APÊNDICE A

ALGORITMOS DE OPERAÇÕES ARITMÉTICAS

A.1 - EP1 - Elemento Processador de 1 *Bit*

A.1.1 - Soma de Inteiros

$C = 0$
para i variando de 0 até $n - 1$
    $A = x_i$
    $B = y_i$
    $(C, z_i) = A + B + C$

Número de ciclos necessários para a soma: $3n + 1$.

A.1.2 - Subtração de Inteiros

$C = 1$
para i variando de 0 até $n - 1$
    $A = x_i$
    $B = y_i$
    $(C, z_i) = A + \overline{B} + C$

Número de ciclos necessários para a subtração: $3n + 1$.

A.1.3 - Multiplicação de Inteiros

$K = y_0$

para i variando de 0 até $n-1$
  $B = x_i$
  $p_i = B \; and \; K$

$p_n = B \; and \; K$

para j variando de 1 até $n-2$
  $K = y_j, C = 0$

  para i variando de 0 até $n-1$
    $A = p_{i+j}$
    $B = x_i$
    $(C, p_{i+j}) = A + B \; and \; K + C$

  $p_{j+n} = A + B \; and \; K + C$

$C = 1, K = y_{n-1}$

para i variando de 0 até $n-1$
  $A = p_{i+n-1}$
  $B = x_i$
  $(C, p_{i+n-1}) = A + B \; nand \; K + C$

$p_{2n-1} = A + B \; nand \; K + C$

Número de ciclos necessários para a multiplicação: $3n^2 + n$ ciclos.

A.1.4 - Divisão de Inteiros

$A = K = x_{n-1}, C = 0$
$B = x_0$
$(C, z_0) = A + B\ xor\ K + C$

para i variando de 1 até $n-2$
    $B = x_i$
    $(C, z_i) = 0 + B\ xor\ K + C$
$A = 0 + 0 + C$
$K = y_{n-1}, C = 1$
$B = y_0, (C,) = 0 + K + C$
$(C, r_0) = 0 + B\ xor\ K + C$

para i variando de 1 até $n-2$
    $B = y_i$
    $(C, r_i) = 0 + B\ xor\ K + C$
$r_{n-1} = 0 + 0 + C$
$B = x_{n-1}$
$q_n = B\ xor\ K$
$B = r_0, C = 1$
$(C, z_{n-1}) = A + \overline{B} + C$

para i variando de 1 até $n-2$
    $B = r_i$
    $(C, z_{i+n-1}) = 0 + \overline{B} + C$
$B = r_{n-1}$
$q_{n-1} = K = 0 + B + C$

para j variando de 2 até n
    $A = z_{n-j}, C = 1$
    $B = r_0, (C,) = 0 + K + C$
    $(C, z_{n-j}) = A + B\ xor\ K + C$

    para i variando de 1 até $n-2$
        $A = z_{i+n-j}$
        $B = r_i$
        $(C, z_{i+n-j}) = A + B\ xor\ K + C$
    $A = z_{2n-1-j}$
    $B = r_{n-1}$
    $q_{n-j} = K = A + \overline{B}\ xor\ K + C$
$z_{n-1} = \overline{K}, C = 0$

para i variando de 0 até $n-1$
    $A = z_i$
    $B = r_i$
    $(C, z_i) = A + B\ and\ \overline{K} + C$
$K = x_{n-1}, C = 1$
$B = z_0, (C,) = 0 + K + C$
$(C, r_0) = 0 + B\ xor\ K + C$

para i variando de 1 até $n-1$
    $B = z_i$
    $(C, r_i) = 0 + B\ xor\ K + C$

$K = q_n, C = 1$
$B = q_0, (C,) = 0 + K + C$
$(C, q_0) = 0 + B\ xor\ K + C$

para i variando de 1 até $n-1$
    $B = q_i$
    $(C, q_i) = 0 + B\ xor\ K + C$

$q_n = 0 + K + C$

Número de ciclos necessários para a multiplicação: $3n^2 + 10n + 6$ ciclos.

