

1 SMA0180 - Matemática Discreta I: Entrega de Trabalho 5

Nome: Rafael Zimmer; nUsp: 12542612 Data: 24/10/2021

2 Algoritmo de Euclides

```
1 input_size gcd_extended(input_size divisor, input_size dividend,
2                           input_size *i, input_size *j, int spacing)
3 {
4     for (int i = 0; i < spacing; i++) { printf(" "); }
5     if (spacing != 0) {
6         printf("    - Iteracao %d -> Dividendo: %ld; Divisor: %ld\n", spacing, dividend, divisor);
7     }
8
9     input_size i_temporary, j_temporary;
10
11     // Caso base da funcao recursiva,
12     // retorna o ultimo dividendo quando o divisor e 0 (Resto anterior foi 0)
13     if (divisor == 0) {
14         *i = 0;
15         *j = 1;
16
17         for (int i = 0; i < spacing; i++) { printf(" "); }
18         printf(" => Maior divisor em comum: %ld\n", dividend);
19         return dividend;
20     }
21
22     input_size modulo = dividend % divisor;
23     input_size recursive_extended = gcd_extended(modulo, divisor, &i_temporary, &j_temporary, spacing + 1);
24
25     // Pela equacao dividendo * i + divisor * j = 1,
26     // e poss vel atribuir a i e j valores a medida que
27     // a funcao recursiva e retornada
28     *i = j_temporary - (dividend / divisor) * i_temporary;
29     *j = i_temporary;
30
31     return recursive_extended;
32 }
```

3 Casos Teste

```
1 gcc -o main main.c
2 ./main 169 144
3
4 -----
5
6 Chamada do Algoritmo de Euclides:
7
8     - Iteracao 2 -> Dividendo: 169; Divisor: 144
9     - Iteracao 3 -> Dividendo: 144; Divisor: 25
10    - Iteracao 4 -> Dividendo: 25; Divisor: 19
11      - Iteracao 5 -> Dividendo: 19; Divisor: 6
12        - Iteracao 6 -> Dividendo: 6; Divisor: 1
13          - Iteracao 7 -> Dividendo: 1; Divisor: 0
14            => Maior divisor em comum: 1
15
16 -----
17
18 o inverso de 144 em Z_169 e 27
```

```

1 gcc -o main main.c
2 ./main 12542612 1973
3
4 -----
5
6 Chamada do Algoritmo de Euclides:
7
8   - Iteracao 1 -> Dividendo: 12542612; Divisor: 1973
9   - Iteracao 2 -> Dividendo: 1973; Divisor: 251
10  - Iteracao 3 -> Dividendo: 251; Divisor: 216
11  - Iteracao 4 -> Dividendo: 216; Divisor: 35
12  - Iteracao 5 -> Dividendo: 35; Divisor: 6
13  - Iteracao 6 -> Dividendo: 6; Divisor: 5
14  - Iteracao 7 -> Dividendo: 5; Divisor: 1
15  - Iteracao 8 -> Dividendo: 1; Divisor: 0
16  => Maior divisor em comum: 1
17
18 -----
19
20 o inverso de 1973 em  $Z_{12542612}$  e 2148709

```

3.1 Caso Extra

```

1 gcc -o main main.c
2 ./main 173 13
3
4 -----
5
6 Chamada do Algoritmo de Euclides:
7
8   - Iteracao 1 -> Dividendo: 173; Divisor: 13
9   - Iteracao 2 -> Dividendo: 13; Divisor: 4
10  - Iteracao 3 -> Dividendo: 4; Divisor: 1
11  - Iteracao 4 -> Dividendo: 1; Divisor: 0
12  => Maior divisor em comum: 1
13
14 -----
15
16 o inverso de 13 em  $Z_{173}$  e 40

```