[26] В. Г. Спринджук, *О рациональных приближениях к алгебраическим числам*, Изв. АН СССР 35 (1971), стр. 991–1007.
[27] Н. И. Фельдман, *Эффективное степенное усиление неравенства Лиувилля*, ibid. стр. 973–990.
[28] С. В. Котов, В. Г. Спринджук, *Уравнение Туэ–Малера в относительном поле и приближение алгебраических чисел алгебраическими числами*, Изв. АН СССР 41 (1977), стр. 723–751.
[29] K. Győry, Z. Z. Papp, *Norm form equations and explicit lower bounds for linear forms with algebraic coefficients*, Studies in Pure Mathematics, Akadémiai Kiadó, Budapest 1983, стр. 245–257.
[30] J. Gaál, *Norm form equations with several dominating variables and explicit lower bounds for inhomogeneous linear forms with algebraic coefficients*, I, II, Studia Sci. Math. Hungar. 19 (1984), стр. 399–411, 20 (1985), стр. 333–344.
[31] С. В. Котов, *Эффективная оценка линейной формы с алгебраическими коэффициентами в архимедовых и p-адических метриках*, Институт математики Акад. наук БССР, Препринт № 24 (125), Минск 1981.
[32] K. Győry, *Explicit lower bounds for linear forms with algebraic coefficients*, Arch. Math. (Basel) 35 (1980), стр. 438–446.
[33] S. V. Kotov, L. A. Trelina, *S-ganze Punkte auf elliptischen Kurven*, J. Reine Angew. Math. 306 (1979), стр. 28–41.
[34] С. В. Котов, *О диофантовых уравнениях норменного вида. I*, Институт математики, Акад. наук БССР, Препринт № 9 (89), Минск 1980.
[35] С. Ленг, *Алгебраические числа*, Мир, Москва 1966.
[36] K. Győry, *On the representation of integers by decomposable forms in several variables*, Publ. Math. Debrecen 28 (1981), стр. 89–98.

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМ. В. И. ЛЕНИНА
Минск, СССР

Поступило 5.7.1988 (1844)

ACTA ARITHMETICA
LIII (1990)

A matrix paraphrase of cyclotomy

by

D. H. LEHMER (Berkeley, Cal.)

Dedicated to the memory of V. G. Sprindžuk

1. Introduction. In a recent letter Albert Whiteman [3] enclosed a preprint of a note on block designs in which he introduced a set of matrices whose properties mimicked the Gaussian periods of classic cyclotomy. I suggested to him that the matrices should be examined further. In reply he gave me permission to make this examination myself. This paper is the result.

2. Notation and nomenclature. Throughout this paper, capital letters will be used to denote matrices. We consider square matrices of a kind known as circulants. A circulant is an n by n matrix of the form

$$M = \begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \dots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \dots & a_{n-3} \\ \dots & \dots & \dots & \dots & \dots \\ a_1 & a_2 & a_3 & \dots & a_0 \end{bmatrix}.$$

The matrix M depends only on its top row, and to save space we write

$$M = \operatorname{cir}(a_0, a_1, a_2, \dots, a_{n-1}).$$

We number the rows and columns from 0 to $n-1$ to allow the use of residue classes modulo n.

If we write

$$M = (\alpha_{ij}) \quad (i, j = 0, 1, \dots, n-1),$$

then

$$\alpha_{ij} = a_{j-i}$$

where we take the subscript modulo n.

We define Z_1 by

$$Z_1 = \operatorname{cir}(0, 1, 0, \dots, 0).$$

Then the general circulant

$$\operatorname{cir}(a_0, a_1, \ldots, a_{n-1}) = a_0 I + a_1 Z_1 + a_2 Z_1^2 + \ldots + a_{n-1} Z_1^{n-1}.$$

