Functiones et Approximatio
58.2 (2018), 269–279
doi: 10.7169/facm/1707

DIOPHANTINE PROPERTIES OF THE SEQUENCES OF PRIME NUMBERS

Natalia Budarina

Abstract: The solvability over the ring of integers $\mathbb{Z}$ of some Diophantine equations is connected with the property of integers to form sequences of prime numbers, in particular, with the property of numbers to be twins. The Diophantine description of the sequences of prime numbers is obtained using the deformation method of quadratic matrix equations.

Keywords: Diophantine equation, twins, prime number, quadratic form, embedding of form, p-adic symbol.

1. Introduction

We consider the question concerning the connection between the sequences of prime numbers with the number of integer solutions of a certain class of non-homogeneous Diophantine equations.

While developing the deformation method of Diophantine quadratic systems, which was introduced by Zhuravlev [8], we have found the way to get the exact formulas for the number of integer solutions of non-homogeneous Diophantine equations. This deformation method allows us to get a construction, which connects sequences of prime numbers with a number of solutions of some non-homogeneous Diophantine equations. These equations appear as a result of the deformation of Diophantine quadratic systems by means of some specializations.

Let $q_1, q_2, \dots, q_k$ be primes, where k is even and

$$q_1 = q, \;\; q_2 = q + 2a_1, \;\; \dots, \;\; q_k = q + 2a_{k-1} \tag{1}$$

with $a_1 < a_2 < \cdots < a_{k-1}$. Let $S = \prod_{i=1}^{k} q_i$ denote the product of numbers of the sequence (1). Then $S = \sum_{i=1}^{k} c_i q^i$, where $c_k = 1$ and the coefficients $c_i = \sigma_{k-i}(2a_1, 2a_2, \cdots, 2a_{k-1})$ for $i = 1, \cdots, k-1$, being the values of elementary symmetric polynomials are even.

2010 Mathematics Subject Classification: primary: 11E20; secondary: 11A41, 11E25

Let $x = (x_1, x_2, x_3, x_4)$ and

$$F(x,t) = 2x_1^2 + x_2^2 + x_3^2 + x_4^2 - 2x_1 t^{k/2} - \sum_{i=1}^{k-1} \frac{c_i}{2} t^i \tag{2}$$

be the polynomial in t with integer coefficients of degree $k-1$, and the coefficients c_i are taken from decomposition of S. Note that the polynomial $F(x,t)$ in x is a non-homogeneous quadratic form with integer coefficients.

Theorem 1. *In the sequence (1), let k be even and all primes q_i odd. Then for $t = q$ the number of integer solutions of the equation*

$$F(x,t) = 0$$

is equal to

$$r_k = 16\alpha_2(A;Q) \prod_{p\,|S,\ p\neq 2} \left(p + \left(\frac{2}{p}\right)\right), \tag{3}$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol.

The coefficient $\alpha_2(A;Q)$ is defined in terms of the 2-adic invariants of the forms A and Q. The local invariants of quadratic forms over $\mathbb{Z}$ can be found in [3, Chapter 15, Subsection 7.2]. The quality $\alpha_2(A;Q)$ will be discussed in detail in Section 2.

Remark 1. Let us emphasize that $t = q$ is the common root of r_k equations $F(x,t) = 0$. Hence, prime numbers q, for which the sequence (1) consists of prime numbers, admit the algebraic parametrization by the roots of polynomials with integer coefficients.

The solubility of some Diophantine equations over the ring of integers $\mathbb{Z}$ is connected with the property of numbers to form sequences of primes, in particular, with the property of numbers to be twin primes. Twin primes have been characterized by Clement [2] in 1949 as follows: the integers $q \geqslant 2$, $q+2$, form a pair of twin primes if and only if $4((q-1)!+1) + q \equiv 0 \pmod{q(q+2)}$.

Sergusov [5] and Leavitt and Mullin [4] proved the following elementary fact: $n = qq'$ where (q, q') is a pair of twin primes, if and only if $\phi(n)\sigma(n) = (n-3)(n+1)$. Here $\sigma(n)$ denotes the sum of all divisors of n and $\phi(n)$ is the Euler function.

We prove the following result.

