Annales Mathematicae Silesianae 12 (1998), 31–33

Prace Naukowe Uniwersytetu Śląskiego nr 1751, Katowice

ON PYTHAGOREAN TRIANGLES

ANDRZEJ SCHINZEL

In memory of Ivan Korec

The following theorem answers a question asked by I. Korec at the Second Czech & Polish Conference on Number Theory.

THEOREM. *If* $m \in \mathbf{N}$, $\operatorname{ord}_2 m$ *is even,* $x_0, y_0, z_0 \in \mathbb{Z}$ *and*

$$x_0^2 + y_0^2 \equiv z_0^2 (\operatorname{mod} m), \tag{1}$$

then there exist $x, y, z \in \mathbb{Z}$ *such that*

$$x^2 + y^2 = z^2,\ x^2 \equiv x_0^2,\ y^2 \equiv y_0^2,\ z^2 \equiv z_0^2 (\operatorname{mod} m).$$

PROOF. Assume first that

$$(x_0,\ y_0,\ z_0,\ m) = 1 \tag{2}$$

and let

$$m = 2^\alpha \prod_{i=1}^{k} p_i^{\alpha_i}, \tag{3}$$

where $\alpha \geqslant 0$, $\alpha \equiv 0 (\operatorname{mod} 2)$, p_i are distinct odd primes and $\alpha_i > 0$ $(1 \leqslant i \leqslant k)$.

Received on August 7, 1998.
1991 *Mathematics Subject Classification.* 11D09.
Key words and phrases: Pythagorean triangles.

For each $i \leqslant k$ there exists $\varepsilon_i \in \{1, -1\}$ such that

$$z_0 - \varepsilon_i y_0 \not\equiv 0 (\operatorname{mod} p_i). \tag{4}$$

Otherwise we should have

$$z_0 \equiv y_0 \equiv 0 (\operatorname{mod} p_i),$$

hence, by (1) and (3) $x_0 \equiv 0(\operatorname{mod} p_i)$, $(x_0, y_0, z_0, m) \neq 1$, contrary to (2). By the Chinese remainder theorem there exists $y_1 \in \mathbb{Z}$ such that

$$y_1 \equiv \varepsilon_i y_0 (\operatorname{mod} p_i^{\alpha_i}) \quad (1 \leqslant i \leqslant k) \tag{5}$$

$$y_1 \equiv y_0 (\operatorname{mod} 2^{\alpha}) \tag{6}$$

and we have

$$y_1^2 \equiv y_0^2 (\operatorname{mod} m). \tag{7}$$

Consider first the case $\alpha = 0$. Then by (4) and (5)

$$(z_0 - y_1, m) = 1$$

and there exists $l \in \mathbb{Z}$ such that

$$2l(z_0 - y_1) \equiv 1 (\operatorname{mod} m). \tag{8}$$

We put

$$x = 2lx_0(z_0 - y_1), \; y = l\big(x_0^2 - (z_0 - y_1)^2\big), \; z = l\big(x_0^2 + (z_0 - y_1)^2\big).$$

We have $x^2 + y^2 = z^2$. On the other hand, by (7), (8) and (1)

$$\begin{aligned}
&x \equiv x_0 (\operatorname{mod} m),\\
&y \equiv l\big(z_0^2 - y_1^2 - (z_0 - y_1)^2\big) \equiv 2ly_1(z_0 - y_1) \equiv y_1 (\operatorname{mod} m),\\
&z \equiv l\big(z_0^2 - y_1^2 + (z_0 - y_1)^2\big) \equiv 2lz_0(z_0 - y_1) \equiv z_0 (\operatorname{mod} m),
\end{aligned}$$

hence

$$x^2 \equiv x_0^2, \; y^2 \equiv y_0^2, \; z^2 \equiv z_0^2 (\operatorname{mod} m).$$

Consider now the case $\alpha > 0$. If $z_0 \equiv x_0 (\operatorname{mod} 2)$ and $z_0 \equiv y_0 (\operatorname{mod} 2)$ we should have by (1) $(x_0, y_0, z_0, m) \neq 1$, contrary to (2).

Without loss of generality we may assume that $z_0 \not\equiv y_0 (\operatorname{mod} 2)$.

Then $x_0 \not\equiv 0 (\bmod 2)$ and, by (6), $z_0 \not\equiv y_1 (\bmod 2)$, by (4) and (5)

$$(z_0 - y_1,\ m) = 1.$$

There exists $l \in \mathbb{Z}$ such that

$$l(z_0 - y_1) \equiv 1 (\bmod m).$$

We put

$$x = l x_0 (z_0 - y_1),\ y = l \frac{x_0^2 - (z_0 - y_1)^2}{2},\ z = l \frac{x_0^2 + (z_0 - y_1)^2}{2}.$$

We have $x^2 + y^2 = z^2$. On the other hand, by (7), (9) and (1)

$$\begin{aligned} x &\equiv x_0 (\bmod m), \\ y &\equiv l \frac{z_0^2 - y_1^2 - (z_0 - y_1)^2}{2} \equiv l y_1 (z_0 - y_1) \equiv y_1 \left(\bmod \frac{m}{2}\right), \\ z &\equiv l \frac{z_0^2 - y_1^2 + (z_0 - y_1)^2}{2} \equiv l z_0 (z_0 - y_1) \equiv z_0 \left(\bmod \frac{m}{2}\right) \end{aligned}$$

hence

$$x^2 \equiv x_0^2,\ y^2 \equiv y_0^2,\ z^2 \equiv z_0^2 (\bmod m),$$

because $m/2 \equiv 0 \bmod 2$.

Assume now, that $(x_0, y_0, z_0, m) = d > 1$. Then

$$\left(\frac{x_0}{d}\right)^2 + \left(\frac{y_0}{d}\right)^2 \equiv \left(\frac{z_0}{d}\right)^2 \bmod \frac{m}{(m, d^2)} \quad \text{and} \quad \left(\frac{x_0}{d}, \frac{y_0}{d}, \frac{z_0}{d}, \frac{m}{(m, d^2)}\right) = 1.$$

Moreover $\operatorname{ord}_2 m/(m, d^2) \equiv 0 \bmod 2$. Hence, by the already proved case of the theorem there exist integers x_1, y_1, z_1 such that $x_1^2 + y_1^2 = z_1^2$ and $x_1^2 \equiv \left(\frac{x_0}{d}\right)^2$, $y_1^2 \equiv \left(\frac{y_0}{d}\right)^2$, $z_1^2 \equiv \left(\frac{z_0}{d}\right)^2 \left(\bmod \frac{m}{(m,d^2)}\right)$. It suffices to take

$$x = d x_1,\ y = d y_1,\ z = d z_1. \qquad \square$$

As observed already by Korec the condition $\operatorname{ord}_2 m$ even cannot be omitted from the theorem. Indeed, the numbers $m = 2^{2\alpha+1}$, $x_0 = y_0 = 2^\alpha$, $z_0 = 0$ satisfy (1), but the conditions $x^2 \equiv x_0^2$, $y^2 \equiv y_0^2$, $z^2 \equiv z_0^2 (\bmod m)$ imply $x^2 + y^2 \not\equiv z^2 (\bmod 2m)$.

INSTYTUT MATEMATYCZNY POLSKIEJ AKADEMII NAUK
ŚNIADECKICH 8
00–950 WARSZAWA
POLAND

e-mail:
schinzel@plearn.edu.pl