Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 11, Number 5 (2015), pp. 3905-3909

http://www.ripublication.com

A Geometrical Solution Of Fermat's Problem

L. A. Matevosyan

Yerevan State University, 1 Al. Manookian St., 025, Yerevan, Armenia
lavrentiy.matevosyan@gmail.com

Theorem. *The equation:*

$$a^p + b^p = c^p, \tag{1}$$

where a, b and c are arbitrary positive integers, and p≥3 is an arbitrary positive integer, has no solution.

Proof. Let us take the numbers *a*, *b* and *c* in (1) as coordinates of a point with respect to an orthogonal Cartesian frame $Oabc$ in Euclidean three dimensional space.
Let the triple of the positive integers (a_0, b_0, c_0) be a solution of (1) for $p = p_0$. Then it is obvious that coordinates of any point of the straight line, connecting the origin of the coordinate frame $O(0,0,0)$ and the point M_0 (a_0, b_0, c_0), satisfy equation (1), too. Let us consider all the lines – together with the line OM_0 – which have the same angle φ_0 with the axis Oc as the angle between the axis Oc and the straight line OM_0 is. Then a circular cone is obtained, which is defined by the following equation:

$$a^2 + b^2 = \lambda_0 c^2, \tag{2}$$

where λ_0 is a constant:

$$\lambda_0 = \frac{a_0^2 + b_0^2}{c_0^2}. \tag{3}$$

Now let us change the variables a, b, c into new variables l, k, m by the following expressions:

$m + l = a;\ m + k = b;\ m + l + k = c$:

From these we have:

$$m = a + b - c;\ k = c - a;\ l = c - b: \tag{4}$$

In this case we obtain from equation (1):

$$(m + l)^p + (m + k)^p = (m + k + l)^p, \tag{5}$$

and (2) can be transformed into the following:

$$(m + l)^2 + (m + k)^2 = \lambda_0 (m + k + l)^2: \tag{6}$$

Let us write (6) in the following form:

$$(2-\lambda_0)m^2+2\cdot(k+l)\cdot(1-\lambda_0)m+(k^2+l^2)\cdot(1-\lambda_0)-2kl\lambda_0=0: \qquad (7)$$

It is easy to see that $1\le\lambda_0<2$.

Indeed, a, b, and c in (1) are positive integers, consequently, $a<c$, $b<c$, hence, $a^2+b^2<2c^2$. Taking this into account, it follows from (3) that $\lambda_0<2$.

We obtain from (1) that $c=\sqrt[p]{a^p+b^p}$; hence, $c^2=\sqrt[p]{(a^p+b^p)^2}$. One can easily see that the following expression takes place, $(a^p+b^p)^2\le(a^2+b^2)^p$, where the equation sign is for the case p = 2 only. Consequently, $c^2\le\sqrt[p]{(a^2+b^2)^p}=a^2+b^2$. Thus, $a^2+b^2\ge c^2$, and it follows from (3) that $\lambda_0\ge 1$, but if p = 2, $\lambda_0=1$:

One can assume in (7) that k and l are mutually prime (coprime), which does not violate generality. Indeed, if k and l have a common factor (multiplier), then it follows from (5) that m, too, has a common factor together with them, and it will possible to divide by the p-power of this common factor.

In (4), substituting a_0, b_0 and c_0 for a, b and c, we obtain:

$$m_0=a_0+b_0-c_0;\ k_0=c_0-a_0;\ l_0=c_0-b_0 \qquad (8)$$

Let us consider the section of cone (7) by the plane $m=m_0$. One can easily see that this a hyperbole having the following equation in the plane $m=m_0$:

$$(1-\lambda_0)k^2-2\lambda_0kl+(1-\lambda_0)l^2+2(1-\lambda_0)m_0k+2(1-\lambda_0)m_0l+(2-\lambda_0)m_0^2=0. \qquad (9)$$

