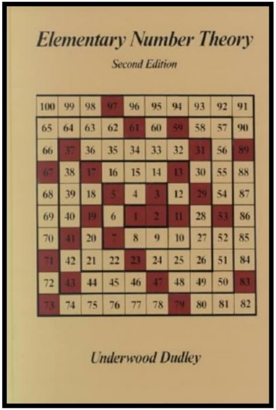
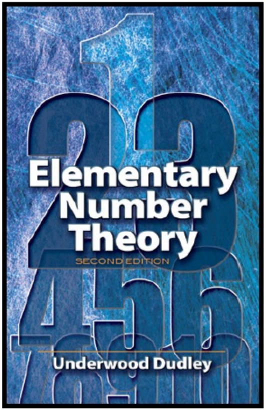
# Elementary Number Theory

**Section 17. Infinite Descent and Fermat's Conjecture**—Proofs of Theorems





# Table of contents

# Theorem 17.1

**Theorem 17.1.** There are no nontrivial solutions of $x^4 + y^4 = z^2$.

**Proof.** ASSUME that a nontrivial solution to $x^4 + y^4 = z^2$ exists. Among the nontrivial solutions, there is one with a smallest value of $z^2$ (since $z^2 \in \mathbb{N}$; this is part of the definition of $\mathbb{N}$ is a set theoretic setting). Let $c^2$ denote this value of $z^2$. Let $a$ and $b$ be corresponding values of $x$ and $y$, respectively. (Our strategy is to construct $x = r$, $y = s$, $z = t$ that also satisfy $x^2 + y^4 = z^2$ with $t^2 < c^2$, given a contradiction.) Notice that we may suppose that $a$ and $b$ are relatively prime, for if prime $p$ divides $a$ and $b$ then $p^2$ divides $c^2$ (by Lemma 1.1) and we have $(a/p)^4 + (b/p)^4 = (c/p^2)^2$, contradicting the minimality of $c$.

# Theorem 17.1

**Theorem 17.1.** There are no nontrivial solutions of $x^4 + y^4 = z^2$.

**Proof.** ASSUME that a nontrivial solution to $x^4 + y^4 = z^2$ exists. Among the nontrivial solutions, there is one with a smallest value of $z^2$ (since $z^2 \in \mathbb{N}$; this is part of the definition of $\mathbb{N}$ is a set theoretic setting). Let $c^2$ denote this value of $z^2$. Let $a$ and $b$ be corresponding values of $x$ and $y$, respectively. (Our strategy is to construct $x = r$, $y = s$, $z = t$ that also satisfy $x^2 + y^4 = z^2$ with $t^2 < c^2$, given a contradiction.) Notice that we may suppose that $a$ and $b$ are relatively prime, for if prime $p$ divides $a$ and $b$ then $p^2$ divides $c^2$ (by Lemma 1.1) and we have $(a/p)^4 + (b/p)^4 = (c/p^2)^2$, contradicting the minimality of $c$.

Notice that if $a$ and $b$ are both odd, that is $a \equiv b \equiv 1 \pmod 2$, then $a^2 \equiv b^2 \equiv 1 \pmod 4$ and $a^4 \equiv b^4 \equiv 1 \pmod{16}$. So $a^4 + b^4 \equiv 2 \pmod{16}$. So with $a^4 + b^4 = c^2$ then $c$ must be even, but if $c \equiv 0 \pmod 2$ then $c^2 \equiv 0 \pmod 4 \equiv 2 \pmod{16}$. Hence, we cannot have both $a$ and $b$ odd.

# Theorem 17.1

**Theorem 17.1.** There are no nontrivial solutions of $x^4 + y^4 = z^2$.

**Proof.** ASSUME that a nontrivial solution to $x^4 + y^4 = z^2$ exists. Among the nontrivial solutions, there is one with a smallest value of $z^2$ (since $z^2 \in \mathbb{N}$; this is part of the definition of $\mathbb{N}$ is a set theoretic setting). Let $c^2$ denote this value of $z^2$. Let $a$ and $b$ be corresponding values of $x$ and $y$, respectively. (Our strategy is to construct $x = r$, $y = s$, $z = t$ that also satisfy $x^2 + y^4 = z^2$ with $t^2 < c^2$, given a contradiction.) Notice that we may suppose that $a$ and $b$ are relatively prime, for if prime $p$ divides $a$ and $b$ then $p^2$ divides $c^2$ (by Lemma 1.1) and we have $(a/p)^4 + (b/p)^4 = (c/p^2)^2$, contradicting the minimality of $c$.