It follows from this that circulants commute and the product of circulants is itself a circulant. The matrix Z_1 and its powers is a matrix paraphrase of the nth roots of unity

$$1, \zeta, \zeta^2, \ldots, \zeta^{n-1}.$$

It may be verified that for

$$T = \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \zeta & \zeta^2 & \ldots & \zeta^{n-1} \\ 1 & \zeta^2 & \zeta^4 & \ldots & \zeta^{2(n-1)} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & \zeta^{n-1} & \zeta^{2(n-1)} & \ldots & \zeta^{(n-1)^2} \end{bmatrix},$$

$$T^{-1} Z_1 T = \operatorname{diag}(1, \zeta, \zeta^2, \ldots, \zeta^{n-1})$$

so Z_1 is diagonalized by T. Consequently the general circulant is also diagonalized by T,

$$T^{-1} \operatorname{cir}(a_0, a_1, a_2, \ldots, a_{n-1})\, T = \operatorname{diag}\left(\sum a_i, \sum a_i \zeta^i, \ldots, \sum a_i \zeta^{(n-1)i}\right).$$

A well-known result on the determinant of a circulant is

$$\det(\operatorname{cir}(a_0, a_1, a_2, \ldots, a_{n-1})) = \prod_{v=0}^{n-1} \sum_{s=0}^{n-1} a_s \zeta^{sv} \tag{1}$$

where $\zeta = \exp(2\pi i/n)$. This may be proved as follows. Let M be the circulant and let

$$D = \operatorname{diag}(1, \zeta^v, \zeta^{2v}, \ldots, \zeta^{(n-1)v}).$$

Since $\det(D) = 1$, $\det(M) = \det(DM)$. If we examine the row sums of MD we see that they are a power of ζ times

$$a_0 + a_1 \zeta^v + a_2 \zeta^{2v} + \ldots + a_{n-1} \zeta^{(n-1)v}. \tag{2}$$

Hence (2) is a factor of $\det(M)$. Since this is true for $v = 0, 1, 2, \ldots, n-1$, $\det(M)$ is divisible by the product of these n factors. But since $\det(M)$ is a polynomial of the form $a_0^n + \ldots$ it is equal to the product.

From now on we replace n by an odd prime p and confine the elements $a_0, a_1, \ldots, a_{p-1}$ to the rational integers.

3. Cyclotomy. Let e be a divisor of $p-1 = ef$ and let g be a primitive root of p. Let $\zeta = \exp(2\pi i/p)$. Classic cyclotomy is based on e exponential sums called the Gaussian periods of p. They are defined by

$$\eta_i = \sum_{k=0}^{e-1} \zeta^{g^{ek+i}} \qquad (i = 0, 1, 2, \ldots, e-1).$$

If we define the cyclotomic class $c(r)$ $(r = 0, \ldots, e-1)$, by that subset

$$x_0, x_1, x_2, \ldots, x_{f-1}$$

of

$$1, 2, 3, \ldots, p-1$$

for which the index of x_i with respect to g is congruent to r (mod e), then we can write

$$\eta_i = \sum_{s \in c(i)} \zeta^s.$$

The special period

$$\eta_0 = \sum_{k=1}^{f} \zeta^{g^{ke}}$$

is unambiguous since the eth powers (mod p) are not dependent on the choice of the primitive root g. It may be well to note that the product of a member of class $c(i)$ by a member of class $c(j)$ is a member of $c(i+j)$ where $i+j$ is taken modulo e.

LEMMA 1. *The sum of the η's is -1.*

Proof. Since every number from 1 to $p-1$ has its own index,

$$1 + \sum_{i=0}^{e-1} \eta_i = \sum_{r=0}^{p-1} \zeta^r = \frac{1-\zeta^p}{1-\zeta} = 0.$$

One of the most important properties of the periods is that the product of any two of them is a linear combination of all of them. More explicitly we have

LEMMA 2. *We have*

$$\eta_i \eta_{i+k} = \sum_{h=0}^{e-1} (k, h) \eta_{i+k} + \theta_k f,$$

where the coefficients (k, h) are the so-called cyclotomic numbers. In fact, (k, h) is the number of times that a number x belonging to a class $c(k)$ is followed by $x+1$, a member of class $c(h)$. The number θ_k is defined by

$$\theta_k = \begin{cases} 1 & \text{if } k = 0 \text{ and } f \text{ is even}, \\ 1 & \text{if } k = e/2 \text{ and } f \text{ is odd}, \\ 0 & \text{otherwise}. \end{cases}$$

Subscripts are taken modulo e.

