# Quadratic form made a perfect power by a new composition theorem on arbitrary quadratic forms

Autor(en): **Choudhry, Ajai**

Objekttyp: **Article**

# QUADRATIC FORM MADE A PERFECT POWER
## BY A NEW COMPOSITION THEOREM
## ON ARBITRARY QUADRATIC FORMS

by Ajai CHOUDHRY

ABSTRACT. This paper deals with the diophantine equation $Q(x_1, x_2, \ldots, x_m) = y^n$, where $m$ and $n$ are arbitrary positive integers and $Q(x_1, x_2, \ldots, x_m)$ is an arbitrary quadratic form in the $m$ variables $x_1, x_2, \ldots, x_m$. While solutions of special cases of this equation have been published earlier, the general equation of this type has not been solved till now. To solve this equation, we first show that, given an arbitrary quadratic form $Q(x_1, x_2, \ldots, x_m)$ in $m$ variables, there exists a *composition formula* $Q(u_i) Q^2(v_i) = Q(w_i)$ where $u_i$ and $v_i$ $(i = 1, 2, \ldots, m)$ are arbitrary variables and the $w_i$ $(i = 1, 2, \ldots, m)$ are cubic forms in the variables $u_i$ and $v_i$ $(i = 1, 2, \ldots, m)$. This is a new composition formula, different from the standard composition formulae of the type $Q(u_i) Q(v_i) = Q(w_i)$ which are known for certain classes of quadratic forms. As the equation $Q(x_i) = y^n$ is not always solvable, we prove a theorem giving a necessary and sufficient condition for its solvability. We use the aforementioned composition formula to obtain parametric solutions of the equation $Q(x_i) = y^n$, and also give some numerical examples.

## 1. INTRODUCTION

This paper deals with the diophantine equation

$$(1.1) \qquad Q(x_1, x_2, \ldots, x_m) = y^n,$$

where $m$ and $n$ are arbitrary positive integers and $Q(x_1, x_2, \ldots, x_m)$ is an arbitrary quadratic form in the $m$ variables $x_1, x_2, \ldots, x_m$. The case $m = 2$ has received considerable attention [1, Chapter 20, pp. 533–543] and a number of authors have also considered several special cases when $m \geq 3$ [1, pp. 543–544]. However, the equation does not seem to have been solved in the most general case as represented by equation (1.1).

We first show in Section 2 that, given any arbitrary quadratic form $Q(x_1, x_2, \ldots, x_m)$ in $m$ variables, there exists a very general composition formula of the type

(1.2)        $Q(u_1, u_2, \ldots, u_m) Q^2(v_1, v_2, \ldots, v_m) = Q(w_1, w_2, \ldots, w_m)$,

where the $u_i$ and $v_i$ $(i = 1, 2, \ldots, m)$ are arbitrary variables while the $w_i$ $(i = 1, 2, \ldots, m)$ are cubic forms in the variables $u_i$ and $v_i$.

As we shall see in Section 3, equation (1.1) does not always have a solution in integers. Accordingly, we first prove a theorem in Section 3 giving a necessary and sufficient condition for the solvability of this equation. When equation (1.1) is solvable in integers, it is easy to find a parametric solution such that $x_i$ $(i = 1, 2, \ldots, m)$ are given by polynomials that have a common polynomial factor. We show in Section 3 that, using the identity proved in Section 2, parametric solutions of equation (1.1) can be obtained such that $x_i$ $(i = 1, 2, \ldots, m)$ are given by polynomials that do not have a common polynomial factor. While there are equations of type (1.1) for which solutions in relatively prime integers simply do not exist, when such solutions are possible, the parametric solutions obtained in the paper may yield solutions of (1.1) in relatively prime integers.

## 2.   A COMPOSITION THEOREM ON ARBITRARY QUADRATIC FORMS

In this section we prove a general composition theorem for arbitrary quadratic forms in any number of variables. This theorem establishes the identity (1.2) which is reminiscent of the well-known composition formulae of the type

(2.1)                                $Q(x_i) Q(y_i) = Q(z_i)$,

where $Q(x_i)$ is a certain quadratic form in the variables $x_i$, and the $z_i$ are bilinear forms in the $x_i$ and $y_i$. All the composition formulae of type (2.1) are known [2, pp. 417–427] but in all such formulae there are restrictions on the quadratic forms $Q(x_i)$ as well as on the number of the variables $x_i$. The identity (1.2) differs from the standard composition formulae in view of the squared quadratic form $Q^2(v_i)$ occurring in (1.2) but there is no restriction either on the quadratic form $Q(u_i)$ or on the number of the variables $u_i$.