Theorem 2. *Let $q \equiv 1 \pmod 8$. Square-free numbers q, $q+2$ form a pair of twin primes if and only if the equation*

$$2x_1^2 + x_2^2 - q(2x_1 + 1) = 0$$

has 8 integer solutions.

This theorem is the natural continuation of the Fermat theorem about two squares, according to which the prime number $q \equiv 1 \pmod 4$ is represented by two squares $q = x^2 + y^2$ and the number of such representations is equal to 8. Theorem 2 permits us to obtain an analogous characteristic for the junior twin q among the pair of prime numbers $q,\ q+2$: this number q can be represented as a rational fraction

$$q = (2x_1^2 + x_2^2)/(2x_1 + 1), \tag{4}$$

and the number of such representations is again equal to 8.

Remark 2. Note that it is easy to prove Theorem 2 using the quadratic form $y_1^2 + 2y_2^2$ (by changing the variables and use formula (13.34) of [6]). But we will give an alternative proof using the deformation method of quadratic Diophantine systems.

The direct generalization of the equation (4) is a family of equations

$$2x_1^2 + x_2^2 - 2qbx_1 = q^2(c - b^2) + q, \tag{5}$$

which are parameterized by integer solutions of the equation $b^2 = 2c-1$ and which have 8 solutions (x_1, x_2). The equation (4) is obtained as a result of a specialization of the equation (5), where $b = c = 1$.

2. Proof of Theorem 1

Representations by quadratic forms of numbers or forms of smaller dimension are induced by primitive representations or embeddings of certain relevant lattices, see [6, Chapter 1, Subsections 1.1 and 1.2] and [6, Chapter 2, Subsection 15.6]. Let Q and A be non-degenerate symmetric integer matrices of sizes $n > m \geqslant 1$ with determinants $|Q| = \det Q$ and $|A| = \det A$. We identify Q and A with the corresponding quadratic forms. The form A is representable by the form Q if there is an $n \times m$ integer matrix X such that $Q[X] = {}^tXQX = A$. A solution X is said to be primitive if the greatest common divisor $d(X)$ of the minors of order m in the matrix X is equal to 1.

The outline of the proof is based on the deformation method [8, part II, Subsections 7.1 and 7.2] of quadratic matrix equations $Q[X] = A$ by the non-homogeneous specialization of the quadratic form $A = \begin{pmatrix} A' & B \\ {}^tB & A'' \end{pmatrix}$ with fixed block A'. Let X be primitive and $X = (X'X'')$ be parted into the blocks accordingly. In this case the matrix equation $Q[X] = A$ can be written as a system

$$\begin{cases} Q[X'] = A', \\ {}^tX'QX'' = B, \\ Q[X''] = A''. \end{cases} \tag{6}$$

The specialization of the quadratic form A with a fixed block A' transforms the matrix quadratic equations $Q[X] = A$ to the system of the homogeneous equations

of the first and the second degree, which is transformed into the non-homogeneous Diophantine equation. Let the genus $[Q]$ be one-class and the set of all solutions $X' : Q[X'] = A'$ forms one orbit $\{X'\}$ with respect to the group of automorphisms $O_{\mathbb{Z}}(Q)$. Further, let the determinant $|A|$ be square-free (then the number of all representations coincides with the number of primitive representations). Then in the case of the odd co-dimension $n - m$ the number of all integer solutions of obtained non-homogeneous Diophantine equation is calculated by the formula (see (13.34) of [6] and [1])

$$r = stab(X')c(n-m)std(n-m)\alpha_2(A;Q) \times \prod_{p|\ |Q|,\ p\neq 2} \left(p^{n'/2} + \delta_p\right) \prod_{p|\ |A|,\ p\neq 2} \left(p^{n'/2} + \epsilon_p\right), \quad (7)$$

where

$$n' = n-m-1, \qquad \epsilon_p = \epsilon_1(A)\left(\frac{(-1)^{n'/2-1}|Q|}{p}\right), \qquad \delta_p = \epsilon_1(Q)\left(\frac{(-1)^{n'/2}|A|}{p}\right).$$