Notice that if $a$ and $b$ are both odd, that is $a \equiv b \equiv 1 \pmod 2$, then $a^2 \equiv b^2 \equiv 1 \pmod 4$ and $a^4 \equiv b^4 \equiv 1 \pmod{16}$. So $a^4 + b^4 \equiv 2 \pmod{16}$. So with $a^4 + b^4 = c^2$ then $c$ must be even, but if $c \equiv 0 \pmod 2$ then $c^2 \equiv 0 \pmod 4 \equiv 2 \pmod{16}$. Hence, we cannot have both $a$ and $b$ odd.

# Theorem 17.1 (continued 1)

**Theorem 17.1.** There are no nontrivial solutions of $x^4 + y^4 = z^2$.

**Proof (continued).** Since $a$ and $b$ are relatively prime, then both cannot be even. So one of $a$ and $b$ is even and the other is odd. Let $a$ be the even one and $b$ the odd one. Then $a^2$, $b^2$, $c$ is a fundamental solution of $x^2 + y^2 = z^2$, where $(a^2, b^2) = 1$, $a^2$ is even, and $b^2$ is odd. Hence, by Lemma 16.3 there are integers $m$ and $n$, $m > n$, relatively prime and of opposite parity, such that $a^2 = 2mn$, $b^2 = m^2 - n^2$, and $c = m^2 + n^2$.

We now show that $n$ must be even. ASSUME that $n$ is odd, so that $m$ must be even. Then as mentioned above, $n^2 \equiv 1 \pmod 4$ and $m \equiv 0 \pmod 4$. But then $b^2 = m^2 - n^2 \equiv -1 \pmod 4$. This is a CONTRADICTION because there $x^1 \equiv -1 \pmod 4$ has no solution. So the assumption that $n$ is odd is false, and hence $n$ is even (so that $m$ is odd).

# Theorem 17.1 (continued 1)

**Theorem 17.1.** There are no nontrivial solutions of $x^4 + y^4 = z^2$.

**Proof (continued).** Since $a$ and $b$ are relatively prime, then both cannot be even. So one of $a$ and $b$ is even and the other is odd. Let $a$ be the even one and $b$ the odd one. Then $a^2$, $b^2$, $c$ is a fundamental solution of $x^2 + y^2 = z^2$, where $(a^2, b^2) = 1$, $a^2$ is even, and $b^2$ is odd. Hence, by Lemma 16.3 there are integers $m$ and $n$, $m > n$, relatively prime and of opposite parity, such that $a^2 = 2mn$, $b^2 = m^2 - n^2$, and $c = m^2 + n^2$.

We now show that $n$ must be even. ASSUME that $n$ is odd, so that $m$ must be even. Then as mentioned above, $n^2 \equiv 1 \pmod 4$ and $m \equiv 0 \pmod 4$. But then $b^2 = m^2 - n^2 \equiv -1 \pmod 4$. This is a CONTRADICTION because there $x^1 \equiv -1 \pmod 4$ has no solution. So the assumption that $n$ is odd is false, and hence $n$ is even (so that $m$ is odd).

# Theorem 17.1 (continued 2)

**Theorem 17.1.** There are no nontrivial solutions of $x^4 + y^4 = z^2$.

**Proof (continued).** Since $n$ is even, say $n = 2q$, so that $a^2 = 2mn = 4mq$, or $(a/2)^2 = mq$. Next, we show that $m$ and $q$ are relatively prime. ASSUME $(m, q) \neq 1$, say prime $p \mid m$ and $p \mid q$. Then $p \mid 2q$ which means that $p \mid n$. But then prime $p$ divides both $m$ and $n$, CONTRADICTING the fact that $m$ and $n$ are relatively prime. So the assumption that $(m, q) = 1$ is false, and hence $m$ and $q$ are relatively prime. Therefore, by Lemma 16.2, $m$ and $q$ are both squares, say $m = t^2$ and $q = v^2$. Since $(m, q) = 1$ then $(t^2, v^2) = 1$ and hence $(t, v) = 1$. We saw above that $m$ is odd, so $t$ is also odd.

Since $n^2 + (m^2 - n^2) = m^2$ (D'uh!) then, because $n = 2q = 2v^2$, $m^2 - n^2 = b^2$, and $m = t^2$, we have $(2v^2)2 + b^2 = (t^2)^2$. That is, $(2v^2, b, t^2)$ form a Pythagorean triple.