A.2 - EP1SH - Elemento Processador de 1 *Bit* com Registrador de Deslocamento Programável

A.2.1 - Soma de Inteiros

$C = 0$
para i variando de 0 até $n - 1$
    $A = x_i$
    $B = y_i$
    $(C, z_i) = A + B + C$

Número de ciclos necessários para a soma: $3n + 1$.

A.2.2 - Subtração de Inteiros

$C = 1$
para i variando de 0 até $n - 1$
    $A = x_i$
    $B = y_i$
    $(C, z_i) = A + \overline{B} + C$

Número de ciclos necessários para a subtração: $3n + 1$.

A.2.3 - Multiplicação de Inteiros

$C = 0, K = y_0$
$B = x_0$ *and* K
$p_0 = B$
$B = x_1$ *and* K

para i variando de 2 até $n - 1$
    $D = 0 + B + C, SH = SH$ *shift right* $1, B = x_i$ *and* K
$D = 0 + B + C, SH = SH$ *shift right* $1, K = y_1$
$D = 0 + B + C, SH = SH$ *shift right* $1, A = SH_0, B = x_0$ *and* $K, C = 0$

para j variando de 1 até $n - 3$
    $(C, p_j = D) = A + B + C, SH = SH$ *shift right* $1, A = SH_0$
    $B = x_1$ *and* K

    para i variando de 2 até $n - 1$
        $(C, D) = A + B + C, SH = SH$ *shift right* $1, A = SH_0, B = x_i$ *and* K
    $(C, D) = A + B + C, SH = SH$ *shift right* $1, K = y_{i+1}$
    $D = A + B + C, SH = SH$ *shift right* $1, A = SH_0, B = x_0$ *and* $K, C = 0$
$(C, p_{n-2} = D) = A + B + C, SH = SH$ *shift right* $1, A = SH_0$
$B = x_1$ *and* K

para i variando de 2 até $n - 1$
    $(C, D) = A + B + C, SH = SH$ *shift right* $1, A = SH_0, B = x_i$ *and* K
$(C, D) = A + B + C, SH = SH$ *shift right* $1, K = y_{n-1}$
$D = A + B + C, SH = SH$ *shift right* $1, A = SH_0, B = x_0$ *and* $K, C = 1$

para i variando de 1 até $n - 1$
    $(C, p_{i+n-2} = D) = A + B + C, SH = SH$ *shift right* $1, A = SH_0$
    $B = x_i$ *nand* K
$(C, p_{2n-2}) = A + B + C$
$p_{2n-1} = A + B + C$

Número de ciclos necessários para a multiplicação: $n^2 + 3n$ ciclos.

A.2.4 - Divisão de Inteiros

$K = C = x_{n-1}$

para i variando de 0 até $n-2$
    $B = x_i \; xor \; K$
    $(C, q_i) = 0 + B + C, B = 0$
$A = 0 + B + C$
$K = C = y_{n-1}$

para i variando de 0 até $n-2$
    $B = y_i \; xor \; K$
    $(C, r_i) = 0 + B + C, B = 0$
$r_{n-1} = 0 + B + C$
$B = x_{n-1} \; xor \; K, C = 0$
$q_n = 0 + B + C$
$B = \overline{r_0}, C = 1$
$(C, D) = A + B + C, SH = SH \; shift \; right \; 1, B = \overline{r_1}$

para i variando de 2 até $n-2$
    $(C, D) = 0 + B + C, SH = SH \; shift \; right \; 1, B = \overline{r_i}$
$(C, D) = 0 + B + C, SH = SH \; shift \; right \; 1, B = r_{n-1}$
$q_{n-1} = K = C = 0 + B + C$

para j variando de 2 até n
    $A = q_{n-j}$
    $B = r_0 \; xor \; K$

    para i variando de 1 até $n-2$
        $(C, D) = A + B + C, SH = SH \; shift \; right \; 1, B = r_i \; xor \; K$
    $(C, D) = A + B + C, SH = SH \; shift \; right \; 1, B = \overline{r_{n-1}} \; xor \; K$
    $q_{n-j} = K = C = A + B + C, B = \overline{(A + B + C)}$
$C = 0$
$D = 0 + B + C, SH = SH \; shift \; right \; 1, B = r_0 \; and \; \overline{K}$