Here $std(n-m)$ is the product of $n-m$ Riemann ζ-functions. The values of $std(n-m)$ for small $n-m$ can be found in [6, (15.3)]. The coefficient $c(n-m)$ depends only on the difference $n-m$ of the dimensions and takes the following values

$$c(1) = 1/2, \qquad c(n-m) = 1 \qquad \text{for } \ n-m > 1.$$

The factor $\alpha_2(A;Q)$ is calculated by the formulas (13.19)–(13.31) in [6]. Here $stab(X')$ is the order of the stabilizer $Stab(X')$, which consists of automorphisms M of the group $O_{\mathbb{Z}}(Q)$ such that $MX' = X'$. The sign $\epsilon_1(A) = \left(\frac{|A_1|}{p}\right)$ is determined from the Jordan decomposition into a direct sum over the ring $\mathbb{Z}_p$ of p-adic integers: $A \sim A_1 \oplus p^\alpha A_{p^\alpha}$ (see [3, chapter 15 subsections 7.1 and 7.2]).

Let us construct the ternary form A for the sequence $\{q_i\}$ of the prime odd numbers, where k is even:

$$A = \begin{pmatrix} A' & B \\ {}^tB & A'' \end{pmatrix} = \begin{pmatrix} 1 & 1 & q \\ 1 & 3 & q^{k/2}+q \\ q & q^{k/2}+q & q^k + \sum_{i=1}^{k-1} \frac{c_i}{2} q^i + q^2 \end{pmatrix} \quad (8)$$

with the determinant $S = \prod_{i=1}^{k} q_i$.

Let us choose the form Q as the sum of six squares, and consider the representation $Q[X] = A$ of the ternary form A (8). The set of solutions $X' : Q[X'] = A' = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 3 \end{smallmatrix}\right)$ forms a single orbit $\{X'\}$ with the representative

$${}^tX' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix},$$

for which $stab(X') = 2!3!2^3 = 96$. When we fix the block X', then the matrix equation $Q[X] = A$ is transformed into the non-homogeneous equation

$$2x_1^2 + x_2^2 + x_3^2 + x_4^2 - 2x_1q^{k/2} - \sum_{i=1}^{k-1} \frac{c_i}{2} q^i = 0. \tag{9}$$

The form A is equivalent to $\begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix} \oplus 2|A|$ over the odd ring $\mathbb{Z}_p$ ($p = q_i$, $i = 1, \ldots, k$) and $\epsilon_p = \epsilon_1(A)\left(\frac{1}{p}\right) = \left(\frac{2}{p}\right)$. We have $n - m = 3$, $std(3) = \frac{1}{6}$ and $|Q| = |1_6| = 1$. Here 1_6 is the identity matrix of order 6. Combining this with formula (7), we obtain that the number of integer solutions of the equation (9) is equal to

$$r_k = 16\alpha_2(A; Q) \prod_{\substack{p|S=|A| \\ p \neq 2}} \left(p + \left(\frac{2}{p}\right)\right).$$

The factor $\alpha_2(A; Q)$ is calculated explicitly by Zhuravlev in [6, Chapter 2, Subsection 13.9], it depends on the 2-adic behaviour of the forms A and Q, from which the non-homogeneous quadratic form $F(x, q)$ was obtained. ■

The question about the choice of the shifts for the constructing sequences, for which the prime numbers exist, arises here. The choice is not simple and there is a problem about a minimal shift. If $k \geqslant 8$ there exist several minimal sequences which have the same last number for every k.

Corollary 1. *For $k = 2, 4, 6, 8, 10, 12$ in the set of all possible sequences of prime odd numbers, minimal sequences are singled out*

$$\begin{aligned}
&q, q+2, \\
&q, q+2, q+6, q+8, \\
&q, q+4, q+6, q+10, q+12, q+16, \\
&q, q+2, q+6, q+8, q+12, q+18, q+20, q+26, \\
&q, q+2, q+6, q+12, q+14, q+20, q+24, q+26, \\
&q, q+2, q+6, q+8, q+12, q+18, q+20, q+26, q+30, q+32, \\
&q, q+2, q+6, q+8, q+12, q+18, q+20, q+26, q+30, q+32, q+36, q+42,
\end{aligned} \tag{10}$$

for which the number of integer solutions of the equation $F(x, q) = 0$ is equal to r_k (3) with

$$\alpha_2(A; Q) = \begin{cases} \frac{1}{8} & \text{for } \begin{cases} k = 2, 10 \text{ and } q \equiv 3 \pmod 4, \\ k = 8'', \end{cases} \\ \frac{3}{8} & \text{for } \begin{cases} k = 2, 10 \text{ and } q \equiv 1 \pmod 4, \\ k = 4, 6, 8', 12. \end{cases} \end{cases} \tag{11}$$

