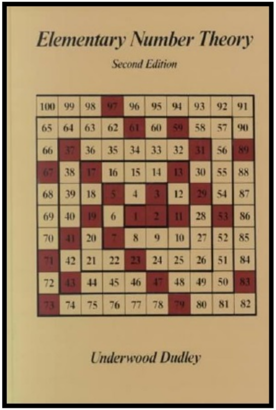
Elementary Number Theory

Section 16. Pythagorean Triangles—Proofs of Theorems



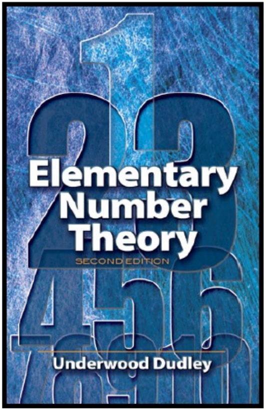


Table of contents

Lemma 16.1

Lemma 16.1. If a, b, c is a fundamental solution of $x^2 + y^2 = z^2$, then exactly one of a and b is even.

Proof. In a fundamental solution, we cannot have both a and b even, otherwise c would need to be even and 2 would divide each of a, b, c, contradicting the definition of "fundamental solution."

Lemma 16.1

Lemma 16.1. If a, b, c is a fundamental solution of $x^2 + y^2 = z^2$, then exactly one of a and b is even.

Proof. In a fundamental solution, we cannot have both a and b even, otherwise c would need to be even and 2 would divide each of a, b, c, contradicting the definition of "fundamental solution." Next, ASSUME both a and b are odd. Then we have $a^2 \equiv 1 \pmod 4$ and $b^2 \equiv 1 \pmod 4$, so that $c^2 = a^2 + b^2 \equiv 2 \pmod 4$. But then c must be even and $c^2 \equiv 0 \pmod 4$, a CONTRADICTION. So the assumption that both a and b are odd is false. Hence, exactly one of a and b is even, as claimed. □

Lemma 16.1

Lemma 16.1. If a, b, c is a fundamental solution of $x^2 + y^2 = z^2$, then exactly one of a and b is even.

Proof. In a fundamental solution, we cannot have both a and b even, otherwise c would need to be even and 2 would divide each of a, b, c, contradicting the definition of "fundamental solution." Next, ASSUME both a and b are odd. Then we have $a^2 \equiv 1 \pmod 4$ and $b^2 \equiv 1 \pmod 4$, so that $c^2 = a^2 + b^2 \equiv 2 \pmod 4$. But then c must be even and $c^2 \equiv 0 \pmod 4$, a CONTRADICTION. So the assumption that both a and b are odd is false. Hence, exactly one of a and b is even, as claimed. □

Lemma 16.2

Lemma 16.2. If $r^2 = st$ and $(s, t) = 1$, then both s and t are squares.

Proof. Use the Fundamental Theorem of Arithmetic (Theorem 2.2, "The Unique Factorization Theorem"), we have the prime-pwer decompositions of s at t:

$$s = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \text{ and } t = q_1^{f_1} q_2^{f_2} \cdots q_j^{f_j}.$$

The hypothesis that s and t are relatively prime, $(s, t) = 1$, gives that no prime appears in both decompositions.

Lemma 16.2

Lemma 16.2. If $r^2 = st$ and $(s, t) = 1$, then both s and t are squares.

Proof. Use the Fundamental Theorem of Arithmetic (Theorem 2.2, "The Unique Factorization Theorem"), we have the prime-pwer decompositions of s at t:

$$s = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \text{ and } t = q_1^{f_1} q_2^{f_2} \cdots q_j^{f_j}.$$

The hypothesis that s and t are relatively prime, $(s, t) = 1$, gives that no prime appears in both decompositions. So

$$r^2 = st = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} q_1^{f_1} q_2^{f_2} \cdots q_j^{f_j}$$

(also by Theorem 2.2) and the p's and q's are distinct primes. Since r^2 is a square, then all exponents $e_1, e_2, \ldots, e_k, f_1, f_2, \ldots f_j$ are even. Hence, s and t are squares, as claimed. □

Lemma 16.2

Lemma 16.2. If $r^2 = st$ and $(s, t) = 1$, then both s and t are squares.