We note that in the identity (1.2), while the $u_i$ and $v_i$ are completely arbitrary, the $w_i$ $(i = 1, 2, \ldots, m)$ are cubic forms in the $u_i$, $v_i$ such that if $u_i$ $(i = 1, 2, \ldots, m)$ are taken as constants, the $w_i$ become quadratic forms

in the variables $v_i$ whereas if $v_i$ $(i = 1, 2, \ldots, m)$ are taken as constants, the $w_i$ become linear forms in the variables $u_i$.

THEOREM 1. *If $Q(x_1, x_2, \ldots, x_m)$ is an arbitrary quadratic form in $m$ variables $x_1, x_2, \ldots, x_m$, with $m$ being an arbitrary integer, there is an identity given by*

$$(2.2) \qquad Q(u_1, u_2, \ldots, u_m) Q^2(v_1, v_2, \ldots, v_m) = Q(w_1, w_2, \ldots, w_m),$$

*where $u_i$ and $v_i$ $(i = 1, 2, \ldots, m)$ are arbitrary variables while $w_i$ $(i = 1, 2, \ldots, m)$ are cubic forms in the variables $u_i$ and $v_i$ defined by*

$$(2.3) \quad w_i = -v_i \left\{ \sum_{i=1}^{m} v_i \frac{\partial Q(u)}{\partial u_i} \right\} + u_i Q(v_1, v_2, \ldots, v_m), \qquad i = 1, 2, \ldots, m.$$

*Proof.* To prove the identity (2.2), we will first obtain a solution of the following diophantine equation in the variables $t_1, t_2, \ldots, t_m, u_1, u_2, \ldots, u_m$:

$$(2.4) \qquad Q(t_1, t_2, \ldots, t_m) = Q(u_1, u_2, \ldots, u_m).$$

We substitute

$$(2.5) \qquad t_i = v_i \theta + u_i, \qquad i = 1, 2, \ldots, m$$

in equation (2.4), and get

$$(2.6) \qquad Q(v_1, v_2, \ldots, v_m) \theta^2 + \left\{ \sum_{i=1}^{m} v_i \frac{\partial Q(u)}{\partial u_i} \right\} \theta = 0.$$

If $Q(v_1, v_2, \ldots, v_m) \neq 0$, a non-zero solution of this equation is given by

$$(2.7) \qquad \theta = -\left\{ \sum_{i=1}^{m} v_i \frac{\partial Q(u)}{\partial u_i} \right\} / Q(v_1, v_2, \ldots, v_m).$$

With this value of $\theta$, using (2.5), we get a solution of (2.4) given by

$$(2.8) \qquad t_i = \frac{w_i}{Q(v_1, v_2, \ldots, v_m)}, \qquad i = 1, 2, \ldots, m$$

where

$$(2.9) \quad w_i = -v_i \left\{ \sum_{i=1}^{m} v_i \frac{\partial Q(u)}{\partial u_i} \right\} + u_i Q(v_1, v_2, \ldots, v_m), \qquad i = 1, 2, \ldots, m.$$

We now have a solution of (2.4) with $u_i$ $(i = 1, 2, \ldots, m)$ being arbitrary while $t_i$ $(i = 1, 2, \ldots, m)$ are given in terms of $u_i$ $(i = 1, 2, \ldots, m)$ as well

as additional arbitrary parameters $v_i$ ($i = 1, 2, \ldots, m$). Substituting the above values of $t_i$ ($i = 1, 2, \ldots, m$) in (2.4), and multiplying by $Q^2(v_1, v_2, \ldots, v_m)$, we get the identity (2.2). This proves the theorem when $Q(v_1, v_2, \ldots, v_m) \neq 0$. Finally we note that when $Q(v_1, v_2, \ldots, v_m) = 0$, the identity (2.2) is readily verified. This completes the proof.

