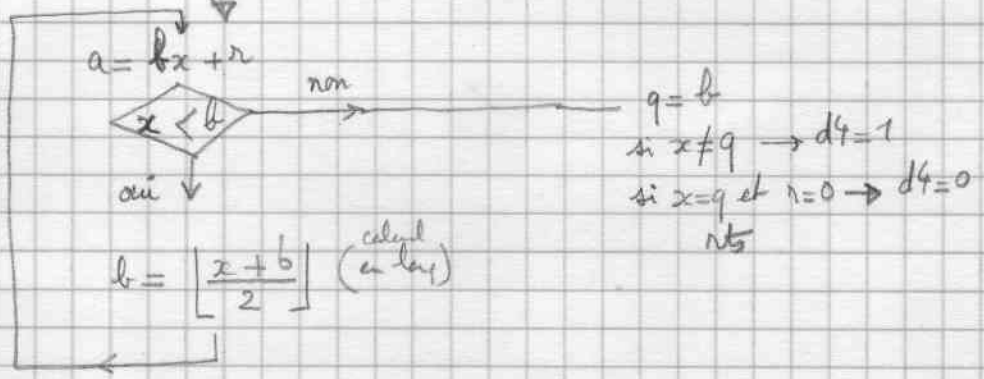
SQRS

Racine carrée de $a \in [0, 2^{32}[$

$2^{16} \leq a < 2^{32}$ → $b = 2^{15} + \left\lfloor \frac{a}{2^{16}} \right\rfloor$

$0 \leq a < 2^{16}$ → $b = 2^8$

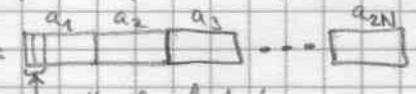
$a = 0$ → $\begin{cases} q = 0 \\ d4 = 0 \end{cases}$



SQRT1 — Racine carrée de |a| (entier)

Si $a \in [0, 2^{32}[$ utilise SQRS (méthode de Héron)

Sinon Normaliser a en multipliant par 4^n $n \geq 0$

de sorte que $a' = 4^n a =$ 

les 2 bits plus haut $\neq 0$

Nb pair de mots

4N octets

Poser $q_{-1} = \lfloor \sqrt{\overline{a_1 a_2}} \rfloor$ calculé par SQRS

Soit :

k	-1	0	1	2	3	...
$i(k)$		4	8	12	20	36, ..., 4N

($i(k) = 4(1+2^k)$ sauf le dernier $= 4N$ et le premier $= 4$)

Pour $k = 0, 1, \ldots$

→ Poser $a_k =$ les $i(k)$ premiers octets de $a' = \overline{a_1 a_2 \ldots a_{\frac{i}{2}}}$

$$q_k^{(0)} = (q_{k-1}+1)\,16^{i(k)-i(k-1)}$$

On sait que $\left[q_{k-1}\, 16^{i(k)-i(k-1)} \right]^2 \leq a_k < q_k^{(0)\,2}$

$q_k^{(0)}$ est donc un point de départ convenable pour la méthode de Héron :

pour $j = 0, 1, \ldots$

$$a_k = q_k^{(j)} x + r \qquad r \in [0, q_k^{(j)}[$$

si $x \geq q_k^{(j)}$ fin $q_k = q_k^{(j)}$ et $d4 = \begin{cases} 0 & \text{racine exacte} \\ 1 & \text{" approchée} \end{cases}$

sinon $q_k^{(j+1)} = \left\lfloor \frac{q_k^{(j)} + x}{2} \right\rfloor$

augmenter j

En réalité, la boucle sur j n'est effectuée que pour la ~~première et~~ dernière valeur de k.

Sinon on prend $q_k = q_k^{(1)}$

augmenter k

1 Pose en libre $[A2^s] = intsqr\left|[A0^e]\right|^{\to a}$

$D1^s = \begin{cases} 0 & \text{exact} \\ 1 & \text{approché} \end{cases}$

```
SQRT1:MOVEQ #0,D0
GIB64:MOVE D0,TSQRF          ) ⊗
;MOVEQ #0,D0                 ) inutile (d0=1 / 0)
      MOVE (A0)+,D0
      AND #$5FFF,D0
      BCLR #14,D0
      BNE ISQ11              ← MOVE (A0),D1   (EXG D0,D1)   MOVE D0,D1 / MOVE (A0),D0
      CMP #2,d1                                                → a = D0.L
      BEQ ISQ11
      CMP #4,d1
X     BNE ISQ13                                              → a long
      MOVE.L (A0)+,D0
```

SP `ISQ11:BSR SQRS` $\begin{cases} d1 = \lfloor \sqrt{a} \rfloor .W \\ d4 = 0/1 \end{cases}$ pose en libre $[A2^s] = intsqr(D0.L)$

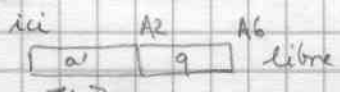
```
      MOVE D1,D0
      BRA XPOSEDO
```

```
ISQ13:MOVEQ #-1,D2
      ASR #2,D1
      BCC ISQ14
      MOVEQ #7,D2
ISQ14:ADDQ #1,D2
      ADD D0,D0
      BCS ISQ15
      ADD D0,D0
      BCC ISQ14
ISQ15:SUBQ #2,A0
      MOVEM.L D2/D3/A6,-(SP)
```

[d1 octets comme par do — Normalise

facteur de normalisation 4^{d2} $0 \le d2 \le 15$


```
      ADD D2,D2
      BSR XROT
      AND #$7FFF,(A2)        ← MOVE (A2)+,(SP)
      MOVE.L (A2),D0
      BSR ISQ11
      MOVE.L A2,4(SP)
```