para i variando de 1 até $n-1$
    $(C, D) = A + B + C, SH = SH \; shift \; right \; 1, B = r_i \; and \; \overline{K}$
$D = A + B + C, SH = SH \; shift \; right \; 1, K = C = x_{n-1}$
$B = A \; xor \; K, SH = SH \; shift \; right \; 1$

para i variando de 0 até $n-2$
    $(C, r_i) = 0 + B + C, SH = SH \; shift \; right \; 1, B = A \; xor \; K$
$(C, r_{n-1}) = 0 + B + C$
$K = C = q_n$

para i variando de 0 até $n-2$
    $B = q_i \; xor \; K$
    $(C, q_i) = 0 + B + C$
$B = q_{n-1} \; xor \; K$
$(C, q_{n-1}) = 0 + B + C, B = K$
$q_n = 0 + B + C$

Número de ciclos necessários para a divisão: $n^2 + 10n + 6$ ciclos.

A.3 - EP1FIFO - Elemento Processador de 1 *Bit* com FIFO

A.3.1 - Soma de Inteiros

$C = 0$
para i variando de 0 até $n-1$
    $A = x_i$
    $B = y_i$
    $(C, z_i) = A + B + C$

Número de ciclos necessários para a soma: $3n+1$.

A.3.2 - Subtração de Inteiros

$C = 1$
para i variando de 0 até $n-1$
    $A = x_i$
    $B = y_i$
    $(C, z_i) = A + \overline{B} + C$

Número de ciclos necessários para a subtração: $3n+1$.

A.3.3 - Multiplicação de Inteiros

$C = 0, K = y_0, IB = 0$
$B = x_0 \text{ and } K, II = IB, IO = IB$
$p_0 = B$
$B = x_1 \text{ and } K$

para i variando de 2 até $n-1$
    $A[II] = 0 + B + C, B = x_i \text{ and } K, II = II + 1$
$A[II] = 0 + B + C, K = y_1, II = II + 1$
$A[II] = 0 + B + C, B = x_0 \text{ and } K, II = II + 1$

para j variando de 1 até $n-3$
    $(C, p_j) = A[IO] + B + C, IO = IO + 1$
    $B = x_1 \text{ and } K$

    para i variando de 2 até $n-1$
        $(C, A[II]) = A[IO] + B + C, B = x_i \text{ and } K, II = II + 1, IO = IO + 1$
    $(C, A[II]) = A[IO] + B + C, K = y_{j+1}, II = II + 1$
    $A[II] = A[IO] + B + C, B = x_0 \text{ and } K, C = 0, II = II + 1, IO = IO + 1$
$(C, p_{n-2}) = A[IO] + B + C, IO = IO + 1$
$B = x_1 \text{ and } K$

para i variando de 2 até $n-1$
    $(C, A[II]) = A[IO] + B + C, B = x_i \text{ and } K, II = II + 1, IO = IO + 1$
$(C, A[II]) = A[IO] + B + C, K = y_{n-1}, II = II + 1$
$A[II] = A[IO] + B + C, B = x_0 \text{ nand } K, C = 1, II = II + 1, IO = IO + 1$

para i variando de 1 até $n-1$
    $(C, p_{i+n-2}) = A[IO] + B + C, IO = IO + 1$
    $B = x_i \text{ nand } K$
$(C, p_{2n-2}) = A[IO] + B + C$
$p_{2n-1} = A[IO] + B + C$

Número de ciclos necessários para a multiplicação: $n^2 + 3n$ ciclos.