Proof. Use the Fundamental Theorem of Arithmetic (Theorem 2.2, "The Unique Factorization Theorem"), we have the prime-pwer decompositions of s at t:

$$s = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \text{ and } t = q_1^{f_1} q_2^{f_2} \cdots q_j^{f_j}.$$

The hypothesis that s and t are relatively prime, $(s, t) = 1$, gives that no prime appears in both decompositions. So

$$r^2 = st = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} q_1^{f_1} q_2^{f_2} \cdots q_j^{f_j}$$

(also by Theorem 2.2) and the p's and q's are distinct primes. Since r^2 is a square, then all exponents $e_1, e_2, \ldots, e_k, f_1, f_2, \ldots f_j$ are even. Hence, s and t are squares, as claimed. □

Lemma 16.3

Lemma 16.3. Suppose that a, b, c is a fundamental solution of $x^2 + y^2 = z^2$, and suppose that a is even. Then there are positive integers m and n with $m > n$, $(m, n) = 1$, and $m \not\equiv n \pmod{2}$ such that $a = 2mn$, $b = m^2 - n^2$, and $c = m^2 + n^2$.

Proof. Since a is even, say $a = 2r$ for some positive integer r, then $a^2 = 4r^2$. Since $a^2 = c^2 - b^2$ we have $4r^2 = (c + b)(c - b)$. Now b is odd by Lemma 16.1 and c is odd by Corollary 16.A, so $c + b$ and $c - b$ are both even. So we have $c + b = 2s$ and $c - b = 2t$ for some positive integers s and t. Solving these two equations for b and c gives $c = s + t$ (summing the two equations) and $b = s - t$ (subtracting the two equations).

Lemma 16.3

Lemma 16.3. Suppose that a, b, c is a fundamental solution of $x^2 + y^2 = z^2$, and suppose that a is even. Then there are positive integers m and n with $m > n$, $(m, n) = 1$, and $m \not\equiv n \pmod 2$ such that $a = 2mn$, $b = m^2 - n^2$, and $c = m^2 + n^2$.

Proof. Since a is even, say $a = 2r$ for some positive integer r, then $a^2 = 4r^2$. Since $a^2 = c^2 - b^2$ we have $4r^2 = (c + b)(c - b)$. Now b is odd by Lemma 16.1 and c is odd by Corollary 16.A, so $c + b$ and $c - b$ are both even. So we have $c + b = 2s$ and $c - b = 2t$ for some positive integers s and t. Solving these two equations for b and c gives $c = s + t$ (summing the two equations) and $b = s - t$ (subtracting the two equations). Since $c + b = 2s$ and $c - b = 2t$, then $4r^2 = (c + b)(c - b)$ implies $4r^2 = 4st$ or $r^2 = st$. We have that s and t are relatively prime, since if $d \mid s$ and $d \mid t$ then $d \mid, (s + t)$ and $d \mid (s - t)$; that is, $d \mid c$ and $s \mid b$. But $(b, c) = 1$ by Exercise 1 (on page 129: If $(x, y) = 1$ and $x^2 + y^2 = z^2$, then $(y, z) = (x, z) = 1$) so $d = \pm 1$, and hence $(s, t) = 1$.

Lemma 16.3

Lemma 16.3. Suppose that a, b, c is a fundamental solution of $x^2 + y^2 = z^2$, and suppose that a is even. Then there are positive integers m and n with $m > n$, $(m, n) = 1$, and $m \not\equiv n \pmod 2$ such that $a = 2mn$, $b = m^2 - n^2$, and $c = m^2 + n^2$.

