МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2005
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2005
Proceedings of the Thirty Fourth Spring Conference of
the Union of Bulgarian Mathematicians
Borovets, April 6–9, 2005

EXPLICITLY CLOSED SOLUTIONS OF DIOPHANTINE EQUATIONS AND THE LATTICE STRUCTURE OF THEM*

M. Belger, H. Kaestner

By Euler's φ-theorem (on congruences) we establish the solutions (x, y) of the Diophantine equations $qx - py = k$ explicitly and in a closed form. For all $k = 0, \pm 1, \pm 2, \ldots$ the total set $\mathbf{L}$ of all these solutions can be interpreted as a certain (point-) lattice Z^2 with respect to an $x - y$-coordinate system. In this sense $\mathbf{L}$ is a two-fold periodic structure modulo c^2 ($:= p^2 + q^2$). Therefore, in an appropriate place choosen solutions in $\mathbf{L}$ can be considered as elementary or generating or in certain sense also as smallest solutions.

1. General solution of Diophantine equations by Euler's φ-function. For $p, q, k \in \mathrm{Z}$, $\gcd(p, q) = 1$, we consider the equation

$$qx - py = k \tag{1}$$

as Diophantine equation. For $k = 1$, let $(x_0, y_0) \in \mathrm{Z}^2$ be a special solution. Then the set

$$\mathbf{L}_k = \left\{(x, y) \in \mathrm{Z}^2 \;\middle|\; (x, y) = k \cdot (x_0, y_0) + l \cdot (p, q) \;\; \forall\, l \in \mathrm{Z}\right\} \tag{2}$$

is the well-known general solution of (1). In $\mathbf{L}_k$ only (x_0, y_0) is unknown. Usually methods for calculation of (x_0, y_0) are the Euclidean algorithm [2; p. 31] or the expansion into a continued fraction. Different from these procedures, here we determine (x_0, y_0) by Euler's φ-theorem. Because the domain of definition for $\varphi(p)$ is $\mathrm{N}\backslash\{0\}$, we assume that $p \geq 1$.

To find (x_0, y_0) we start with Euler's theorem [1; p. 113 f.]

$$q^{\varphi(p)} \equiv 1(p), \gcd(p, q) = 1 \tag{3}$$

That means, there is a number $j \in \mathrm{Z}$ with the property

$$q \cdot q^{\varphi(p)-1} - p \cdot j = 1 \tag{4}$$

Such a number j is obviously $j = j(p, q) = \dfrac{1}{p}(q^{\varphi(p)} - 1) \in \mathrm{Z}$. Therefore, the pair

$$(x_0, y_0) = \left(q^{\varphi(p)-1}, \frac{1}{p}(q^{\varphi(p)} - 1)\right) \tag{5}$$

is a special solution of $qx - py = 1$.

*Key words: Diophantine equations, Euler's φ-theorem, Euler's function, lattice structure.
2000 Mathematics Subject Classification: 11D04, 11P21.

Proposition 1. *The general solution* $\mathbf{L}_k$ *of the Diophantine equation* (1) *(w.l.o.g.* $p \geq 1$*) is given by* (2)*, and in view of* (5) *it follows*

$$(x,y) = k \cdot \left(q^{\varphi(p)-1}, \frac{1}{p}(q^{\varphi(p)} - 1) \right) + l \cdot (p,q) \quad \forall\, l \in \mathrm{Z} \tag{6}$$

2. The geometry of the solutions in L and their lattice structure. The general solution (x,y) is spanned by the vectors

$$\mathbf{x_0} := (x_0, y_0), \qquad \mathbf{c} := (p,q)$$

with $k, l \in \mathrm{Z}$ as coefficients.

Lemma. $\mathbf{x_0}$ *and* $\mathbf{c}$ *are linear independent vectors over* R.

So in respect to a Cartesian $x-y$-coordinate system the total set

$$\mathbf{L} := \bigcup_{k \in \mathrm{Z}} \mathbf{L}_k$$

of solutions of Diophantine equations $qx - py = k$ for all $k \in \mathrm{Z}$ can be interpreted as a 2-dimensional lattice Γ'.