A.3.4 - Divisão de Inteiros

Para $n \leq 16$:

$K = C = x_{n-1}, IB = 0$
$B = x_0 \; xor \; K, II = IB$

para i variando de 1 até $n-1$
  $(C, A[II]) = 0 + B + C, B = x_i \; xor \; K, II = II + 1, IB = IB + 1$
$A[II] = 0 + B + C, IO = IB$
$K = C = y_{n-1}$

para i variando de 0 até $n-2$
  $B = y_i \; xor \; K$
  $(C, r_i) = 0 + B + C, B = 0$
$r_{n-1} = 0 + B + C$
$B = x_{n-1} \; xor \; K$
$q_n = B$
$B = \overline{r_0}, C = 1$
$(C, A[II]) = A[IO] + B + C, B = \overline{r_1}, II = II + 1$

para i variando de 2 até $n-2$
  $(C, A[II]) = 0 + B + C, B = \overline{r_i}, II = II + 1$
$(C, A[II]) = 0 + B + C, B = r_{n-1}, II = II + 1$
$q_{n-1} = A[II] = K = C = 0 + B + C, IB = IB - 1$

para j variando de 2 até n
  $B = r_0 \; xor \; K, II = IB, IO = IB$

  para i variando de 1 até $n-2$
    $(C, A[II]) = A[IO] + B + C, B = r_i \; xor \; K, II = II + 1, IO = IO + 1$
  $(C, A[II]) = A[IO] + B + C, B = \overline{r_{n-1}} \; xor \; K, II = II + 1, IO = IO + 1$
  $q_{n-j} = A[II] = K = C = A[IO] + B + C, B = \overline{(A[IO] + B + C)}, IB = IB - 1$
$A[II] = B, C = 0, IB = IB + 1$
$B = r_0 \; and \; \overline{K}, II = IB, IO = IB$

para i variando de 1 até $n-1$
  $(C, A[II]) = A[IO] + B + C, B = r_i \; and \; \overline{K}, II = II + 1, IO = IO + 1$
$A[II] = A[IO] + B + C, K = C = x_{n-1}, IO = IB$
$B = A[IO] \; xor \; K, IO = IO + 1$

para i variando de 0 até $n-2$
  $(C, r_i) = 0 + B + C, B = A[IO] \; xor \; K, IO = IO + 1$
$(C, r_{n-1}) = 0 + B + C$
$K = C = q_n$
$B = q_0 \; xor \; K$

para i variando de 0 até $n-2$
  $(C, q_i) = 0 + B + C, B = A[IO] \; xor \; K, IO = IO + 1$
$(C, q_{n-1}) = 0 + B + C, B = K$
$q_n = 0 + B + C$

Número de ciclos necessários para a divisão: $n^2 + 7n + 10$ ciclos.

Para $n \leq 32$:

$K = C = x_{n-1}, IB = 0$
$B = x_0 \ xor \ K, II = IB$

para i variando de 1 até $n-1$
    $(C, q_{i-1}) = 0 + B + C$
    $B = x_i \ xor \ K$
$A[II] = 0 + B + C, IO = IB$
$K = C = y_{n-1}$

para i variando de 0 até $n-2$
    $B = y_i \ xor \ K$
    $(C, r_i) = 0 + B + C, B = 0$
$r_{n-1} = 0 + B + C$
$B = x_{n-1} \ xor \ K$
$q_n = \overline{B}$
$B = \overline{r_0}, C = 1$
$(C, A[II]) = A[IO] + B + C, B = \overline{r_1}, II = II + 1$

para i variando de 2 até $n-2$
    $(C, A[II]) = 0 + B + C, B = \overline{r_i}, II = II + 1$
$(C, A[II]) = 0 + B + C, B = r_{n-1}, II = II + 1$
$q_{n-1} = K = C = 0 + B + C, IB = IB - 1$

para j variando de 2 até n
    $B = r_0 \ xor \ K, II = IB, IO = IB$
    $A[II] = q_{n-j}$

    para i variando de 1 até $n-2$
        $(C, A[II]) = A[IO] + B + C, B = r_i \ xor \ K, II = II + 1, IO = IO + 1$
    $(C, A[II]) = A[IO] + B + C, B = \overline{r_{n-1}} \ xor \ K, II = II + 1, IO = IO + 1$
    $q_{n-j} = K = C = A[IO] + B + C, B = \overline{(A[IO] + B + C)}, IB = IB - 1$
$A[II] = B, C = 0, IB = IB + 1$
$B = r_0 \ and \ \overline{K}, II = IB, IO = IB$

para i variando de 1 até $n-1$
    $(C, A[II]) = A[IO] + B + C, B = r_i \ and \ \overline{K}, II = II + 1, IO = IO + 1$
$A[II] = A[IO] + B + C, K = C = x_{n-1}, IO = IB$
$B = A[IO] \ xor \ K, IO = IO + 1$

