التعريف الآتي يبين مسألة الجذور التربيعية للأعداد الصحيحة بصورة عامة.

تعريف(٤):

تعرف مسالة الجذور التربيعية SQR قياس العدد n على أنها..

إذا كان n عدد صحيحا مؤلفا، وكان $a \in Q_n$ فجد جذرا تربيعيا للعدد a قياس n.

ملاحظة:

مسألة الجذور التربيعية QSR SQR تختزل بزمن حدودي إلى مسألة التحليل.

البرهان:

الخوارزمـــية السابقة بينت كيفية حل مسألة QSR SQR في الحالة التي يكون فيها n عددا أوليا، كما تبين المبرهنة (٢) حل المسألة إذا كان لدينا تحليلا للعدد n، وبالتالي نخلص إلى أنه إذا كان لدينا العددان الأوليان p و q حيث $n = pq$ فإننا نستطيع إيجاد الجذور التربيعية للعدد $a \in Q_n$ قياس n أي أن..

$$QRP \leq_p FAC$$

المبرهنة التالية تبين لنا أن العكس صحيح أيضا .

مبرهنة(٣):

مسألة تحليل العدد n تختزل بزمن حدودي إلى مسالة إيجاد الجذور التربيعية قياس n. أي أن

$$FAC \leq_P SQR$$

البرهان:

لنفـــرض أن A خوارزمية حدودية تستخدم لحل مسالة الجذور التربيعية، عندئذ نستطيع استخدام الخوارزمية A لتحليل العدد المؤلف n على النحو التالي:

١. نختار عددا عشوائيا x بحيث يكون $\gcd(x, n) = 1$

٢. نحسب $a \equiv x^2 \pmod n$

٣. نستخدم x و a كبيانات مدخلة للخوارزمية A لإيجاد جذر تربيعي y للعدد a قياس n.

٤. إذا كانت $y \equiv \pm x \pmod n$ فإن الخوارزمية تفشل، لذا فإننا نعيد الكرة باختيار عدد عشوائي آخر x.

أمـــا إذا كانـــت $y \not\equiv \pm x \pmod n$ فـــإن $1 < \gcd(x - y, n) < n$ ولذا فإن $\gcd(x - y, n) = p$ أو $\gcd(x - y, n) = q$ وبذلك نكون قد حصلنا على تحليل للعدد n.

ملاحظات:

- بما أن للعدد a أربعة جذور تربيعية غير متطابقة قياس n هي $\pm x, \pm y$ فان احتمال نجاح كل محاولة من المحاولات الخوارزمية هو $\frac{1}{2}$ ، وبالتالي فإن عدد المحاولات المتوقعة قبل الحصول على قاسم للعدد n هو 2 ومن ثم فإن الزمن المتوقع لتنفيذ الخوارزمية يجب أن يكون حدوديا.