Instead of the linear combination (6) for the general solution (x,y) sometimes it is advantageous to take the orthogonal linear combination

$$(x,y) = \frac{k}{c^2} \cdot (q,-p) + \frac{1}{c^2} \left(c^2 l - h(k) \right) \cdot (p,q) \qquad \forall\, l \in \mathrm{Z},$$

where

$$h(k) := \frac{k}{p}(q - c^2 q^{\varphi(p)-1}) \in \mathrm{Z}; \qquad c := |\mathbf{c}|\,. \tag{7}$$

Now with respect to an orthonormal Cartesian $x-y$-coordinate system we consider the lattice

$$\Gamma = \{(x,y) \in \mathrm{Z}^2\}.$$

As far as we interprete the equation $qx - py = k$ as the equation of a straight line in R^2, we have determined the rational lattice line $\mathbf{G}_k$, which has the parametrisation

$$\mathbf{G}_k = \left\{ (x,y) \in \mathrm{R}^2 \;\middle|\; (x,y) = k \cdot (x_0,y_0) + t \cdot (p,q), t \in \mathrm{R} \right\}. \tag{8}$$

So the solutions $(x,y) \in \mathbf{L}_k$ of the Diophantine equation $qx - py = k$ correspond to the lattice points on $\mathbf{G}_k$:

$$\mathbf{L}_k = \mathbf{G}_k \cap \Gamma.$$

(In Fig. 1 $p = 1$, $q = 2$.) Two arbitrary neighbouring lattice points $A, B \in \mathbf{G}_k$ have the distance

$$d(A,B) = c^2 = p^2 + q^2. \tag{9}$$

In other words, the lattic points on $\mathbf{G}_k$ are distributed modulo c^2.

The rational lattice lines $\mathbf{G}_k$ form a parallel family with the distance

$$d(\mathbf{G}_k, \mathbf{G}_{k+1}) = \frac{1}{c} \qquad \forall\, k \in \mathrm{Z}. \tag{10}$$

The same is true for the parallel family of orthogonal rational lattice lines

$$\mathbf{G}_k^{\perp} : px + qy = k \qquad \forall\, k \in \mathrm{Z}. \tag{11}$$

All the above facts about $\mathbf{G}_k$ are to carry over $\mathbf{G}_k^{\perp}$. So we obtain an orthogonal net

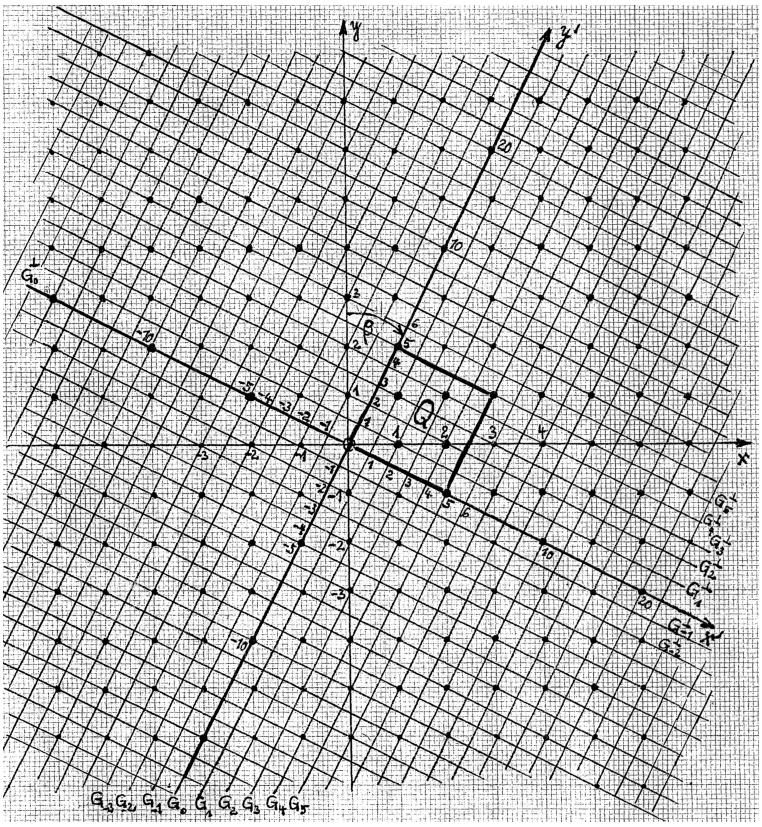

Fig. 1. $p-1$, $q=2$, $\operatorname{tg}\beta=-\dfrac{1}{2}$, $G_k: 2x-1y=k$

of coordinate lines of a new $x'-y'$-coordinate system. More detailed, $(x,y)\to(x',y')$ is a coordinate transformation $(x,y)\to(x^*,y^*)\to(x',y')$. Obviously, this is a composition consisting of the rotation

$$\begin{pmatrix} x^* \\ y^* \end{pmatrix} = \begin{pmatrix} \cos\beta & \sin\beta \\ -\sin\beta & \cos\beta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix},$$

and the stretching

$$\begin{pmatrix} x^{\copyright} \\ y^{\copyright} \end{pmatrix} = c \cdot \begin{pmatrix} x^* \\ y^* \end{pmatrix}$$

where $\sin\beta=-\dfrac{p}{c}$, $\cos\beta=\dfrac{q}{c}$.

