# Criptografia para Segurança de Dados
# Gabarito da Lista 1

**Thales Paiva**
thalespaiva@gmail.com

29/04/2014

## Sumário

# 1 Exercício 1

Escrever todos os valores de $i$, $u_i$, $v_i$, $a_i$ e $b_i$ quando o Algoritmo de Euclides Estendido é aplicado com entrada $(3540, 714)$.

**Resolução:** A tabela abaixo mostra a execução do algoritmo com os parâmetros pedidos. Note que os valores de $a_i$ e $b_i$ estão relacionados aos de $x_{i-2}$ e $x_{i-1}$.

| $i$ | $x_{i-2}$ | $x_{i-1}$ | $q_i$ | $x_i \leftarrow x_{i-2} \bmod x_{i-1}$ | $u_i$ | $v_i$ |
|---|---|---|---|---|---|---|
| -2 | | | | | 1 | 0 |
| -1 | | | | | 0 | 1 |
| 0 | 3540 | 714 | 4 | 684 | 1 | -4 |
| 1 | 714 | 684 | 1 | 30 | -1 | 5 |
| 2 | 684 | 30 | 22 | 24 | 23 | -114 |
| 3 | 30 | 24 | 1 | 6 | **-24** | **119** |
| 4 | 24 | 6 | 4 | 0 | 119 | -590 |
| 5 | 6 | 0 | | | | |

# 2 Exercício 2

Utilizando o Algoritmo de Euclides estendido (pg. 244 do livro) calcular $3541^{-1} \bmod 119$.

**Resolução:** Note que $3541^{-1} \bmod 119$ existe se e somente se $mdc(3541, 119) = 1$. Ainda, se este for o caso, o Algoritmo de Euclides Estendido aplicado a $(3541, 119)$ calculará $u, v \in \mathbb{Z}$ tais que:

$$3541u + 119v = 1 \Rightarrow 3541u = 1 \bmod 119 \Rightarrow u = 3541^{-1} \bmod 119$$

A tabela abaixo mostra a aplicação do Algoritmo de Euclides Estendido aplicado a $(3541, 119)$:

Como $3541 \times 41 + 119 \times (-1220) = 1$, temos que $3541^{-1} \bmod 119 = 41$.

| $i$ | $x_{i-2}$ | $x_{i-1}$ | $q_i$ | $x_i \leftarrow x_{i-2} \bmod x_{i-1}$ | $u_i$ | $v_i$ |
|---|---|---|---|---|---|---|
| -2 | | | | | 1 | 0 |
| -1 | | | | | 0 | 1 |
| 0 | 3541 | 119 | 29 | 90 | 1 | -29 |
| 1 | 119 | 90 | 1 | 29 | -1 | 30 |
| 2 | 90 | 29 | 3 | 3 | 4 | -119 |
| 3 | 29 | 3 | 9 | 2 | -37 | 1101 |
| 4 | 3 | 2 | 1 | 1 | **41** | **-1220** |
| 5 | 2 | 1 | 2 | 0 | | |

# 3 Exercício 3

Dado que $N = 8 \bmod 17$ e $N = 4 \bmod 31$, utilizando o Teorema Chinês do Resto (pg. 247 do livro) calcular $N \bmod (17 \times 31)$.

**Resolução:** Pela aplicação do Algoritmo de Euclides Estendido, temos que:

$$1 = mdc(17, 31) = 11 \times 17 + (-6) \times 31$$

Pelo Teorema Chinês do Resto, temos que:

$$N = 4 \times 11 \times 17 + 8 \times (-6) \times 31 = -740 \bmod (17 \times 31)$$

Fazendo a redução a $\mathbb{Z}_{17\times31} = \mathbb{Z}_{527}, temos$ :

$$N = -740 = -213 = 314 \bmod (17 \times 31)$$

# 4 Exercício 4

Relacionado ao Algoritmo RSA, dadas a fatoração de $n = qr = 17 \times 31$ e a chave pública p = 433, calcular a chave particular $s$ utilizando as fórmulas $\Phi(qr) = (q-1)(r-1)$ e $s = p^{-1} \bmod \Phi(qr)$ (pg. 128 do livro).

**Resolução:** Do enunciado:

$s = 433^{-1} \bmod \Phi(17 \times 31) = 433^{-1} \bmod (16 \times 30) = 433^{-1} \bmod 480$

Pelo algoritmo de Euclides Estendido aplicado a $(433, 480)$, temos que:

$$(-143) \times 433 + 129 \times 480 = 1 \Rightarrow -143 = 433^{-1} \bmod 480$$

Reduzindo -143 a $\mathbb{Z}_{480}$, temos:

$$-143 = 337 \bmod 480$$