Proof. Since a is even, say $a = 2r$ for some positive integer r, then $a^2 = 4r^2$. Since $a^2 = c^2 - b^2$ we have $4r^2 = (c + b)(c - b)$. Now b is odd by Lemma 16.1 and c is odd by Corollary 16.A, so $c + b$ and $c - b$ are both even. So we have $c + b = 2s$ and $c - b = 2t$ for some positive integers s and t. Solving these two equations for b and c gives $c = s + t$ (summing the two equations) and $b = s - t$ (subtracting the two equations). Since $c + b = 2s$ and $c - b = 2t$, then $4r^2 = (c + b)(c - b)$ implies $4r^2 = 4st$ or $r^2 = st$. We have that s and t are relatively prime, since if $d \mid s$ and $d \mid t$ then $d \mid, (s + t)$ and $d \mid (s - t)$; that is, $d \mid c$ and $s \mid b$. But $(b, c) = 1$ by Exercise 1 (on page 129: If $(x, y) = 1$ and $x^2 + y^2 = z^2$, then $(y, z) = (x, z) = 1$) so $d = \pm 1$, and hence $(s, t) = 1$.

Lemma 16.3 (continued)

Lemma 16.3. Suppose that a, b, c is a fundamental solution of $x^2 + y^2 = z^2$, and suppose that a is even. Then there are positive integers m and n with $m > n$, $(m, n) = 1$, and $m \not\equiv n \pmod 2$ such that $a = 2mn$, $b = m^2 - n^2$, and $c = m^2 + n^2$.

Proof (continued). Since s and t are relatively prime, then Lemma 16.2 implies that s and t are both squares. Say $s = m^2$ and $t = n^2$ for some positive integers m and n. Since $a = 2r$, $a^2 = 4r^2$, and $r^2 = st$, then we have $a^2 = 4r^2 = 4st = 4m^2n^2$ or $a = 2mn$. Hence $c = s + t = m^2 + n^2$ and $b = s - t = m^2 - n^2$; so a, b, and c are as claimed in terms of m and n. Next, since b is positive then $m > n$, as claimed. Since b is odd, then $m \not\equiv n \pmod 2$, as claimed. Finally, suppose $d \mid m$ and $d \mid n$. Then $d \mid a$ since $a = 2mn$, and $d \mid b$ since $b = m^2 - n^2$. But because we have a fundamental solution, then $(a, b) = 1$ and so $d = \pm 1$. Therefore $(m, n) = 1$, as claimed. □

Lemma 16.3 (continued)

Lemma 16.3. Suppose that a, b, c is a fundamental solution of $x^2 + y^2 = z^2$, and suppose that a is even. Then there are positive integers m and n with $m > n$, $(m, n) = 1$, and $m \not\equiv n \pmod{2}$ such that $a = 2mn$, $b = m^2 - n^2$, and $c = m^2 + n^2$.

Proof (continued). Since s and t are relatively prime, then Lemma 16.2 implies that s and t are both squares. Say $s = m^2$ and $t = n^2$ for some positive integers m and n. Since $a = 2r$, $a^2 = 4r^2$, and $r^2 = st$, then we have $a^2 = 4r^2 = 4st = 4m^2n^2$ or $a = 2mn$. Hence $c = s + t = m^2 + n^2$ and $b = s - t = m^2 - n^2$; so a, b, and c are as claimed in terms of m and n. Next, since b is positive then $m > n$, as claimed. Since b is odd, then $m \not\equiv n \pmod{2}$, as claimed. Finally, suppose $d \mid m$ and $d \mid n$. Then $d \mid a$ since $a = 2mn$, and $d \mid b$ since $b = m^2 - n^2$. But because we have a fundamental solution, then $(a, b) = 1$ and so $d = \pm 1$. Therefore $(m, n) = 1$, as claimed. □

Lemma 16.4

Lemma 16.4. If $a = 2mn$, $b = m^2 - n^2$, and $c = m^2 + n^2$, then a, b, c is a solution of $x^2 + y^2 = z^2$. If in addition, $m > n$, m and n are positive, $(m, n) = 1$, and $m \not\equiv n \pmod 2$, then a, b, c is a fundamental solution.

