Proof by Induction

Let the number be $a_{k-1}\, a_{k-2} \cdots a_0$. Partition the digits from right into groups of 2. Adding an extra leading 0 if number of digits is odd. Let the partitions be $b_0\, b_1\, b_2 \ldots b_n$ and original number $a = b_0 \times 10^{2n-2} + b_1 \times 10^{2n-4} \cdots b_n \times 1$

each b_i is a 2 digit number.

Let $[b_0 \ldots b_i]$ be the number formed $b_0 \times 10^{2i-2} + b_1 \times 10^{2i-4} + \cdots b_i$

Proof by induction on variable i.

Let q_i be the quotient after group b_i is taken in long division, and let dig[i] denote the i^{th} digit from the left of q_i (0 indexed). Let ~~remainder~~ rem_i denote remainder after b_i is taken in long division

~~$\text{divisor}_0 = 0$ $\quad \text{divisor}_1 = 2q_1$ $\quad \text{divisor}_2 = 10 \times q + q$~~

Induction Hypotheses :

for any i, ~~Post Condition for SQRT function is~~ that

$[b_0 \dots b_i] - q_i^2$ is positive and minimum

and $rem_i = [b_0 \dots b_i] - q_i^2$. $\therefore$ q_i is integer square root of the number $[b_0 \dots b_i]$.

Also that $divisor_{i+1} = 2 \times q_i$

Induction Base Case :

for b_0, divisor is 0 so findNextNum returns maximum integer c such that $c^2 \leq b_0$.

hence $q_0 = c$ is Integer Square root of b_0 and

$rem_0 = b_0 - q_0^2$ is remainder.

And $divisor_0 = 0$, and at $i=1$, $divisor_1 = 10 \times 0 + 2 \times q_0$

$\therefore$ $divisor_1 = 2q_0$

Induction Step :

Assuming hypotheses to be true,

q_i is integer square root of $[b_0 \ldots b_i]$ after b_i has been considered by SQRT function.

We now consider b_{i+1}, the next 2 digits taken in variable ff.

The new number becomes $[b_0 \ldots b_i] \times 100 + b_{i+1}$ and we try to find largest digit c such that $(divisor_{i+1} \times 10 + c) \times c \leq rem_i \times 100 + b_{i+1}$

($rem_i \times 100 + b_{i+1}$ is rem_{i+1}, as b_{i+1} is inserted to its right).

Note that $rem_i = [b_0 \ldots b_i] - q_i^2$,

and also that $divisor_{i+1} = 2 \times q_i$

$$\therefore \; (20 q_i + c) \times c \leq [b_0 \ldots b_i] \times 100 - q_i^2 \times 100 + b_{i+1}$$

$$\Rightarrow 100 q_i^2 + 20 q_i c + c^2 \leq [b_0 \ldots b_{i+1}]$$

$$\Rightarrow \max_c (10 q_i + c)^2 \leq [b_0 \ldots b_{i+1}],$$

$\therefore$ $10 q_i + c$ is integer square root of $[b_0 \ldots b_{i+1}]$ and according to algorithm, $q_{i+1} = 10 q_i + c$.

Also divisor is changed as

→ $divisor_{i+2} = 10 \times divisor_{i+1} + 2 \times c$

$\therefore$ $divisor_{i+2} = 10 \times 2 q_i + 2c = 2 \times (10 q_i + c)$

$= 2 \times q_{i+1}$

$\therefore$ Induction Hypothesis is Correct.