Proof of Corollary 1. The problem concerning the number of integer solutions of non-homogeneous equations (9) is reduced to the calculation of the factor $\alpha_2(A;Q)$. The form A (8) has the odd determinant S, then according to the formula (13.31) in [6], the factor $\alpha_2(A;Q)$ is equal to

$$\alpha_2(A;Q) = \begin{cases} \frac{3}{8} & \text{if } oct \equiv \pm 1 \pmod 8, \\ \frac{1}{8} & \text{if } oct \equiv \pm 3 \pmod 8. \end{cases} \tag{12}$$

Here the octane number is

$$coct = oct(A;Q) \equiv t_1(Q) - t_1(A) \pmod 8 \text{ if } \left(\frac{S\cdot|Q|}{2}\right) = +1$$

and

$$oct = oct(A;Q) \equiv t_1(Q) - t_1(A) + 4 \pmod 8 \text{ if } \left(\frac{S\cdot|Q|}{2}\right) = -1.$$

For $Q = 1_6$ and A (8) we have $t_1(Q) = 6$ and $t_1(A) = t(A)$.

We calculate the oddity of the forms A using the following matrix analogue of the reduction of quadratic forms to the diagonal forms over the local rings $\mathbb{Z}_p$, see [7, subsection 5.3] and [3, chapter 15 subsection 4.4]).

Let the integral quadratic form A be split into the blocks

$$A = \begin{pmatrix} D & C & C_1 \\ {}^tC & A_1 & C_2 \\ {}^tC_1 & {}^tC_2 & A_2 \end{pmatrix} \tag{13}$$

and the square block A_1 has the determinant $|A_1| \not\equiv 0 \pmod p$. We take the integral matrix

$$M = \begin{pmatrix} 1 & 0 & 0 \\ -A_1^{-1}\cdot {}^tC & 1 & -A_1^{-1}\cdot C_2 \\ 0 & 0 & 1 \end{pmatrix} \tag{14}$$

with the determinant $|M| = 1$ as the reducing matrix M. Then the original form A is equivalent over the ring $\mathbb{Z}_p$ to the form $A[M] = {}^tMAM$, which is decomposable as a direct sum. On multiplying the matrices, we obtain

$$A \sim A_1 \oplus \begin{pmatrix} \tilde{D} & \tilde{C_1} \\ {}^t\tilde{C_1} & \tilde{A} \end{pmatrix} \tag{15}$$

where the blocks $\tilde{D}$, $\tilde{C_1}$ and $\tilde{A}$ are calculated from the formulae

$$\tilde{D} = D - A_1^{-1}[{}^tC], \qquad \tilde{C_1} = C_1 - CA_1^{-1}C_2, \qquad \tilde{A} = A_2 - A_1^{-1}[C_2].$$

If the coefficient $\frac{c_{k-1}}{2} = \frac{1}{2}\sigma_1(2a_1, 2a_2, \cdots, 2a_{k-1}) = \sum_{i=1}^{k-1} a_i$ is odd (for the sequences $k = 2, 10$ of prime numbers, which are defined in the condition of Corollary 1) then over $\mathbb{Z}_2$ the form A is equivalent to

$$A \sim \begin{pmatrix} 3 & q^{k/2}+q \\ q^{k/2}+q & q^k + \sum_{i=1}^{k-1}\frac{c_i}{2}q^i + q^2 \end{pmatrix} \oplus |A|\cdot(2q^k + 3\sum_{i=1}^{k-1}\frac{c_i}{2}q^i + 2q^2 - 2q^{\frac{k+2}{2}}).$$