para i variando de 0 até $n-2$
    $(C, r_i) = 0 + B + C, B = A[IO] \ xor \ K, IO = IO + 1$
$(C, r_{n-1}) = 0 + B + C$
$K = C = q_n$

para i variando de 0 até $n-2$
    $B = q_i \ xor \ K$
    $(C, q_i) = 0 + B + C$
$B = q_{n-1} \ xor \ K$
$(C, q_{n-1}) = 0 + B + C, B = K$
$q_n = 0 + B + C$

Número de ciclos necessários para a divisão: $n^2 + 10n + 7$ ciclos.

A.4 - EP4 - Elemento Processador de 4 *Bits*

A.4.1 - Soma de Inteiros

$C = 0$
para i variando de 0 até $n/4 - 1$
    $A = X_i$
    $B = Y_i$
    $(C, Z_i) = A + B + C$

Número de ciclos necessários para a soma: $3n/4 + 1$.

A.4.2 - Subtração de Inteiros

$C = 1$
para i variando de 0 até $n/4 - 1$
    $A = X_i$
    $B = Y_i$
    $(C, Z_i) = A + \overline{B} + C$

Número de ciclos necessários para a subtração: $3n/4 + 1$.

A.4.3 - Multiplicação de Inteiros

$SH = Y_0, j = 0$
$K = SH_0, SH = SH \; shift \; right \; 1, B = X_0$

para i variando de 0 até $n/4 - 2$
    $P_i = B \; and \; K$
    $B = X_{i+1}$
$P_{n/4-1} = B \; and \; K$
$P_{n/4} = 0$

vá para (2)

(1) $SH = Y_j$
$K = SH_0, SH = SH \; shift \; right \; 1, A = P_j, C = 0$
$B = X_0$
$(C, P_j) = A + B \; and \; K + C$

para i variando de 1 até $n/4 - 1$
    $A = P_{i+j}$
    $B = X_i$
    $(C, P_{i+j}) = A + B \; and \; K + C$
$P_{j+n/4} = 0 + 0 + C$

(2) $K = SH_0, SH = SH \; shift \; right \; 1, A = P_j, C = 0$
$B = X_0$

para i variando de 1 até $n/4 - 1$
    $(C, P_{i+j-1}) = A + (B \; and \; K) \; shift \; left \; 1 + (C, 0000)$
    $A = P_{i+j}$
    $(C, A) = A + (B \; and \; K) \; shift \; right \; 3 + C, B = X_i$
$(C, P_{j+n/4-1}) = A + (B \; and \; K) \; shift \; left \; 1 + (C, 0000)$
$A = P_{j+n/4}$
$P_{j+n/4} = A + (B \; and \; K) \; shift \; right \; 3 + C$
$K = SH_0, SH = SH \; shift \; right \; 1, A = P_j, C = 0$
$B = X_0$

para i variando de 1 até $n/4 - 1$
    $(C, P_{i+j-1}) = A + (B \; and \; K) \; shift \; left \; 2 + (C, 0000)$
    $A = P_{i+j}$
    $(C, A) = A + (B \; and \; K) \; shift \; right \; 2 + C, B = X_i$
$(C, P_{j+n/4-1}) = A + (B \; and \; K) \; shift \; left \; 2 + (C, 0000)$
$A = P_{j+n/4}$
$P_{j+n/4} = A + (B \; and \; K) \; shift \; right \; 2 + C$

se $j == n/4 - 1$, então vá para (3)
$K = SH_0, SH = SH \; shift \; right \; 1, A = P_j, C = 0$
$B = X_0$

para i variando de 1 até $n/4 - 1$
    $(C, P_{i+j-1}) = A + (B \; and \; K) \; shift \; left \; 3 + (C, 0000)$
    $A = P_{i+j}$
    $(C, A) = A + (B \; and \; K) \; shift \; right \; 1 + C, B = X_i$