Here λ_0 is a rational number. Let us represent this number as the fraction $\frac{n}{r}$ where $(n,r)=1$. Taking into account that if $p\ge3$, $1<\lambda_0<2$, we have:

$$r<n<2r,\ (n,r)=1: \qquad (10)$$

In (9), substituting this value of λ_0, we get:

$$(n-r)k^2+2nkl+(n-r)l^2+2(n-r)m_0k+2(n-r)m_0l-(2r-n)m_0^2=0: \qquad (11)$$

As is shown in [1, p 226], in the following transformation:

$$\begin{cases} x=\overline{\alpha}k+\overline{\beta} \\ y=\overline{\alpha}l+\overline{\gamma} \end{cases} \qquad (12)$$

one can choose the integers $\overline{\alpha},\overline{\beta},\overline{\gamma}$ in such a way that after the transformation the factors of the first orders of x and y vanish in the equation. Then (11) takes the following form:

$$(n-r)x^2+2nxy+(n-r)y^2=M: \qquad (13)$$

By the way which is presented on the same page, we get:

$$\overline{\alpha}=D=n^2-(r-n)^2; \qquad \overline{\beta}=-n(r-n)m_0-(r-n)(r-n)m_0;$$

$$\overline{\gamma}=-n(r-n)m_0-(r-n)(r-n)m_0$$

$$M=(r-2n)\left[(r-n)(r-n)^2m_0^2+2n(r-n)^2m_0^2+(r-n)(r-n)^2m_0^2\right]-(2r-n)m_0^2r^2(2n-r)^2, \quad (14)$$

or (after transformations):

$$\overline{\alpha} = D = r(2n-r);\ \overline{\beta} = \overline{\gamma} = r(n-r)m_0;\ M = r^3 n m_0^2 (2n-r), \tag{15}$$

then (12) takes the following form:

$$\begin{cases} x = r(2n-r)k + r(n-r)m_0 \\ y = r(2n-r)l + r(n-r)m_0 \end{cases}, \tag{16}$$

and (13) is written in the following form:

$$(n-r)x^2 + 2nxy + (n-r)y^2 = r^3 n m_0^2 (2n-r). \tag{17}$$

It follows from (16) that r is a common factor for x_0 and y_0. Consequently, $(x_0, y_0) = r\ d$. Dividing (17) by ($r^2\ d^2$), we get:

$$(n-r)\overline{x}^2 + 2n\overline{x}\,\overline{y} + (n-r)\overline{y}^2 = rn\left(\frac{m_0}{d}\right)^2 (2n-r), \tag{18}$$

where:

$$\overline{x} = \frac{x}{rd};\ \overline{y} = \frac{y}{rd},\ (\overline{x}, \overline{y}) = 1.$$

We can write (18) in the following form:

$$(n-r)x^2 + 2nxy + (n-r)y^2 = N,\ (x, y) = 1, \tag{19}$$

if in (18) we substitute x for $\overline{x}$ and y for $\overline{y}$ and N for $\frac{M}{r^2 d^2}$. It follows from (10) that all coefficients in (19) are positive. Let us make the following one-modular transformation:

$$\begin{cases} x' = \alpha x + \beta y \\ y' = \gamma x + \delta y \end{cases},\ \alpha\delta - \beta\gamma = 1 \tag{20}$$

where $\alpha = x_0$, $\beta = y_0$. We get:

$$(n-r)x^2 + 2nxy + (n-r)y^2 = A\ x'^2 + 2Bx'\ y' + Cy'^2, \tag{21}$$

with the following (see [2], p 280):

$$A = (n-r)\alpha^2 + 2n\alpha\gamma + (n-r)\gamma^2,$$

or:

$$A = (n-r)x_0{}^2 + 2nx_0\gamma + (n-r)\gamma^2. \tag{22}$$

Let us see whether there is, a pair ((δ, γ)) for which the following conditions take place:

$$A = N, \tag{23}$$

$$0 < B < N. \tag{24}$$

Taking into account that $\alpha = x_0$, $\beta = y_0$, we get from (23):