So we have

$$\begin{pmatrix} x^{\copyright} \\ y^{\copyright} \end{pmatrix} = \begin{pmatrix} q & -p \\ p & q \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \tag{12}$$

The unit measure on the x'-axis is the same as that on y', namely $\frac{1}{c}$, and $k\left(\frac{1}{q},0\right)$ respectively $k\left(0,-\frac{1}{p}\right)$ is the intersection point of $\mathbf{G}_k$ and the x-axis respectively the y-axis. Analogically, $k\left(\frac{1}{p},0\right)$ resp. $k\left(0,\frac{1}{q}\right)$ is the intersection point of $\mathbf{G}_k^{\perp}$ and the x-axis resp. the y-axis. The Figure shows that the lattice Γ in the new $x'-y'$-coordinate system leads to a lattice constellation Γ' which reflect the lattice structure of the total set $\mathbf{L}=\bigcup\limits_{k\in\mathrm{Z}}\mathbf{L}_k$ of solutions for Diophant equations $qx-py=k$ or $px+qy=k'$ accurately and applicably. For fixed $k,k'\in\mathrm{Z}$ the solutions of $qx-py=k$ as well as of $px+qy=k'$ are distributed on $\mathbf{G}_k$ and $\mathbf{G}_{k'}^{\perp}$ modulo c^2. So it is clear that it is sufficient, instead of $\mathbf{L}$ only to look for all solutions from the square

$$\mathbf{Q}=\left\{(x^{\copyright},y^{\copyright})\in\mathrm{Z}^2 \quad \middle| \; 0\le x',y'\le c^2-1\right\} \tag{13}$$

(or also for $1\le x',y'\le c^2$). The Figur shows the situation for $p=1$, $q=2$, also $c^2=5$. The solution situation on $\mathbf{Q}$ has a two-fold periodic continuation on all squares in the x'- and y'-direction (in the direction $(-q,p)$ and (p,q)). So the solution structur of $\mathbf{L}$ has a quadratic partition on R^2 and we have to ask only for solutions in $\mathbf{Q}$, which with respect to the $x'-y'$-coordinate system are the smallest non-negative solutions $(x',y'\ge 0)$.

3. Smallest or generating solutions in L. There are problems for which are seeked such solutions.

Definition. *Solutions $(x,y)\in\mathbf{L}$, which are located in the square $\mathbf{Q}$, are said to be* smallest solutions *with respect to the $x'-y'$-coordinate system.*

Because the knowledge of such solutions already has as a consequence the knowledge of the total set $\mathbf{L}$ of solutions, we can call them also *generating solutions.* How to find them analytically?

At first by (12) we transform the solutions $(x,y)\in\mathbf{L}_k$ of $qx--py=k$ from (6) and (7) in the new coordinate representation (x',y'):

$$(x^{\copyright},y^{\copyright})=\big(k,c^2l-h(k)\big) \tag{14}$$

Now we have to seek solutions $(x',y')\in\mathbf{Q}$, that means, we have to evaluate the conditions

$$\begin{aligned} &0\le x'=k\le c^2-1\\ &0\le y'\le c^2-1 \end{aligned} \tag{15}$$

Because y' modulo c^2 is uniquly determined, from (15) it follows that $y'=y'(k)$ with respect to $\mathbf{Q}$ is a well-defined integer-valued function of integer variables*. By (14) the same is true for $l=l(k)$. According to (15) for $k=0,1,\ldots,$ for c^2-1 we have

$$0\le c^2l(k)-h(k)\le c^2-1 \qquad \text{or} \qquad 0\le l(k)-\frac{h(k)}{c^2}\le 1-\frac{1}{c^2}.$$

Because of $c^2=p^2+q^2\ge 2$, it follows now that $\frac{1}{2}\le 1-\frac{1}{c^2}<1$ and, therefore,

*For $0\le y'\le c^2-1$, $k\in\mathrm{Z}$ is $y'=y'(k)$ a integer-valued number-theoretical function of the period c^2.

$$\frac{h(k)}{c^2} \le l(k) \le 1 + \frac{h(k)}{c^2}.$$

That means

$$a) \quad l(k) = \left[1 + \frac{h(k)}{c^2}\right] = 1 + \left[\frac{h(k)}{c^2}\right] \text{ if } c^2 \big| h(k) \qquad b) \quad l(k) = 0 \text{ if } c^2 \big| h(k).$$

Whereas $a)$ is clear, $b)$ follows from (7) and $\dfrac{h(k)}{k} = \dfrac{q - c^2 q^{\varphi(p)-1}}{p} \in \mathrm{Z}$.