$(C, P_{j+n/4-1}) = A + (B \; and \; K) \; shift \; left \; 3 + (C, 0000)$
$A = P_{j+n/4}$
$P_{j+n/4} = A + (B \; and \; K) \; shift \; right \; 1 + C, j = j + 1$

vá para (1)

(3) $K = C = SH_0, A = P_j$

$B = X_0, (C, A) = A + K \; shift \; right \; 1 + C$

para *i* variando de 1 até $n/4 - 1$

$(C, P_{i+j-1}) = A + (\overline{B} \; and \; K) \; shift \; left \; 3 + (C, 0000)$
$A = P_{i+j}$
$(C, A) = A + (\overline{B} \; and \; K) \; shift \; right \; 1 + C, SH = B = X_i$

$(C, P_{j+n/4-1}) = A + (\overline{B} \; and \; K) \; shift \; left \; 3 + (C, 0000), SH = SH \; shift \; right \; 1$
$A = P_{j+n/4}, SH = SH \; shift \; right \; 1$
$(C, A) = A + (\overline{B} \; and \; K) \; shift \; right \; 1 + C, SH = SH \; shift \; right \; 1$
$P_{j+n/4} = A + K \; shift \; left \; 3 + (C, 0000)$
$K = C = SH_0, A = P_{n/4}$
$B = Y_0$
$(C, P_{n/4}) = A + (\overline{B} \; and \; K) + C$

para *i* variando de 1 até $n/4 - 1$

$A = P_{i+n/4}$
$B = Y_i$
$(C, P_{i+n/4}) = A + (\overline{B} \; and \; K) + C$

Número de ciclos necessários para a multiplicação: $12(n/4)^2 + 10\,n/4 + 1$ ciclos.

A.4.4 - Divisão de Inteiros

$K = C = (X_{n/4-1})_3$

para i variando de 0 até $n/4-1$

$B = X_i$

$(C, Z_i) = 0 + B \; xor \; K + C$

para i variando de $n/4$ até $2n/4-1$

$Z_i = 0$

$K = C = (Y_{n/4-1})_3$

para i variando de 0 até $n/4-1$

$B = Y_i$

$(C, R_i) = 0 + B \; xor \; K + C$

$K = C = (1111)_3$

para j variando de 1 até $n/4$

para h variando 1 até 3

$A = Z_{n/4-j}$

$B = R_0, (C, A) = A + K \; shift \; right \; 1 + C$

para i variando de 1 até $n/4$

$(C, Z_{i+n/4-j-1}) = A + (B \; xor \; K) \; shift \; left \; (4-h) + (C, 0000)$

$A = Z_{i+n/4-j}$

$(C, A) = A + (B \; xor \; K) \; shift \; right \; h + C, B = R_i$

$(C, Z_{2n/4-j-1}) = A + (B \; xor \; K) \; shift \; left \; (4-h) + (C, 0000)$

$A = Z_{2n/4-j}$

$(C, A) = A + (B \; xor \; K) \; shift \; right \; h + C, B = R_i$

$(C, Z_{2n/4-j} = B) = A + K \; shift \; left \; (4-h) + (C, 0000)$

$SH_0 = K = C = (\overline{B} \; shift \; left \; h)_3, SH = SH \; shift \; left \; 1$

para i variando de 0 até $n/4-2$

$A = Z_{i+n/4-j}$

$B = R_i$

$(C, Z_{i+n/4-j} = B) = A + B \; xor \; K + C$

$A = Z_{2n/4-j-1}$

$B = R_{n/4-1}$

$(C, Z_{2n/4-j-1}) = A + B \; xor \; K + C, SH_0 = K = C = (\overline{Z_{2n/4-j-1}})_3, SH = SH \; shift \; left \; 1$

$Q_{n/4-j} = SH$

$A = Z_0, C = 0$

$B = R_0$

$(C, Z_0) = A + B \; and \; \overline{K} + C$

para i variando de 1 até $n/4-1$

$A = Z_i$

$B = R_i$

$(C, Z_i) = A + B \; and \; \overline{K} + C$

$K = C = (X_{n/4-1})_3$

para i variando de 0 até $n/4-1$

$B = Z_i$

$(C, R_i) = 0 + B \; xor \; K + C$