As an example, we have the identity

$$
\begin{aligned}
(u_1^2 + u_2^2 + u_3^2)(v_1^2 + v_2^2 + v_3^2)^2 = {} & \{(-v_1^2 + v_2^2 + v_3^2)u_1 - 2u_2 v_1 v_2 - 2u_3 v_1 v_3\}^2 \\
& + \{-2u_1 v_1 v_2 + (v_1^2 - v_2^2 + v_3^2)u_2 - 2u_3 v_2 v_3\}^2 \\
& + \{-2u_1 v_1 v_3 - 2u_2 v_2 v_3 + (v_1^2 + v_2^2 - v_3^2)u_3\}^2 \,.
\end{aligned}
$$

As a more general example, we have the identity

$$
(au_1^2 + bu_2^2 + cu_3^2 + du_4^2)(av_1^2 + bv_2^2 + cv_3^2 + dv_4^2)^2 = aw_1^2 + bw_2^2 + cw_3^2 + dw_4^2 \,,
$$

where

$$
\begin{aligned}
w_1 &= (-av_1^2 + bv_2^2 + cv_3^2 + dv_4^2)u_1 - 2bu_2 v_1 v_2 - 2cu_3 v_1 v_3 - 2du_4 v_1 v_4 \,, \\
w_2 &= -2au_1 v_1 v_2 + (av_1^2 - bv_2^2 + cv_3^2 + dv_4^2)u_2 - 2cu_3 v_2 v_3 - 2du_4 v_2 v_4 \,, \\
w_3 &= -2au_1 v_1 v_3 - 2bu_2 v_2 v_3 + (av_1^2 + bv_2^2 - cv_3^2 + dv_4^2)u_3 - 2du_4 v_3 v_4 \,, \\
w_4 &= -2au_1 v_1 v_4 - 2bu_2 v_2 v_4 - 2cu_3 v_3 v_4 + (av_1^2 + bv_2^2 + cv_3^2 - dv_4^2)u_4 \,,
\end{aligned}
$$

with $a$, $b$, $c$, $d$, $u_i$, $v_i$ ($i = 1, 2, 3, 4$) being arbitrary parameters.

## 3. QUADRATIC FORM MADE A PERFECT POWER

In Section 3.1 we consider the solvability of equation (1.1). In the following two subsections, Section 3.2 and Section 3.3, we obtain parametric solutions of equation (1.1) in terms of $m$ arbitrary parameters.

### 3.1 SOLVABILITY OF THE EQUATION $Q(x_i) = y^n$

Equation (1.1) is not always solvable in integers. Apart from the obvious cases when $n$ is even and $Q(x_1, x_2, \ldots, x_m)$ is a negative definite form so that (1.1) cannot have any integer solutions, it is well known that the quadratic equation $Q(x_1, x_2, \ldots, x_m) = y^2$ is not always solvable when $m \leq 4$. For instance, it is readily established that the quadratic equation

$$
\tag{3.1} 2x_1^2 + 3x_2^2 = y^2 \,,
$$

has no solution in integers.

Even when equation (1.1) has an integer solution, it is possible that it may have no solutions in relatively prime integers. As an example, consider the equation

$$(3.2) \qquad 2x_1^2 + 2x_2^2 = y^4.$$

If $x_1$ and $x_2$ are both odd integers, it is easily seen that the left-hand side of (3.2) is $\equiv 4 \pmod{16}$, while if one of the integers $x_1$, $x_2$ is odd and one is even, then the left-hand side of (3.2) is $\equiv 2$ or $10 \pmod{16}$. Since the only fourth power residues modulo 16 are 0 and 1, it is clear that neither can $x_1$ and $x_2$ be both odd nor can one of them be odd and one even. Thus, for any solution of (3.2), both $x_1$ and $x_2$ must be even, and hence cannot be relatively prime. A numerical solution of (3.2) is $x_1 = 2$, $x_2 = 2$. Thus, equation (3.2) has solutions in integers but no solution in relatively prime integers.

We further note that if a solution of (1.1) is given by $x_i = X_i$ ($i = 1, 2, \ldots, m$) and $y = Y$, another solution of (1.1) is given by $x_i = r^n X_i$ ($i = 1, 2, \ldots, m$) and $y = r^2 Y$, where $r$ is an arbitrary parameter. It follows that if we find a solution of (1.1) in rational numbers, or a parametric solution in terms of polynomials with rational numbers as coefficients, by choosing a suitable integer value of $r$, we can readily obtain a solution in integers, or in terms of polynomials with integer coefficients.

We now prove a theorem about the solvability of equation (1.1).

THEOREM 2. *If $Q(x_1, x_2, \ldots, x_m)$ is any arbitrary quadratic form with integer coefficients in $m$ variables $x_1, x_2, \ldots, x_m$, the diophantine equation*

$$(3.3) \qquad Q(x_1, x_2, \ldots, x_m) = y^n$$

*always has a solution in integers when $n$ is odd. Further, when $n$ is even, equation (3.3) has a solution in integers if and only if the quadratic diophantine equation*

$$(3.4) \qquad Q(x_1, x_2, \ldots, x_m) = Y^2$$

*has a solution in integers.*

*Proof.* When $n = 2k + 1$ is an odd integer, a simple parametric solution of (3.3) is given by $x_i = r^k s_i$, $y = r$, where $r = Q(s_1, s_2, \ldots, s_m)$ and the $s_i$ are arbitrary, for with these values of $x_i$, we have $Q(x_i) = r^{2k} Q(s_i) = r^{2k+1} = y^n$. This parametric solution readily yields solutions of equation (3.3) in integers.

