```
Algorithm P-adic$\sqrt{\ }$ $(a, u_0, p, B)$

  Input   $a \in \mathbb{Z}^+$
          $p > 2$
          $u_0 \in \mathbb{Z}$ s.t. $a - u_0^2 \equiv 0 \pmod{p}$
                    and $u_0 \not\equiv 0 \pmod{p}$
          $B > \sqrt{a}$ a bound.

  Output  FAIL $\Rightarrow \sqrt{a} \notin \mathbb{Z}$  or  $\sqrt{a}$

  $u \leftarrow$ mods$(u_0, p)$
  $i \leftarrow 1/(2u_0)$ mod $p$
  for $k = 1, 2, 3, \ldots$ do
      $e \leftarrow a - u^2$
      if $e = 0$ then output $u$.
      if $p^k > 2B$ then output FAIL
      $e \leftarrow e/p^k$
      $u_k \leftarrow$ mods$(i \cdot e, p)$
      $u \leftarrow u + u_k p^k$
  end for

end.
```