Proof. It is straightforward to verify that a, b, c is a solution:

$$\begin{aligned} a^2 + b^2 &= (2mn)^2 + (m^2 - n^2)^2 = 4m^2n^2 + m^4 - 2m^2n^2 + n^4 \\ &= m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2 = c^2. \end{aligned}$$

Lemma 16.4

Lemma 16.4. If $a = 2mn$, $b = m^2 - n^2$, and $c = m^2 + n^2$, then a, b, c is a solution of $x^2 + y^2 = z^2$. If in addition, $m > n$, m and n are positive, $(m, n) = 1$, and $m \not\equiv n \pmod{2}$, then a, b, c is a fundamental solution.

Proof. It is straightforward to verify that a, b, c is a solution:

$$\begin{aligned} a^2 + b^2 &= (2mn)^2 + (m^2 - n^2)^2 = 4m^2n^2 + m^4 - 2m^2n^2 + n^4 \\ &= m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2 = c^2. \end{aligned}$$

To show that a, b, c is a *fundamental* solution, ASSUME p is an odd prime such that $p \mid a$ and $p \mid b$. Since $c^2 = a^2 + b^2$ then $p \mid c$. Since $p \mid b$ and $p \mid c$ then $p \mid (b + c)$ and $p \mid (b - c)$. But $b + c = 2m^2$ and $b - c = -2n^2$ (by hypothesis). So $p \mid 2m^2$ and $p \mid 2n^2$. Since p is odd, then $p \mid m^2$ and $p \mid n^2$ and hence $p \mid m$ and $p \mid n$. But this is a CONTRADICTION, since m and n are relatively prime.

Lemma 16.4

Lemma 16.4. If $a = 2mn$, $b = m^2 - n^2$, and $c = m^2 + n^2$, then a, b, c is a solution of $x^2 + y^2 = z^2$. If in addition, $m > n$, m and n are positive, $(m, n) = 1$, and $m \not\equiv n \pmod{2}$, then a, b, c is a fundamental solution.

Proof. It is straightforward to verify that a, b, c is a solution:

$$\begin{aligned} a^2 + b^2 &= (2mn)^2 + (m^2 - n^2)^2 = 4m^2n^2 + m^4 - 2m^2n^2 + n^4 \\ &= m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2 = c^2. \end{aligned}$$

To show that a, b, c is a *fundamental* solution, ASSUME p is an odd prime such that $p \mid a$ and $p \mid b$. Since $c^2 = a^2 + b^2$ then $p \mid c$. Since $p \mid b$ and $p \mid c$ then $p \mid (b + c)$ and $p \mid (b - c)$. But $b + c = 2m^2$ and $b - c = -2n^2$ (by hypothesis). So $p \mid 2m^2$ and $p \mid 2n^2$. Since p is odd, then $p \mid m^2$ and $p \mid n^2$ and hence $p \mid m$ and $p \mid n$. But this is a CONTRADICTION, since m and n are relatively prime.

Lemma 16.4 (continued)

Lemma 16.4. If $a = 2mn$, $b = m^2 - n^2$, and $c = m^2 + n^2$, then a, b, c is a solution of $x^2 + y^2 = z^2$. If in addition, $m > n$, m and n are positive, $(m, n) = 1$, and $m \not\equiv n \pmod{2}$, then a, b, c is a fundamental solution.

Proof (continued). So the assumption that there is an odd prime p which divides both a and b is false (and 2 does not divide b since $b = m^2 - n^2$ where $m \not\equiv n \pmod{2}$, and so b is odd), so that a and b have no common factors and $(a, b) = 1$. Notice that since m and n are positive by hypothesis then $a = 2mn$ is positive, and since $m > n$ by hypothesis then $b = m^2 - n^2$ is positive. That is, a, b, c is a fundamental solution, as claimed. □