Thus, we obtain the following decomposition

$$A \sim_{\mathbb{Z}_2} diag\left(3, 3\left(2q^k + 3\sum_{i=1}^{k-1}\frac{c_i}{2}q^i + 2q^2 - 2q^{\frac{k+2}{2}}\right), \right.$$
$$\left. |A|\left(2q^k + 3\sum_{i=1}^{k-1}\frac{c_i}{2}q^i + 2q^2 - 2q^{\frac{k+2}{2}}\right)\right),$$

and the oddity of A is

$$t(A) \equiv tr(A) \equiv 3 + \left(2q^k + 3\sum_{i=1}^{k-1}\frac{c_i}{2}q^i + 2q^2 - 2q^{\frac{k+2}{2}}\right)(3 + |A|) \pmod 8.$$

If the coefficient $\frac{c_{k-1}}{2} = \frac{1}{2}\sigma_1(2a_1, 2a_2, \cdots, 2a_{k-1})$ is even (for the sequences $k = 4, 6, 8, 12$ of prime numbers) then over $\mathbb{Z}_2$ the form A is equivalent to

$$A \sim \begin{pmatrix} 1 & q \\ q & q^k + \sum_{i=1}^{k-1}\frac{c_i}{2}q^i + q^2 \end{pmatrix} \oplus |A| \cdot \left(q^k + \sum_{i=1}^{k-1}\frac{c_i}{2}q^i\right)$$

and the oddity of A is

$$t(A) \equiv 1 + \left(q^k + \sum_{i=1}^{k-1}\frac{c_i}{2}q^i\right)(1 + |A|) \pmod 8.$$

Substituting the oddities $t(A)$ into the formulae for the octane number and using formulae (12), we get the result (11). ■

The following statement is a consequence of the proof of Corollary 1 and (3).

Corollary 2. *Let q and $q + 2$ be a pair of prime numbers, then the number of integer solutions of the equation $2x_1^2 + x_2^2 + x_3^2 + x_4^2 - 2x_1q - q = 0$ is equal to*

$$r_2 = \begin{cases} 6(q+1)^2 & for \;\; q \equiv 1 \pmod 8, \\ 2(q^2-1) & for \;\; q \equiv 3 \pmod 8, \\ 6(q-1)(q+3) & for \;\; q \equiv 5 \pmod 8, \\ 2(q+1)(q+3) & for \;\; q \equiv 7 \pmod 8. \end{cases} \tag{16}$$

From Theorem 1 it follows that in the fourth-dimensional space the non-centered ellipsoid

$$\frac{(x_1 - \frac{1}{2}q^{\frac{k}{2}})^2}{S/4} + \frac{x_2^2}{S/2} + \frac{x_3^2}{S/2} + \frac{x_4^2}{S/2} = 1$$

with the half-integer shift $\frac{1}{2}q^{\frac{k}{2}}$, k is even, relates to the sequence of prime numbers. On this ellipsoid there is r_k (3) integer points such that $(x_1, x_2, x_3, x_4) = 1$.

Remark 3. If k is odd in the sequence (1) then we cannot obtain a result similar to Theorem 1 by using the above-mentioned deformation method.

3. Proof of Theorem 2

Consider the binary form

$$A = \begin{pmatrix} 2 & q \\ q & q^2+q \end{pmatrix} \tag{17}$$

with the determinant $|A| = q(q+2)$. Let q and $q+2$ be prime numbers, then the determinant $|A|$ has precisely two prime divisors. Let us embed the form A in the ternary form $Q = 1_3$. The form $Q = 1_3$ is one-class form and there is an embedding of A in Q over $\mathbb{Z}$ if and only if there is an embedding of A in Q over every $\mathbb{Z}_p$. Over $\mathbb{Z}_{-1} = \mathbb{R}$ the positive definite forms Q represent the positive definite forms A.

In our case the embedding of A in Q exists over $\mathbb{Z}_2$ if and only if there exists a difference $Q \ominus A$ (see [6, Chapter 1, Subsection 8.5]). The calculation of the forms $Q \ominus A$ over $\mathbb{Z}_2$ can be reduced to the following subtraction formula for 2-symbols:

$$1^{+3}_{I,3} \ominus 1^{\epsilon_1 2}_{II,0} = 1^{\epsilon_1 1}_{I,3},$$

where $\epsilon_1 = \left(\frac{q(q+2)}{2}\right)$. Taking into account the conditions of existing of the factors in 2-symbols (see [3, Chapter 15, Subsection 7.7]), we obtain that only the 2-symbol $1^{-1}_{I,3}$ exists. So, we obtain that

$$\epsilon_1 = \left(\frac{q(q+2)}{2}\right) = -1,$$

and hence, $q \equiv 1 \pmod 4$.