For proof, see Storer [2], p. 25, together with proofs of the identities

$$(i, j) = \begin{cases} (j, i) & \text{if } f \text{ is even}, \\ (j+e/2, i+e/2) & \text{if } f \text{ is odd}, \end{cases}$$

$$\sum_{j=0}^{e-1}(i,j) = f-\theta_i. \tag{3}$$

4. The matrices H_r. Following Whiteman, we introduce a set of e matrices

$$H_0, H_1, H_2, \dots, H_{e-1}$$

which are paraphrases of the Gaussian periods. We define

$$H_r = \operatorname{cir}(a_0, a_1, a_2, \dots, a_{p-1})$$

where

$$a_j = \begin{cases} 1 & \text{if } j \in c(r), \\ 0 & \text{otherwise.} \end{cases}$$

For example, if we choose

$$p = 5,\ e = 2,\ g = 2,\ c(0) = 1,\ 4,\ c(1) = 2,\ 3,$$

then

$$H_0 = \begin{bmatrix} 0&1&0&0&1 \\ 1&0&1&0&0 \\ 0&1&0&1&0 \\ 0&0&1&0&1 \\ 1&0&0&1&0 \end{bmatrix}, \quad H_1 = \begin{bmatrix} 0&0&1&1&0 \\ 0&0&0&1&1 \\ 1&0&0&0&1 \\ 1&1&0&0&0 \\ 0&1&1&0&0 \end{bmatrix}.$$

THEOREM 1.

$$H_r = \sum_{j\in c(r)} Z^j = \sum_{v=0}^{f-1} Z^{g^{ev+r}}, \quad \textit{where } Z = Z_1.$$

Proof. Obvious.

Let J be the matrix, all of whose elements are equal to unity.

THEOREM 2.

$$\sum_{r=0}^{e-1} H_r = J-I.$$

Proof. $$\sum_{r=0}^{e-1} H_r = \sum_{v=0}^{f-1}\sum_{r=0}^{e-1} Z^{g^{ev+r}} = \sum_{j=1}^{p-1} Z^j = J-I.$$

THEOREM 3.

$$H_rH_{r+k} = \sum_{h=0}^{e-1}(k,h)H_{r+h} + \theta_k f I.$$

Proof. Let $H_r = (a_{ij})$ and $H_{r+k} = (b_{ij})$ and let $C = H_rH_{r+k}$. Then

$$C_{ij} = \sum_{m=0}^{p-1} a_{im}b_{mj} = \sum_{m=0}^{p-1} a_{m-i}b_{j-m} = \sum_{t=0}^{p-1} a_t b_{j-i-t}.$$

We know that C is a circulant. We need to consider only the top row of C. Since $a_0 = 0$,

$$C_{0j} = \sum_{t=1}^{p-1} a_t b_{j-t}.$$

Most of the terms vanish. In fact, C_{0j} is the number of times that there exist two numbers x and y whose sum is $j \pmod p$ and $x \in c(r)$ and $y \in c(r+k)$. In other words, C_{0k} is the number of solutions (x, y) of the congruence

$$g^{xe+r} + g^{ye+r+k} \equiv j \pmod p. \tag{4}$$

There are two cases: Case I, $j \equiv 0 \pmod p$, and Case II, $j \not\equiv 0 \pmod p$. Case I subdivides into three subcases.

Case Ia: $k = 0$ and f is even. In this case the congruence (4) becomes

$$(x-y)e \equiv (p-1)/2 \pmod{p-1} \quad \text{or} \quad x-y \equiv f/2 \pmod f.$$

This congruence has f solutions.

Case Ib: $k = e/2$ and f is odd. Then we have

$$x-y \equiv (f+1)/2 \pmod f.$$

This congruence has also f solutions.

Case Ic: All other values of k. The congruence (4) shows that if f is even then e divides k, which is impossible. When f is odd (4) gives

$$2(x-y) \equiv f \pmod 2.$$

This is also impossible. Thus Case I implies that $C_{00} = f\theta_k$.

Case II: $j \neq 0$. Let $j \in c(h+r)$. Substituting into (4) and dividing both sides by g^{xe+r} gives

$$1 + g^{(y-x)e+k} \equiv g^{(m-x)e+h} \pmod p.$$

This means that, for $j > 0$, $C_{0j} = (k, h)$ in case $j \in c(h+r)$. Hence this proves Theorem 3.

