If $a, b$ are positive integers with $\gcd(a, b) = 1$ and if $ab$ is a square, prove that $a$ and $b$ are squares.

**Solution.**

Let $x > 0$ be an integer such that $ab = x^2$. If $x = 1$ then $ab = 1$ and hence $a = b = 1 = 1^2$. Thus we may assume that $x > 1$.

Let $x = p_1^{e_1} \ldots p_n^{e_n}$ be the prime factorization of $x$. Thus $p_1, \ldots, p_n$ are distinct primes and $e_i \geq 1$ are integers. Then

$$x^2 = p_1^{2e_1} \ldots p_n^{2e_n}$$

is the prime factorization of $x^2$. Thus

$$x^2 = ab = p_1^{2e_1} \ldots p_n^{2e_n}.$$ 

Since $a|x^2$ and $b|a^2$, it follows that

$$a = p_1^{s_1} \ldots p_n^{s_n}, \quad b = p_1^{t_1} \ldots p_n^{t_n}$$  

where $0 \leq s_i \leq 2e_i$ and $0 \leq t_i \leq 2e_i$ for $i = 1, \ldots, n$. We have

$$x^2 = ab = p_1^{s_1+t_1} \ldots p_n^{s_n+t_n} = p_1^{2e_1} \ldots p_n^{2e_n}$$

which, by the Fundamental Theorem of Arithmetic, implies that $s_i + t_i = 2e_i$ for $i = 1, \ldots, n$.

The assumption that $\gcd(a, b) = 1$ implies that there is no $i$ such that $s_i > 0$ and $t_i > 0$. Thus for each $i$ either $s_i = 0$ and $t_i = 2e_i$, or $t_i = 0$ and $s_i = 2e_i$.

Thus all the $s_i$ and $t_i$ are even. It now follows from (*) that both $a$ and $b$ are squares.

**1.67 Definition.** Let $p \geq 2$ be a prime. For a rational number $a$ define the $p$-adic norm $||a||_p$ of $a$ as follows. Set $||0||_p = 0$. If $a \neq 0$ is a rational number, then represent $a$ as $a = \pm p^{e_1} p_1^{e_{p_1}} \ldots p_n^{e_{p_n}}$ where $e_i \in \mathbb{Z}$ and where $p, p_1, \ldots, p_n$ are distinct primes. Then we set $||a||_p = p^{-e}$.

We will need to prove:

**Lemma 1**

Let $x, y, x_1, y_1$ be nonzero integers such that $\gcd(y, p) = \gcd(y_1, p) = 1$. Then $||\frac{x}{y} + \frac{x_1}{y_1}||_p \leq 1$. 
Proof. We have

\[ z = \frac{x}{y} + \frac{x_1}{y_1} = \frac{xy_1 + x_1y}{yy_1}. \]

Since \( \gcd(yy_1, p) = 1 \), in the representation of \( z \) as a product of powers of primes, the prime \( p \) will occur with exponent \( \geq 0 \). By definition this means that \( ||z||_p \leq p^{-0} = 1 \). This completes the proof of the lemma.

(i) For any rational numbers \( a, b \) prove that \( ||ab||_p = ||a||_p ||b||_p \) and that \( ||a + b||_p \leq \max\{ ||a||_p, ||b||_p \} \).

If at least one of \( a, b \) is equal to zero, then clearly \( 0 = ||ab||_p = ||a||_p ||b||_p \).
Suppose now that \( a \neq 0, b \neq 0 \). Let \( a = \epsilon p^{e_1} \cdots p^{e_n} \) and \( b = \epsilon' p^{e'_1} q_1^{s_1} \cdots q_{m}^{s_{m}} \) be representations as in the definition of \( ||.||_p \), where \( \epsilon, \epsilon' \in \{ -1, 1 \} \). Then

\[ ab = \epsilon \epsilon' p^{e + e'} p_1^{e_1} \cdots p_n^{e_n} q_1^{s_1} \cdots q_m^{s_{m}} \]

and hence by definition

\[ ||ab||_p = p^{-e - e'} = p^{-e} p^{-e'} = ||a||_p ||b||_p, \]

as required.

If at least one of \( a, b \) is equal to 0, then it is easy to see that \( ||a + b||_p \leq \max\{ ||a||_p, ||b||_p \} \) holds. Assume that \( a \neq 0, b \neq 0 \). Also we may assume that \( a \neq -b \) since the inequality \( ||a + b||_p \leq \max\{ ||a||_p, ||b||_p \} \) is obvious if \( a + b = 0 \).

Again, represent \( a \) and \( b \) as \( a = \epsilon p^{e_1} \cdots p_n^{e_n} \) and \( b = \epsilon' p^{e'_1} q_1^{s_1} \cdots q_{m}^{s_{m}} \). Put \( e'' = \min\{ e, e' \} \). Then

\[ a + b = p^{e''} (\epsilon p^{e - e''} p_1^{e_1} \cdots p_n^{e_n} + \epsilon' p^{e'-e''} q_1^{s_1} \cdots q_m^{s_{m}}) \]

Since \( e - e'' \geq 0, e' - e'' \geq 0 \), Lemma 1 implies that \( ||\epsilon p^{e - e''} p_1^{e_1} \cdots p_n^{e_n} + \epsilon' p^{e'-e''} q_1^{s_1} \cdots q_{m}^{s_{m}}||_p \leq 1 \). Therefore, by multiplicativity of \( ||.||_p \) established above, we have:

\[ ||a+b||_p \leq p^{-e''} \cdot 1 = p^{-\min\{e, e'\}} = p^{\max\{-e, -e'\}} = \max\{ p^{-e}, p^{-e'} \} = \max\{ ||a||_p, ||b||_p \}. \]

(ii) Define \( \delta_p(a, b) = ||a - b||_p \) where \( a, b \in \mathbb{Q} \).
(a) Prove that for any rationals \(a, b\) \(\delta_p(a, b) \geq 0\) and that \(\delta_p(a, b) = 0\) if and only if \(a = b\).

By definition \(||a - b||_p = 0\) when \(a - b = 0\) and \(||a - b|| = p^{-e}\) for some \(e \in \mathbb{Z}\) when \(a - b \neq 0\). This implies that \(\delta_p(a, b) \geq 0\) and that \(\delta_p(a, b) = 0\) if and only if \(a = b\).

(b) For all rationals \(a, b\) prove that \(\delta_p(a, b) = \delta_p(b, a)\).

By definitions of \(||.||_p\) and of \(\delta_p\)

\[
\delta_p(a, b) = ||a - b||_p = ||b - a||_p = \delta_p(b, a).
\]

(c) If \(a, b\) are integers and \(p^n|(a - b)\), where \(n \geq 0\) is an integer, then \(\delta_p(a, b) \leq p^{-n}\).

We may assume \(a > b\).

Since \(p^n|(a - b)\), the prime factorization of \(a - b\) is

\[
a - b = p^e p_1^{e_1} \ldots p_s^{e_s},
\]

where \(e \geq n\). Therefore

\[
\delta_p(a, b) = ||a - b||_p = p^{-e} \leq p^{-n}.
\]