Démonstration de : ① $\sqrt{N}$ **deux fois traçable**

$\Leftrightarrow$ ② $\exists$ **(** a **;** b **;** c **;** d **) entiers naturels tels que** $N = (a^2+b^2)(c^2+d^2)$ **avec** $a > b \geq 1$ **et** $c > d \geq 1$

Et alors on a $\sqrt{N} = \begin{bmatrix} ac+bd \\ |ad-bc| \end{bmatrix} = \begin{bmatrix} ac-bd \\ ad+bc \end{bmatrix}$

$\boxed{① \Rightarrow ② :}$

① : $\sqrt{N}$ deux fois traçable $\exists$ (A ; B ; C ; D) entiers naturels tels que $N = A^2+B^2 = C^2+D^2$ avec $A \neq C$ et de D.

② sera démontrée en 3 propositions :

<u>Proposition 1 :</u> (A ; B ; C ; D) peuvent être ordonnés de telle façon que $A > C$ avec A et C de même parité

$D > B$ avec B et D de même parité

- On peut supposer que A est le plus grand des 4 entiers A, B, C, D et comme $A \neq C$ et $A \neq D$ on a $A > C$ et $A > D$,
  Alors $B^2 = N - A^2 < N - D^2 = C^2$
  $< N - C^2 = D^2$ donc $B < C$ et $B < D$.
- $N = A^2 + B^2 = C^2 + D^2$ donc
  - Si N est impair, A et B ainsi que C et D doivent être de parités différentes donc, quitte à inverser C et D (inversion compatible avec les relations d'ordre du précédent point), on peut supposer que A et C ainsi que B et D sont de même parité.
  - Et si N est pair, A et B doivent être de même parité, ainsi que C et D.
    Or si $A = 0\ [\,2\,]$ et $B = 0\ [\,2\,]$ alors $A^2 + B^2 = 0\ [\,4\,]$; et si $C = 1\ [\,2\,]$ et $D = 1\ [\,2\,]$ alors $C^2 + D^2 = 2\ [\,4\,]$
    Donc $A^2 + B^2 \neq C^2 + D^2$.
    Donc si N est pair alors nécessairement A, B, C , D sont tous de même parité (donc en particulier A, C et B, D)

<u>Proposition 2 :</u> $\exists$ (a ; b ; c ; d) entiers naturels tels que $A = ad + bc$; $B = ac - bd$; $C = ad - bc$; $D = ac + bd$

$A^2 + B^2 = C^2 + D^2$ donc $A^2 - C^2 = D^2 - B^2$ donc $(A - C)(A + C) = (D - B)(D + B)$

Avec $(A - C)$; $(A + C)$; $(D - B)$; $(D + B)$ entiers naturels pairs non nuls (d'après la proposition 1)

Posons alors $\text{PGCD}(A - C ; D - B) = 2a$ et $\text{PGCD}(A + C ; D + B) = 2b$

On a $A - C = 2aq$; $D - B = 2ar$ où q et r sont 1[ers] entre eux (et non nuls)

$A + C = 2bd$; $D + B = 2bc$ où c et d sont 1[ers] entre eux (et non nuls)

Alors $(A - C)(A + C) = 4abdq = (D - B)(D + B) = 4abcr$

Donc $dq = cr$ donc $d \mid cr$ avec d et c 1[ers] entre eux donc (Gauss) : $d \mid r$ donc $r = kd$ (k entier naturel non nul)

$q \mid cr$ avec q et r 1[ers] entre eux donc (Gauss) : $q \mid c$ donc $c = k'q$ (k' entier naturel non nul)

Donc $dq = cr = k'q \times kd$ donc $kk' = 1$ donc $k = k' = 1$ d'où $r = d$ et $q = c$

Il vient alors que : $A - C = 2ac$; $D - B = 2ad$; $A + C = 2bd$; $D + B = 2bc$;

D'où : $A = (2ac + 2bd)/2 = ac + bd$; $C = (2ac - 2bd)/2 = ac - bd$;

$D = (2ad + 2bc)/2 = ad + bc$; $B = (2bc - 2ad)/2 = bc - ad$

<u>Proposition 3 :</u> $N = (a^2+b^2)(c^2+d^2)$ avec $a > b \geq 1$ et $c > d \geq 1$

Avec la proposition 2 : $N = A^2 + B^2 = (ac + bd)^2 + (ad - bc)^2 = C^2 + D^2 = (ac - bd)^2 + (ad + bc)^2$

$= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2$

$= (a^2 + b^2)(c^2 + d^2)$

De plus
- $A \neq C$ donc $A^2 - C^2 = (A + C)(A - C) = 4abcd \neq 0$ donc a, b, c, d non nuls
- $A \neq D$ donc $A - D = (ac + bd) - (ad + bc) = (a - b)(c - d) \neq 0$ donc $a \neq b$ et $c \neq d$.
- Comme $N = (a^2 + b^2)(c^2 + d^2)$, on peut inverser a avec b et c avec d et donc supposer $a \geq b$ et $c \geq d$

Donc $\exists$ (a ; b ; c ; d) entiers naturels tels que $N = (a^2 + b^2)(c^2 + d^2)$ avec $a > b \geq 1$ et $c > d \geq 1$ ②

$\boxed{② \Rightarrow ① :}$

② : $\exists$ (a ; b ; c ; d) entiers naturels tels que $N = (a^2+b^2)(c^2+d^2)$ avec $a > b \geq 1$ et $c > d \geq 1$

On a : $N = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 = (ac - bd)^2 + (ad + bc)^2$

$= (ac + bd)^2 + (ad - bc)^2 = (ac + bd)^2 + | ad - bc |^2$

Avec (ac – bd) ; (ad + bc) ; (ac + bd) ; | ad – bc | entiers naturels (ac – bd est positif car $a > b > 0$ et $c > d > 0$)

Donc $\sqrt{N} = \begin{bmatrix} ac + bd \\ |ad - bc| \end{bmatrix} = \begin{bmatrix} ac - bd \\ ad + bc \end{bmatrix}$

Pour conclure que $\sqrt{N}$ est deux fois traçable il reste à montrer que (ac + bd) ≠ (ac – bd) et (ac + bd) ≠ (ad + bc) :

- (ac + bd) – (ac – bd) = 2bd ≠ 0 car b ≠ 0 et d ≠ 0 donc (ac + bd) ≠ (ac – bd)
- (ac + bd) – (ad + bc) = (a – b)(c – d) ≠ 0 car a ≠ b et c ≠ d donc (ac + bd) ≠ (ad + bc)

Donc $\sqrt{N}$ est deux fois traçable et $\sqrt{N} = \begin{bmatrix} ac + bd \\ |ad - bc| \end{bmatrix} = \begin{bmatrix} ac - bd \\ ad + bc \end{bmatrix}$ ①

CQFD.