If A is embedded in $Q = 1_3$ over an odd ring $\mathbb{Z}_p$ ($p = q$ or $p = q+2$), then the form A is equivalent to the direct sum $A_1 \oplus pA_p$ with $\dim A_1 = 1$ and $\dim A_p = 1$. The minimal embedding for such forms A has the following form [7, (6.7)]:

$$A \hookrightarrow A_1 \oplus \begin{pmatrix} pA_p & 1 \\ 1 & 0 \end{pmatrix} = J(A). \tag{18}$$

Its dimension is equal to 3, and sign $\left(\frac{|A_1|}{p}\right)\left(\frac{-1}{p}\right) = \epsilon_2$. Since the sign $\left(\frac{|1_3|}{p}\right) = +1$, for the existing of the embedding of the form A in Q (or for the existing of $Q \ominus J(A)$) it is necessary that

$$\epsilon_2 = \left(\frac{|A_1|}{p}\right)\left(\frac{-1}{p}\right) = +1. \tag{19}$$

For the cases $p = q$ and $p = q+2$ we have $|A_1| = 2$, so that the condition (19) is equivalent to

$$\begin{aligned} &q \equiv 1; 3 \pmod 8 \quad \text{for } p = q, \\ &q \equiv \pm 1 \pmod 8 \quad \text{for } p = q+2. \end{aligned} \tag{20}$$

Now consider the embedding of the form A in $Q = 1_3$ over the odd rings $\mathbb{Z}_p$ ($p \neq 2, q, q+2$). The calculation of the forms $Q \ominus A$ over $\mathbb{Z}_p$ can be reduced to the following subtraction formula for p-symbols:

$$1^{+3} \ominus 1^{(\frac{q(q+2)}{p})2} = 1^{(\frac{q(q+2)}{p})1}.$$

Corresponding p-symbols on the right-hand side exist (see [3, Chapter 15, Subsection 7.7]).

So, the embedding of the form A (17) in $Q = 1_3$ over $\mathbb{Z}$ is possible only when $q \equiv 1 \pmod 8$. By formula (13.34) in [6], the weight of representations of the form A by the form Q is equal to

$$\frac{r(A;Q)}{o(Q)} = \alpha_2(A;Q) \prod_{p|\,|A|,\, p\neq 2} \left(1 + \left(\frac{-2}{p}\right)\right), \tag{21}$$

where $o(Q) = |O_{\mathbb{Z}}(Q)|$. The factor $\alpha_2(A;Q)$ can be calculated using formula (13.31) in [6]:

$$\alpha_2(A;Q) = \begin{cases} \frac{1}{2} & \text{for } \ oct \equiv \pm 1 \pmod 8, \\ 0 & \text{for } \ oct \equiv \pm 3 \pmod 8. \end{cases}$$

The octane number is

$$oct = oct(A;Q) \equiv t_1(Q) - t_1(A) \equiv 3 \pmod 8 \ \text{ if } \ \left(\frac{|A|}{2}\right) = +1$$

or

$$oct = oct(A;Q) \equiv t_1(Q) - t_1(A) + 4 \equiv -1 \pmod 8 \ \text{ if } \ \left(\frac{|A|}{2}\right) = -1.$$

Consequently,

$$\alpha_2(A;Q) = \begin{cases} \frac{1}{2} & \text{for } \ q \equiv 1 \pmod 4, \\ 0 & \text{for } \ q \equiv 3 \pmod 4. \end{cases}$$

