1 \\ &= 4n^2 + 4(n^2 + n)^2 + 4n + 1 \\ &= 4(n^2 + n)^2 + 4(n^2 + n) + 1 \\ &= (2(n^2 + n) + 1)^2\end{aligned}$$

□

**Exercise 4.5** Prove that, if  $x$  and  $y$  are both sums of two squares, then so is their product  $xy$ .

*Proof.* Being  $x$  and  $y$  both sums of two squares, we can write them like so:

$$\begin{aligned}x &= x_1^2 + x_2^2 \\ y &= y_1^2 + y_2^2\end{aligned}$$

This implies that

$$\begin{aligned}xy &= (x_1^2 + x_2^2)(y_1^2 + y_2^2) \\ &= x_1^2 y_1^2 + x_1^2 y_2^2 + x_2^2 y_1^2 + x_2^2 y_2^2\end{aligned}$$

After several failed attempts at completing the squares (i.e., adding and subtracting the same thing), the following Python script was used to gain some insight into the underlying pattern of  $xy$ :

```
def find_squares(x, y):
    x1, x2 = x
    y1, y2 = y
    n = (x1**2 + x2**2)*(y1**2 + y2**2)
    return [(i,j) for i in xrange(n)
            for j in xrange(i,n)
            if n == i**2 + j**2]
```

For example,

- `find_squares((2,3), (5,7))` → `[(1, 31), (11, 29)]`.
- `find_squares((1,2), (3,4))` → `[(2, 11), (5, 10)]`.

Playing with this script and guessing how to combine the elements in the input tuples in order to generate an output tuple  $(z_1, z_2)$ , the following pattern emerged:

$$\begin{aligned} z_1 &= x_2 y_1 + x_1 y_2 \\ z_2 &= x_2 y_2 - x_1 y_1 \end{aligned}$$

Indeed,

$$\begin{aligned} z_1^2 + z_2^2 &= (x_2 y_1 + x_1 y_2)^2 + (x_2 y_2 - x_1 y_1)^2 \\ &= ((x_2 y_1)^2 + (x_1 y_2)^2 + 2x_2 y_1 x_1 y_2) + ((x_2 y_2)^2 + (x_1 y_1)^2 - 2x_2 y_2 x_1 y_1) \\ &= x_2^2 y_1^2 + x_1^2 y_2^2 + x_2^2 y_2^2 + x_1^2 y_1^2 \\ &= x_1^2 y_1^2 + x_1^2 y_2^2 + x_2^2 y_1^2 + x_2^2 y_2^2 \\ &= xy \end{aligned}$$

□

## Chapter 11: Permutation Algorithms

**Exercise 11.1** Prove *Cayley's theorem*: Any group  $G$  is isomorphic to a subgroup of the symmetric group on  $G$ ,  $\text{Sym}(G)$ .

*Proof.* For any  $a \in G$ , consider the following function  $F_a : G \rightarrow G$ :

$$F_a(x) = ax$$

- $F_a$  is one-to-one, since  $F_a(x) = ax = ay = F_a(y)$  implies that  $x = y$  (left multiplying by  $a^{-1}$ ).
- $F_a$  is onto: for a given  $y \in G$ ,  $F_a(a^{-1}y) = a(a^{-1}y) = (aa^{-1})y = y$ .

Thus,  $F_a$  is a bijection on  $G$ , which in turn means that  $F_a$  is a permutation of the elements in  $G$ . Thus,  $S = \{F_a / a \in G\}$  is a subset of  $\text{Sym}(G)$ . Moreover,  $S$  is a subgroup of  $\text{Sym}(G)$ :

- $S$  contains the identity permutation:  $F_{e_G}(x) = e_G x = x$ .
- $S$  is closed by composition:  $(F_a \circ F_b)(x) = F_a(F_b(x)) = a(bx) = (ab)x = F_{ab}(x)$ .
- $S$  is closed by inverses:  $F_a^{-1} = F_{a^{-1}}$ , since  $(F_a \circ F_{a^{-1}})(x) = a(a^{-1}x) = x$ .

Let  $\mathcal{F} : G \rightarrow S$  be a function defined as follows:

$$\mathcal{F}(a) = F_a$$

Then,  $\mathcal{F}$  is a group isomorphism from  $G$  to  $S$ :

- $\mathcal{F}(ab) = F_{ab} = F_a \circ F_b = \mathcal{F}(a) \circ \mathcal{F}(b)$ , using that  $S$  is closed by composition.
- $\mathcal{F}$  is one-to-one, since  $\mathcal{F}(a) = \mathcal{F}(b)$  implies that  $F_a(x) = ax = bx = F_b(x)$ , and so  $a = b$  after right multiplying by  $x^{-1}$ .
- $\mathcal{F}$  is onto, since for a given  $F_a \in S$ ,  $\mathcal{F}(a) = F_a$ .

□

**Exercise 11.2** What is the order of  $S_n$ ?

*Answer.*  $S_n$  contains every permutation of  $\{1, \dots, n\}$ . Since there are  $n!$  of them, the order of  $S_n$  is  $n!$ . □

**Exercise 11.3** Prove that, if  $n > 2$ ,  $S_n$  is not abelian.

*Proof.* Let  $P_1 = (213 \dots n)$  and let  $P_2 = (312 \dots n)$ . Then,

- $P_1 \circ P_2 = (132 \dots n)$ , and
- $P_2 \circ P_1 = (321 \dots n)$ .

Since  $P_1 \circ P_2 \neq P_2 \circ P_1$ ,  $S_n$  is not commutative.

□