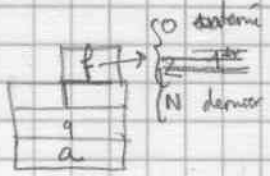
[A2] = q


```
ISQ17: MOVE.L  4(SP), A2
       MOVE    (A2), D0        ici A2 = q
       MOVE    D0, D1
       ADD     D0, D0
       MOVE    (SP), D2
```

X

```
       CLR     -(SP)           f
       SUBQ    #4, D0
       BNE     ISQ19
       MOVEQ   #2, D0
       MOVE    D0, (SP)        ⊗
ISQ19: ADD     D0, D0
       ADDQ    #4, D0
       CMP     D2, D0
       BCS     ISQ20
       MOVE    D2, D0
       MOVE    D0, (SP)
ISQ20: MOVE.L  10(SP), A0      a'
       MOVE    D0, (A0)
       ASR     #1, D0
       SUB     D1, D0
       MOVE    D0, -(SP)       Δq
       MOVE.L  A2, A0
       MOVEQ   #1, D0
       MOVE.L  A0, -(SP)
       MOVE.L  A6, A1
       MOVE    #$4001, (A6)+
       BSR     XADD1
       MOVE.L  (SP), A0
       BSR     XLB76
       MOVE.L  (SP)+, A2       q+1
       MOVE    (SP)+, D0       Δq
       ADD     D0, (A2)
```

détermine la longueur suivante
suite 4, 8, 12, 20, ..., lg(a)
0 4 8 16 ...



a'₁ = les 10 premiers octets de a'

10 = augmentation de longueur de q+1

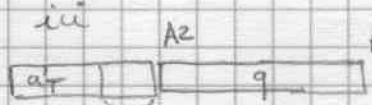
pose q+1

rajoute des zéros après q+1

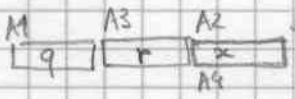
T

```
       MOVE.L  A6, A0          inutile de réinitialiser (puisque placé pour q+1)
       ADD     D0, A6
       ADD     D0, A6
       BSR     VERA6
       ASR     #1, D0
       SUBQ    #1, D0
ISQ22: CLR     (A6)+
       DBRA    D0, ISQ22
```

```
ISQ24: MOVEM.L 6(SP), A0/A1      q  a'
       EXG  A0,A1
       BSR  XDIV1
       MOVE (SP)+,D2
X      BEQ  ISQ28                → ne pas comparer
       MOVE.L A2,A0              x
       MOVE.L 4(SP),A1           q
       MOVEQ #1,D4
       BSR  XCMP1                cmp q,x
X      BCS  ISQ28                → x<q continuer
       ↓x≥q : fin
       MOVE.L A3,A6
       BNE  ISQ26                → x>q  d4=1
       CMP  #$4000(A6)
       BNE  ISQ26                → x=q mais r≠0
       MOVEQ #0,D4               ) racine exacte
ISQ26: SUBQ #2,D2
       BEQ  ISQ17
       fin
ISQ26: MOVEM.L (SP)+,D2/A0       n
       MOVE.L D4,-(SP)
       NEG  D2
       BSR  XROT
       MOVE.L 4(SP),A0
       BSR  XLB76
       MOVEM.L (SP)+,D4/A2
       RTS
ISQ28: MOVE D2,-(SP)
       MOVE.L A2,A1              x
       MOVE.L 6(SP),A0           q
       BSR  XADD1                x+q
       MOVE.L A2,A0
       MOVEQ #-1,D2
       BSR  XROT                 ⌊(x+q)/2⌋
```



0 interrompre
~~2 dois~~
N fin



$a'_T = qx + r$

⊗

MOVEM.L x fin de x A1/A6,-(SP)

```
MOVE.L  6(SP),A0      9
BSR     XLB76
MOVE    (SP)+,D2      ?
BEQ     ISQ17   <-----{ TST   TSQRF      { 0  intégr
MOVE    D2,-(SP)      { BNE   ISQ26      { 1  valeur approchée
BRA     ISQ24
```

TSQRF : D.W 0

lecture .L $d0^e = a \in [0, 2^{32}[$

sortie .W $d1^s = \lfloor \sqrt{a} \rfloor = b \in [0, 2^{15}[$

.L $d4^s = \begin{cases} 0 & \text{si } x^2 = a \\ 1 & \text{sinon} \end{cases}$

détruit d1/d2/d4

```
SQRS:  MOVE.L  D0,D1
       BEQ     ISQ44        → a=0
       SWAP    D1
       TST     D1
       BEQ     ISQ48        → a<2^16

       OR      #16,SR
       BRA     ISQ41

ISQ40: ADD     D2,D1
ISQ41: ROXR    #1,D1

ISQ42: MOVE.L  D0,D2        d0 = a = bx + r
       DIVU    D1,D2        d1 = b
       BVS     ISQ46  → x ≥ 2^16   d2 = [ r | x ]
       CMP     D1,D2
       BCS     ISQ40        → x < b
       BNE     ISQ46        → b² ≠ a
       SWAP    D2
       TST     D2
       BNE     ISQ46        → b² ≠ a
ISQ44: MOVEQ   #0,D4
       RTS

ISQ48: MOVEQ   #1,D4
       RTS
       MOVE    #$100,D1
       BRA     ISQ42
```

temps de calculs (3 vérifications)

$d0_H$	temps
FFFF	45 µs
7FFF	100 µs
3FFF	123
1FFF	130
FFF	145
7FF	151
FF	188
F	228
1	262
0	314 µs