When $n = 2k$, any integer solution of equation (3.3) immediately gives an integer solution of (3.4) with $Y = y^k$. Conversely if equation (3.4) has a solution in integers, say, $x_i = s_i$ $(i = 1, 2, \ldots, m)$, $Y = r$, a solution in integers of equation (3.3) is given by $x_i = r^{k-1}s_i$ $(i = 1, 2, \ldots, m)$, $y = r$, since then $Q(x_i) = Q(r^{k-1}s_i) = r^{2k-2}Q(s_i) = r^{2k} = y^n$.

The conditions of solvability of equation (3.4) are well-known [3, p. 42]. Thus, given any arbitrary quadratic form $Q(x_i)$ in any number of variables, we can readily determine whether or not equation (3.3) has a solution in integers. In fact, if (3.4) has an integer solution, we can easily find a parametric solution of (3.4), and use it as indicated above to obtain a parametric solution of (3.3).

While we have obtained parametric solutions of equation (3.3) whenever this equation is solvable, we note that these parametric solutions give values of $x_i$ $(i = 1, 2, \ldots, m)$ in terms of polynomials which necessarily have a common polynomial factor. We will obtain in the next two subsections parametric solutions that do not have this property, and hence may lead to solutions of (3.3) in coprime integers.

### 3.2   THE EQUATION $Q(x_i) = y^n$ WHEN $n$ IS ODD

In this section we consider the equation (3.3) when $n$ is odd, that is, the diophantine equation

$$(3.5) \qquad Q(x_1, x_2, \ldots, x_m) = y^{2k+1},$$

where $k$ is an arbitrary positive integer and $Q(x_1, x_2, \ldots, x_m)$ is an arbitrary quadratic form with integer coefficients in $m$ variables $x_1, x_2, \ldots, x_m$. We will use the composition theorem of Section 2 to obtain parametric solutions of equation (3.5) such that $x_i$ $(i = 1, 2, \ldots, m)$ do not have a common polynomial factor.

Since $u_i$ and $v_i$ $(i = 1, 2, \ldots, m)$ are completely arbitrary in (2.2), we can use this formula $h$ times as follows:

$$
\begin{aligned}
Q(u_i)Q^{2h}(v_i) &= Q(w_i)Q^{2h-2}(v_i) \\
&= Q(w_i')Q^{2h-4}(v_i) \\
&\qquad \vdots \\
&= Q(z_1, z_2, \ldots, z_m),
\end{aligned}
$$

(3.6)

where $z_1, z_2, \ldots, z_m$ are forms of degree $2h + 1$ in the variables $u_i, v_i$ $(i = 1, 2, \ldots, m)$.

Another, more interesting way of using the identity (2.2) is as follows:

$$Q(u_i) \underbrace{Q^2(v_i)Q^2(u_i)Q^2(v_i)Q^2(u_i)\ldots}_{h \text{ terms}} = Q(w_i) \underbrace{Q^2(u_i)Q^2(v_i)Q^2(u_i)\ldots}_{h-1 \text{ terms}}$$

$$= Q(w_i') \underbrace{Q^2(v_i)Q^2(u_i)\ldots}_{h-2 \text{ terms}}$$

(3.7)

$$\vdots$$

$$= Q(z_1, z_2, \ldots, z_m),$$

$$\text{or,} \quad Q^{h_1}(u_i)Q^{h_2}(v_i) = Q(z_1, z_2, \ldots, z_m),$$

where $h_1 = h + 1$, $h_2 = h$ if $h$ is even and $h_1 = h$, $h_2 = h + 1$ if $h$ is odd, and as before, $z_1, z_2, \ldots, z_m$ are forms of degree $2h + 1$ in the variables $u_i$, $v_i$ ($i = 1, 2, \ldots, m$). Naturally, the forms $z_i$ in the identity (3.6) and the forms $z_i$ in the identity (3.7) are different.