THEOREM 4.

$$\sum_{r=0}^{e-1} H_rH_{r+k} = f(J-I) + (pI-J)\theta_k.$$

Proof. Use Theorems 3 and 2 and (3).

5. The period polynomial. An important feature of cyclotomy is the period polynomial, the irreducible monic polynomial which the e periods satisfy. We use the notation

$$\Phi_e(x) = \prod_{i=0}^{e-1} (x-\eta_i) = x^e + x^{e-1} + \ldots + b_e.$$

That this polynomial plays a role in the theory of the matrices H_r is evident from the following theorems.

THEOREM 5. *The characteristic polynomial of each of the matrices H_r is*

$$\Phi(\lambda) = -(\lambda - f)[\Phi_e(\lambda)]^f.$$

Proof. The characteristic polynomial of H_r is the determinant of the circulant

$$\det(\mathrm{cir}(-\lambda, a_1, a_2, \ldots, a_{p-1}))$$

where

$$a_k = \begin{cases} 1 & \text{if } r \in c(k), \\ 0 & \text{otherwise.} \end{cases}$$

By (1) this determinant is

$$\prod_{v=0}^{p-1} (-\lambda + \sum_{s=1}^{p-1} a_s \zeta^{vs}) = -(\lambda - f) \prod_{v=0}^{e-1} (\lambda - \eta_v)^f = -(\lambda - f)\Phi_e(\lambda)^f.$$

This does not depend on r.

THEOREM 6. *The p eigenvalues of each H_r are the same and consist of f and the e periods $\eta_0, \eta_1, \ldots, \eta_{e-1}$, the eta's having multiplicity f.*

Proof. The result follows directly from Theorem 5.

THEOREM 7. *The determinant of H_r is $f[\Phi_e(0)]^f$.*

Proof. Set $\lambda = 0$ in Theorem 5.

Formulas for $\Phi_e(0)$ in terms of the standard quadratic forms are known for certain values of e. We tabulate them for $e \leqslant 5$ below.

e	$\Phi_e(0)$
1	1
2	$\{p-(-1)^{(p-1)/2}\}/4$
3	$\{((l+3)p-1)/27, (4p = l^2+27m^2), l \equiv 1 \pmod 3\}$
4	$\{(p-1)^2-4p(a-1)^2\}/256$ where $p = a^2+b^2$, $a \equiv 1 \pmod 4$
5	$\{8+8p^2(x+5)-p(x^3+10x^2+40x+80+625w(u^2-v^2)-1250w^2\}/25000$ where $16p = x^2+50u^2+50v^2+125w^2$, $xw = v^2-u^2-4uv$, $x \equiv 1 \pmod 5$.

6. Eigenvectors of H_r. Corresponding to each of the $e+1$ distinct

eigenvalues of H_r, given in Theorem 6, we have an eigenvector depending on one or more free parameters. Let the vector $(y_0, y_1, \ldots, y_{p-1})$ be defined by

$$(x_0, x_1, \ldots, x_{p-1})H_r = (y_0, y_1, \ldots, y_{p-1})$$

where each y_j is a sum of precisely e of the x's. Then if $(x_0, x_1, \ldots, x_{p-1})$ is an eigenvector of H_r corresponding to the eigenvalue λ of H_r, the components x_j must satisfy the following system of p linear equations

$$y_j = \lambda x_j \quad (j = 0, 1, \ldots, p-1). \tag{5}$$

If we choose the eigenvalue f of H_r, we have the comparatively simple result.

THEOREM 8. *Let V be the p-dimensional vector*

$$V = (\alpha, \alpha, \ldots, \alpha) \quad (\alpha \neq 0).$$

Then V is an eigenvector of H_r corresponding to the eigenvalue f of H_r.

Proof. The system (5) becomes

$$y_j = f x_j.$$

One solution is

$$x_0 = x_1 = x_2 = \ldots = x_{p-1} \neq 0$$

because each y is a sum of e nonzero terms. Hence V is an eigenvector of H_r corresponding to the eigenvalue f.