This leads to $\dfrac{k}{c^2} \in \mathrm{Z}$, respectively $k = \nu \cdot c^2$, $\nu \in \mathrm{Z}$. So the first inequality (15) in case $b)$ is:

$$0 \le k = \nu \cdot c^2 \le c^2 - 1, \nu \in \mathrm{Z}.$$

This is possible only for $\nu = 0$, i.e. only for $k = 0$ and because of (8) for $h(k) = h(0) = 0$.

Proposition 2. *With respect to the $x' - y'$-coordinate system the smallest solutions $(x', y') \in \mathbf{Q}$ of $qx - py = k$ will be obtained by* (14) *for*

$$l = l(k) = \begin{cases} 1 + \left[\dfrac{h(k)}{c^2}\right] & \text{for } 1 \le k \le c^2 - 1 \\ 0 & \text{for } k = 0 \end{cases} \tag{16}$$

Theorem. *The vectors $(q, -p)$ and (p, q) of the Diophantine equation $qx - py = k$ span the square $\mathbf{Q}$. Then the smallest or also generating solutions $(x, y) \in \mathbf{Q}$ of this Diopahntine equation are given by*

$$(x, y) = \frac{k}{c^2} \cdot (q, -p) + \left(1 - \left\{\frac{h(k)}{c^2}\right\}\right) \cdot (p, q) \text{ for } k = 1, 2, \ldots, c^2 - 1 \tag{17}$$

$(x, y) = (0, 0)$ *for $k = 0$, where $h(k)$ is given by* (7) *and* $\{a\} := a - [a]$.

Remark 1. Because of the periodic behaviour of the solutions in $\mathbf{L}$ in the directions $(q, -p)$ and (p, q), we need only that part of $\mathbf{Q}$ which is defined by (13). Formula (17) would give for $k = 0$ resp. $k = c^2$ the solution points (p, q) resp. $(p + q, q - p)$ on the boundary of $\mathbf{Q}$. But we need only $k = 0$ and, therefore, $(x, y) = (0, 0)$.

Remark 2. The Diophantine equation $px + qy = k'$ behaves in a way "orthogonal" to $qx - py = k$ as we can observe geometrically also by $\mathbf{G}_{k'}^{\perp} \perp \mathbf{G}_k$. So our results for $qx - py = k$ are applicable also for $px + qy = k'$ as far as we rotate the coordinate system by 90°.

Concluding remark. The general solution and the generating solutions of a Diophant equation we have found on Eulers φ-function. Then, the advantage is an explicitely established and closed form of the solutions, different from the well-known recursive form, if we use the Euclidean algorithm or the expansion into a continued fraction.

REFERENCES

[1] T. M. Apostol. Introduction to Analytic Number Theory. New York, Springer, 1976.

[2] P. Bundschuh. Einführung in die Zahlentheorie. Berlin, Heidelberg, New York, Springer 1991 (2. Aufl.).

[3] I. M. Winogradow. Elemente der Zahlentheorie. Berlin, VEB Deutscher Verlag der Wissenschaften, 1955.

ЕКСПЛИЦИТНИ ЗАТВОРЕНИ РЕШЕНИЯ НА ДИОФАНТОВИ УРАВНЕНИЯ И РЕШЕТЪЧНИ СТРУКТУРИ ЗА ТЯХ

Мартин Белгер, Херберт Кестнер

Посредством Ойлеровата φ-теорема намираме експлицитно и в затворена форма решенията (x, y) на Диофантовите уравнения $qx - py = k$. За $k = 0, \pm 1, \pm 2, \ldots$ множеството $\mathbf{L}$ от тези решения може да се интерпретира като определена точкова решетка Z^2. В този смисъл $\mathbf{L}$ е една двукратна периодична структура по модул $c^2 = p^2+q^2$. Следователно, в подходящо място решенията в $\mathbf{L}$ могат да се разглеждат като елементарни или породени в определен смисъл от най-малки решения.