$$(n-r)x_0{}^2 + 2nx_0\gamma + (n-r)\gamma^2 = (n-r)x_0{}^2 + 2nx_0 y_0 + (n-r)y_0{}^2,$$

and:

$$2nx_0(\gamma - y_0) + (n-r)(\gamma^2 - y_0{}^2) = 0,$$

or:

$$(\gamma - y_0)[2nx_0 + (n-r)(\gamma + y_0)] = 0. \tag{25}$$

It is obtained from (25):

$$\gamma = y_0 \text{, or } \gamma = -y_0 - \frac{2nx_0}{n-r}. \tag{26}$$

Now let us show that the number $\gamma = -y_0 - \frac{2nx_0}{n-r}$ is not integer. Indeed, substituting the value of x_0, we get:

$$\gamma = -y_0 - \frac{2n}{n-r}\left[(2n-r)k + (n-r)m_0\right]\cdot\frac{1}{d} = -y_0 - \frac{2n}{n-r}\cdot\frac{2n-r}{d}k + 2nm_0\frac{1}{d}. \tag{27}$$

It is easy to see (using the formula for $(a+b)^p$) that from (5) one can get:

$$m^p = kl \cdot P(k,l,m) \tag{28}$$

where $P(k,l,m)$ is a polynomial with respect to k, l and m.

It follows from (28) that m can be divided by any prim factor of k, as well as by any prime factor of l. Besides (as $(n,r)=1$) $(n,n-r)=1$ and $(2n-r,n-r)=1$: Consequently, the fraction $\frac{2n(2n-r)k}{n-r}$ in (27) can be cancelled only by 2 and by the factors of k. It follows from here that if ($n-r$) has another factor except these, then γ is not integer. As $(k,l)=1$, then $k \neq l$ and we can assume that $l > k$. If $k=1$, then $l \geq 2$. Hence, if l has a factor more than 2, then γ is not an integer, because the denominator $(n-r)$ of the above-mentioned fraction cannot be cancelled by the numerator, 2. And, if $l=2$, then it follows from (11) that $(n-r)$ is divided by 4 and, being cancelled by 2 of the numerator, remains a fraction, that is, it does not become an integer. It is also obvious, that the above-said fraction is not an integer, if $l > 2$, as well.

The case $\gamma = y_0$ is left only. In this case it follows from (22):

$$A = (n-r)x_0^{\,2} + 2nx_0y_0 + (n-r)y_0^{\,2} = N, \tag{29}$$

$$B = (n-r)x_0y_0 + n\left(x_0\delta + y_0^{\,2}\right) + (n-r)\delta y_0. \tag{30}$$

It follows from the condition $k < l$ that $x_0 < y_0$. In (20), making the following transformation, $x_0 = \alpha$, $y_0 = \beta = \gamma$, we get $\delta x_0 - y_0^{\,2} = 1$, which gives $\delta > y_0$. In this case we get from (29) and (30):

$$B > N. \tag{31}$$

The representation of N by (29) is called eigen representation of N if $(x_0, y_0) = 1$. The following theorem is known (see [2, p 282, Theorem 286]). N has eigen representation by the quadratic form (a,b,c) iff there exists such $(A,B,C) \sim (a,b,c)$, that $A = N$, $0 \leq B < N$. According to this theorem, N cannot be represented by the quadratic form $(n-r)x^2 + 2nxy + (n-r)y^2$, because (31) takes place together with (30).

Consequently, our suggestion that equation (1) has a solution for positive integers (a_0, b_0, c_0) for any p_0 satisfying the condition $p \geq 3$ is not correct.

The theorem is proved.

References

1. Arnold I. V. – *Theory of Numbers,* "Narkompros of RSFSR" Publishers, 1939 (in Russian).
2. Bukhshtab A. A. – *Theory of Numbers,* "Prosveshtcenie" Publishers, Moscow, 1966 (in Russian).