The eigenvector corresponding to the eigenvalue η (any one of the periods) is not so obvious. For $p = 3$, $e = 2$, $f = 1$ we have

$$\eta_0 = \omega, \quad \eta_1 = \omega^2.$$

The eigenvector of H_0 corresponding to η is

$$(\eta x_2, \eta^2 x_2, x_2).$$

The eigenvector of H_1 corresponding to η is

$$(\eta^2 x_2, \eta x_2, x_2).$$

For $p = 5$, $g = 2$, $e = 2$, $f = 2$, the eigenvector of H_0 corresponding to η is

$$(-x_3+\eta x_4, -\eta x_3-\eta x_4, \eta x_3-x_4, x_3, x_4).$$

The eigenvector of H_1 is

$$(x_3-(\eta+1)x_4, (\eta+1)x_3+(\eta+1)x_4, (\eta+1)x_3-x_4, x_3, x_4).$$

7. Symmetry among the H_r. We observe that for $p = 3$, $e = 2$,

$$H_0 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \quad \text{and} \quad H_1 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

are asymmetric matrices, whereas we see in Section 4 for $p = 5$, $g = 2$, $e = 2$, H_0 and H_1 are symmetric. The question of symmetry is answered by

THEOREM 9. *The matrices*

$$H_0, H_1, \ldots, H_{e-1}$$

are all symmetric or all asymmetric according as f is even or odd.

Proof. Suppose that $f = (p-1)/e$ is even. Then

$$-1 \equiv p-1 \equiv g^{(p-1)/2} \equiv g^{ef/2} \equiv (g^{f/2})^e \pmod{p}$$

is an eth power residue of p. Hence if $r \in c(k)$ then $p-r \in c(k)$.

Let $H_k = \operatorname{cir}(0, a_1, a_2, \ldots, a_{p-1}) = \{\alpha_{ij}\}$. Then

$$a_r = a_{p-r} \quad (r = 1, 2, \ldots, p-1).$$

Since H_k is a circulant,

$$\alpha_{ij} = a_{j-i} = a_{p-j+i} = a_{i-j} = \alpha_{ji}.$$

Hence H_k is symmetric.

Conversely, suppose that H_k is symmetric. Then for every ordered pair (i, j) we have

$$a_{j-i} = a_{i-j} \quad \text{or} \quad a_k = a_{p-k} \quad (k = 0, 1, 2, \ldots, p-1).$$

This implies that -1 is an eth power residue of p. But by Euler's criterion it follows that

$$(-1)^f = (-1)^{(p-1)/e} \equiv 1 \pmod{p}.$$

This proves that f is even. This theorem is a paraphrase of the well-known fact that the η's are real if and only if f is even.

8. The discriminant of the H_r. This matrix is defined as the product

$$\Delta = \Delta_e = \prod_{i<j} (H_i - H_j)^2.$$

It is a polynomial in I and J. The simplest case is that of $e = 2$.

THEOREM 10. $\Delta_2 = pI - J$.

Proof. Let $\chi(k)$ be the Legendre symbol mod p. Then

$$H_0 - H_1 = \operatorname{cir}(\chi(0), \chi(1), \ldots, \chi(p-1))$$

and

$$\Delta_2 = (H_0 - H_1)^2 = \operatorname{cir}(b_0, b_1, \ldots, b_{p-1})$$

where

$$b_i = \sum_{j=0}^{p-1} \chi(j)\chi(j+i).$$

Obviously

$$b_0 = p-1.$$

If $i > 0$, the sum b_i is one of Jacobsthal's character sums [1] and equal to -1. Hence

$$\Delta_2 = \operatorname{cir}(p-1, -1, -1, \ldots, -1) = pI - J.$$

THEOREM 11. *Let $p = 3f+1$ and let $4p = l^2 + 27m^2$. Then*

$$\Delta_3 = m^2 p(pI - J).$$

Proof. For $e = 3$ the cyclotomic numbers (i, j) can be expressed in terms of p, l, m (see Storer [2], p. 35). For example,

$$\begin{aligned} 18(0,0) &= 2p-16+2l, \\ 18(0,1) &= 2p-4-l-9m, \\ 18(0,2) &= 2p-4-l+9m, \\ 18(1,2) &= 2p+2+2l, \\ (1,0) &= (2,2) = (0,1), \\ (0,2) &= (1,1) = (2,0), \\ (2,1) &= (1,2). \end{aligned} \tag{6}$$