# Theorem 17.1 (continued 2)

**Theorem 17.1.** There are no nontrivial solutions of $x^4 + y^4 = z^2$.

**Proof (continued).** Since $n$ is even, say $n = 2q$, so that $a^2 = 2mn = 4mq$, or $(a/2)^2 = mq$. Next, we show that $m$ and $q$ are relatively prime. ASSUME $(m, q) \neq 1$, say prime $p \mid m$ and $p \mid q$. Then $p \mid 2q$ which means that $p \mid n$. But then prime $p$ divides both $m$ and $n$, CONTRADICTING the fact that $m$ and $n$ are relatively prime. So the assumption that $(m, q) = 1$ is false, and hence $m$ and $q$ are relatively prime. Therefore, by Lemma 16.2, $m$ and $q$ are both squares, say $m = t^2$ and $q = v^2$. Since $(m, q) = 1$ then $(t^2, v^2) = 1$ and hence $(t, v) = 1$. We saw above that $m$ is odd, so $t$ is also odd.

Since $n^2 + (m^2 - n^2) = m^2$ (D'uh!) then, because $n = 2q = 2v^2$, $m^2 - n^2 = b^2$, and $m = t^2$, we have $(2v^2)2 + b^2 = (t^2)^2$. That is, $(2v^2, b, t^2)$ form a Pythagorean triple.

# Theorem 17.1 (continued 3)

**Theorem 17.1.** There are no nontrivial solutions of $x^4 + y^4 = z^2$.

**Proof (continued).** If $p \mid 2v^2$ and $p \mid b$, then $p \mid n$ (since $n = 2v^2$) and $p \mid b$; and if $p \mid n$ and $p \mid b$, then $p \mid n$ and $p \mid m$ (since $m^2 = b^2 + n^2$). That is, if $p$ divides both $2v^2$ and $b$, then $p$ divides both $n$ and $m$. Since $(m, n) = 1$, then there is not $p$ dividing both $n$ and $m$, and hence there is no $p$ dividing $2v^2$ and $b$. That is, $(2v^2, b) = 1$. Hence, $2v^2, b, t^2$ is a fundamental solution to $x^2 + y^2 = z^2$ (i.e., $(2v^2, b, t^2)$ is a primitive Pythagorean triple).

By Lemma 16.3, there are integers $M$ and $N$, with $(M, N) = 1$ and $M \not\equiv N \pmod 2$, such that $2v^2 = 2MN$, $b = M^2 - N^2$, and $t^2 = M^2 + N^2$. So $v^2 = MN$ where $(M, N) = 1$. By Lemma 16.2, we have that $M = r^2$ and $N = s^2$ for some integers $r$ and $s$. Since $t^2 = M^2 + N^2$, then we have $t^2 = (r^2)^2 + (s^2)^2$, or $r^4 + s^4 = t^2$.

# Theorem 17.1 (continued 3)

**Theorem 17.1.** There are no nontrivial solutions of $x^4 + y^4 = z^2$.

**Proof (continued).** If $p \mid 2v^2$ and $p \mid b$, then $p \mid n$ (since $n = 2v^2$) and $p \mid b$; and if $p \mid n$ and $p \mid b$, then $p \mid n$ and $p \mid m$ (since $m^2 = b^2 + n^2$). That is, if $p$ divides both $2v^2$ and $b$, then $p$ divides both $n$ and $m$. Since $(m, n) = 1$, then there is not $p$ dividing both $n$ and $m$, and hence there is no $p$ dividing $2v^2$ and $b$. That is, $(2v^2, b) = 1$. Hence, $2v^2, b, t^2$ is a fundamental solution to $x^2 + y^2 = z^2$ (i.e., $(2v^2, b, t^2)$ is a primitive Pythagorean triple).

By Lemma 16.3, there are integers $M$ and $N$, with $(M, N) = 1$ and $M \not\equiv N \pmod 2$, such that $2v^2 = 2MN$, $b = M^2 - N^2$, and $t^2 = M^2 + N^2$. So $v^2 = MN$ where $(M, N) = 1$. By Lemma 16.2, we have that $M = r^2$ and $N = s^2$ for some integers $r$ and $s$. Since $t^2 = M^2 + N^2$, then we have $t^2 = (r^2)^2 + (s^2)^2$, or $r^4 + s^4 = t^2$.

# Theorem 17.1 (continued 4)

**Theorem 17.1.** There are no nontrivial solutions of $x^4 + y^4 = z^2$.

**Proof (continued).** But then we have another solution of $x^4 + y^4 = z^2$ and in this solution we have $t^2 = m \leq m^2 < m^2 + n^2 = c \leq c^2$. But this is a CONTRADICTION to the fact that $c^2$ was a minimal value of $z^2$ among all solutions to $x^4 + y^4 = z^2$. This contradiction shows that the original assumption that there exists a nontrivial solution to $x^4 + y^4 = z^2$ is false. Hence, there are no nontrivial solutions to this equation, as originally claimed. $\square$