A necessary and sufficient condition for rational roots

K. Rustan M. Leino and Rajit Manohar and Greg Nelson

3 May 1994

We show the necessary and sufficient condition under, for positive integers n, m, k where the two latter a relative prime, $n^{m/k}$ is a rational. The proof is a slight extension of the one in [KRML 30], which, in turn is an extension of the proof in [KRML 0].

For any prime p and positive integer n, we let $P.p.n$ denote the number of occurrences of p in a prime factorization of n. Let n, m, k be positive integers such that m and k are relative prime. Then,

$$
\begin{array}{ll}
 & n^{m/k} \text{ is rational} \\
= & \quad \{ \text{ def. rational } \} \\
 & \langle \exists x, y \mid y \neq 0 \triangleright n^{m/k} = x/y \rangle \\
= & \quad \{ \sqrt{n} > 0 \text{, and math } \} \\
 & \langle \exists x, y \mid x > 0 \wedge y > 0 \triangleright n^{m/k} = x/y \rangle \\
= & \quad \{ \text{ math } \} \\
 & \langle \exists x, y \mid x > 0 \wedge y > 0 \triangleright n^m \cdot y^k = x^k \rangle \\
= & \quad \{ \text{ prime factorization } \} \\
 & \langle \exists x, y \mid x > 0 \wedge y > 0 \triangleright \langle \forall p \triangleright P.p.(n^m \cdot y^k) = P.p.(x^k) \rangle \rangle \\
= & \quad \{ P.p.(a \cdot b) = P.p.a + P.p.b \} \\
 & \langle \exists x, y \mid x > 0 \wedge y > 0 \triangleright \langle \forall p \triangleright m \cdot P.p.n + k \cdot P.p.y = k \cdot P.p.x \rangle \rangle \\
\Rightarrow & \quad \{ a + b = c \wedge k|b \wedge k|c \Rightarrow k|a \} \\
 & \langle \exists x, y \mid x > 0 \wedge y > 0 \triangleright \langle \forall p \triangleright k|m \cdot P.p.n \rangle \rangle \\
= & \quad \{ \text{ range of } x, y \text{ nonempty } \} \\
 & \langle \forall p \triangleright k \text{ divides} m \cdot P.p.n \rangle \\
= & \quad \{ k \text{ and } m \text{ are relative prime } \} \\
 & \langle \forall p \triangleright k \text{ divides} P.p.n \rangle \\
= & \quad \{ \text{ prime factorization } \} \\
 & \langle \exists r \mid r > 0 \triangleright n = r^k \rangle \quad .
\end{array}
$$

For the other direction, if n has the form r^k, then $(r^k)^{m/k} = r^m$, which is integral, and thus also rational. Hence, we have established, for all positive n, m, k for which m and k are relative prime,

$$n^{m/k} \text{ rational} \equiv \langle \exists r \mid r > 0 \triangleright n = r^k \rangle \quad .$$

As a consequence, with $m, k := 1, 2$, we have

$$\sqrt{n} \text{ rational} \equiv n \text{ is a perfect square} \quad ,$$

which is the result of [KRML 30].

References

[KRML 0] K.R.M. Leino. $\sqrt{2}$ *is irrational, revisited*, 1991.

[KRML 30] K.R.M. Leino and Greg Nelson. *The rational square roots are the perfect squares*, 1994.