By Theorem 3 we have

$$\begin{aligned} H_0H_1 &= (1,0)H_0 + (1,1)H_1 + (1,2)H_2, \\ H_1H_2 &= (1,0)H_1 + (1,1)H_2 + (1,2)H_0, \\ H_2H_0 &= (1,0)H_2 + (1,1)H_0 + (1,2)H_1, \\ H_0^2 &= (0,0)H_0 + (0,1)H_1 + (0,2)H_2 + fI, \\ H_1^2 &= (0,0)H_1 + (0,1)H_2 + (0,2)H_0 + fI, \\ H_2^2 &= (0,0)H_2 + (0,1)H_0 + (0,2)H_1 + fI. \end{aligned} \tag{7}$$

By definition,

$$\begin{aligned} \sqrt{\Delta_3} &= (H_0 - H_1)(H_1 - H_2)(H_2 - H_0) \\ &= H_0H_1^2 + H_1H_2^2 + H_2H_0^2 - H_0H_2^2 - H_1H_0^2 - H_2H_1^2. \end{aligned}$$

Using Theorem 3 twice on each of the six terms, multiplying both sides by 18, and using (6) and (7), we can express $\sqrt{\Delta_3}$ as a linear combination of the H's as follows

$$\sqrt{\Delta_3} = m[H_0 + H_1 + H_2 - (p-1)I]. \tag{8}$$

Using Theorem 2 and squaring (8) we obtain

$$\Delta_3 = m^2(J - pI)^2 = m^2(p^2I - 2pJ + pJ) = m^2p(pI - J)$$

which is the theorem.

References

[1] E. Jacobsthal, *Anwendungen einer Formel aus der Theorie der Quadratischen Reste*, Dissertation, Berlin 1906.

[2] Thomas Storer, *Cyclotomy and difference sets*, in *Lectures in Advanced Math.*, vol. 2, Markham, Chicago 1967, vii + 134 pp.

[3] A. L. Whiteman, *A family of symmetric block designs*, J. Combin. Theory, Sec. A, 47 (1988), 153–156.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALIFORNIA
Berkeley, California 94720
U.S.A.

Received on 26.8.1988
and in revised form on 16.11.1988 (1861)

ACTA ARITHMETICA
LIII (1990)

On unit equations with rational coefficients

by

B. BRINDZA* (Sydney) and K. GYŐRY* (Debrecen)

To the memory of Professor V. G. Sprindžuk

1. Introduction. Let K be an algebraic number field of degree n with ring of integers O_K and unit group U_K. Many numbertheoretical problems lead to equations of the types

$$ax+by=c \quad \text{in } x, y\in U_K \tag{1}$$

or more generally

$$ax+by=c \quad \text{in } x, y\in O_K\setminus\{0\} \quad \text{with } \max\{|N_{K/Q}(x)|, |N_{K/Q}(y)|\} \leqslant N \tag{2}$$

where a, b and c are given non-zero elements of K and $N \geqslant 1$ is a given integer. For surveys on equations (1) and (2) and their applications we refer to [15], [8], [9], [10], [20], [11], [18], [6] and [12]. Equation (1) is called a *unit equation*. For $N = 1$, equation (2) becomes equation (1). Further, for $N \geqslant 1$, equation (2) can be reduced to finitely many unit equations. The number of solutions of (1) can be estimated from above by a bound which depends only on n (cf. Evertse [3]). Moreover, most of the unit equations have considerably fewer solutions (cf. Győry [7] and Evertse, Győry, Stewart and Tijdeman [5]). These and other related results will be referred to in more detail at the beginnings of Sections 2 and 3.

The main purpose of the present paper is to considerably refine the results of [7] and [5] in the important special case when the coefficients a, b, c in (1) are rational numbers. Furthermore, we shall establish our results for the more general equation (2) having rational coefficients a, b, c. In this situation (2) cannot be reduced in general to equations of type (1) with rational coefficients. It will be enough to deal with the case when, in (1) and (2), a, b and c are pairwise relatively prime positive integers (cf. Section 2). We shall show (cf. Section 2, Theorem 1) that for all but finitely many triples $(a, b, c)\in N^3$ with coprime a, b, c, equation (2) has at most one, so-called trivial, solution.

* Research supported in part by Grant 273 from the Hungarian National Foundation for Scientific Research.