Further, we use the deformation method of Diophantine quadratic systems $Q[X] = A$ in non-homogeneous case [1]. The representations $X' : Q[X'] = A' = 2$ form a single orbit with the representative ${}^tX' = (0,1,1)$. The order of its stabilizer is $stab(X') = 2 \cdot 2! = 4$. The left-hand side of equality (21) takes the form

$$\frac{r(A;Q)}{o(Q)} = \frac{r_{X'}(A;Q)}{stab(X')},$$

where $r_{X'}(A;Q)$ is the number of representations $X = (X'X'') : Q[X] = A$ with the fixed block X'. Then the matrix equation $Q[X] = A$ with fixed block A' is transformed into the non-homogeneous equation

$$2x_1^2 + x_2^2 - 2qx_1 = q. \tag{22}$$

Consequently, for the prime $q \equiv 1 \pmod 8$ and $q+2$, the number of integer solutions of equation (22) is equal to

$$r_{X'} = 2\left(1+\left(\frac{-2}{q}\right)\right)\left(1+\left(\frac{-2}{q+2}\right)\right) = 8. \tag{23}$$

Conversely, let q and $q+2$ be odd and square-free numbers, and the number of integer solutions of the non-homogeneous equation (22) is equal to 8.

The formula for the number of integer solutions of the non-homogeneous equation (22) which was got as the section of the matrix equation $Q[X] = A$ using specialization of the form A (17) can be represented in the form

$$r = 4\alpha_2(A;Q)\prod_{p|q}\left(1+\left(\frac{-2}{p}\right)\right)\prod_{p|q+2}\left(1+\left(\frac{-2}{p}\right)\right), \tag{24}$$

where accordingly to (13.31) in [6], $\alpha_2(A;Q) = \frac{1}{2}$ or 0 for $|A| \equiv \pm 3 \pmod 8$ or $\equiv \pm 1 \pmod 8$ respectively.

As $r = 8$, then $\alpha_2(A;Q) = \frac{1}{2}$ and let

$$\prod_{p|q}\left(1+\left(\frac{-2}{p}\right)\right) = 2^{\beta_1} \qquad \text{and} \qquad \prod_{p|q+2}\left(1+\left(\frac{-2}{p}\right)\right) = 2^{\beta_2}, \tag{25}$$

where $\beta_1, \beta_2 \geqslant 1$. Collecting the results from above, the equality (24) can be written as

$$2^{1+\beta_1+\beta_2} = 2^3.$$

Consequently, $\beta_1 = \beta_2 = 1$, i.e. every product of the equation (24) contains only one factor. Thus, q and $q+2$ are prime numbers. From (25) it follows that $\left(\frac{-2}{q}\right) = \left(\frac{-2}{q+2}\right) = +1$ and we conclude that $q \equiv 1 \pmod 8$. ■

Remark 4. The strongest restriction in Theorem 2 is the condition of square-free numbers q and $q+2$, but the theory of quadratic forms does not let us catch this condition.

References

[1] N.V. Budarina, *On the number of solutions of non-homogeneous equations*, Chebyshev's collection **2** (2001) 19–30 (in Russian).

[2] P.A. Clement, *Congruences for sets of primes*, Amer. Math. Monthly **56** (1949) 23–25.

[3] J.H. Conway, J.A. Sloane, *Sphere packings, lattices and groups*, Grundlehren Math. Wiss., Vol. 290, New York, Berlin, Springer-Verlag, 1988.

[4] W.G. Leavitt, A.A. Mullin, *Primes differing by a fixed integer*, Math. Comp. **37** (1981) 581–585.

[5] I.S.A. Sergusov, *On the problem of prime-twins*, Jaroslav. Gos. Ped. Inst. Ucen.Zap. **82** (1971) 85–86 (in Russian).

[6] V.G. Zhuravlev, *Representation of a form by the genus of quadratic forms*, Algebra i Analiz (1) **8** (1996) 21–112 (in Russian).
[7] V.G. Zhuravlev, *Embedding p-elementary lattices*, Izv. Ross. Akad. Nauk Ser. Mat. (1) **63** (1999) 77–106 (in Russian).
[8] V.G. Zhuravlev, *Deformations of quadratic Diophantine systems*, Izv. Ross. Akad. Nauk Ser. Mat. (6) **65** (2001) 15–56 (in Russian).

Address: Natalia Budarina: Dundalk Institute of Technology, Dublin Road, Dundalk, Co. Louth, Ireland.

E-mail: buda77@mail.ru

Received: 1 March 2017; **revised:** 24 October 2017