If we take $h = k$ and substitute $u_i = s_i$, $v_i = s_i$ ($i = 1, 2, \ldots, m$) in the final identity given either by (3.6) or by (3.7), we get an identity $Q^{2k+1}(s_i) = Q(z_1, z_2, \ldots, z_m)$, and it follows that a solution of (3.5) is given by $x_i = z_i$, $y = Q(s_i)$. However, in both cases the forms $z_i$ ($i = 1, 2, \ldots, m$) reduce respectively to the forms $Q^k(s_i)s_i$ ($i = 1, 2, \ldots, m$) and we get the solution of (3.5) already mentioned in Theorem 1. A similar situation arises if we take $u_i = s_i$, $v_i = -s_i$ ($i = 1, 2, \ldots, m$) and use either of the two identities (3.6) or (3.7).

If, on the other hand, we substitute values of $u_i$, $v_i$ in (3.7) such that $Q(u_i) = Q(v_i)$ but $u_i$ and $v_i$ are not of the type already mentioned, we obtain a parametric solution of (3.5) such that $x_i$ ($i = 1, 2, \ldots, m$) do not have a common polynomial factor. For instance, if $Q(x_i) = \sum_{i=1}^{m} a_i x_i^2$, we may simply take $v_1 = -u_1$, $v_i = u_i$ ($i = 2, 3, \ldots, m$), when we have $Q(u_i) = Q(v_i)$, and substituting these values of $v_i$ in the identity (3.7), we get $Q^{2h+1}(u_i) = Q(z_1, z_2, \ldots, z_m)$, where $z_i$ ($i = 1, 2, \ldots, m$) are forms in the variables $u_i$ and it follows that a parametric solution of equation (3.5) is given by

(3.8)
$$x_i = z_i(u_1, u_2, \ldots, u_m), \qquad i = 1, 2, \ldots, m,$$
$$y = Q(u_1, u_2, \ldots, u_m).$$

This solution gives $x_i$ ($i = 1, 2, \ldots, m$) in terms of polynomials that do not have a common factor.

As an example, a parametric solution of the equation

(3.9)
$$ax_1^2 + bx_2^2 + cx_3^2 = y^7,$$

obtained as described above, is given by

$$
\begin{aligned}
x_1 = (&-a^3 u_1^6 + 21 a^2 b u_1^4 u_2^2 + 21 a^2 c u_1^4 u_3^2 - 35 a b^2 u_1^2 u_2^4 \\
&- 70 abc u_1^2 u_2^2 u_3^2 - 35 a c^2 u_1^2 u_3^4 + 7 b^3 u_2^6 + 21 b^2 c u_2^4 u_3^2 \\
&+ 21 b c^2 u_2^2 u_3^4 + 7 c^3 u_3^6) u_1 \,,
\end{aligned}
$$

$$
\begin{aligned}
x_2 = (&7 a^3 u_1^6 - 35 a^2 b u_1^4 u_2^2 - 35 a^2 c u_1^4 u_3^2 + 21 a b^2 u_1^2 u_2^4 \\
&+ 42 abc u_1^2 u_2^2 u_3^2 + 21 a c^2 u_1^2 u_3^4 - b^3 u_2^6 - 3 b^2 c u_2^4 u_3^2 \\
&- 3 b c^2 u_2^2 u_3^4 - c^3 u_3^6) u_2 \,,
\end{aligned}
$$

(3.10)

$$
\begin{aligned}
x_3 = (&7 a^3 u_1^6 - 35 a^2 b u_1^4 u_2^2 - 35 a^2 c u_1^4 u_3^2 + 21 a b^2 u_1^2 u_2^4 \\
&+ 42 abc u_1^2 u_2^2 u_3^2 + 21 a c^2 u_1^2 u_3^4 - b^3 u_2^6 \\
&- 3 b^2 c u_2^4 u_3^2 - 3 b c^2 u_2^2 u_3^4 - c^3 u_3^6) u_3 \,,
\end{aligned}
$$

$$
y = a u_1^2 + b u_2^2 + c u_3^2 \,,
$$

where $u_1$, $u_2$ and $u_3$ are arbitrary parameters.

As a numerical example, a solution of the equation

$$
(3.11) \qquad\qquad x_1^2 + 2 x_2^2 + 3 x_3^2 = y^7 \,,
$$

obtained by substituting $a = 1$, $b = 2$, $c = 3$, $u_1 = 1, u_2 = 3, u_3 = 4$ in (3.10), is as follows:

$$
(3.12) \qquad x_1 = 1861397, \quad x_2 = -594969, \quad x_3 = -793292, \quad y = 67.
$$

This solution is in coprime integers, that is, $\gcd(x_1, x_2, x_3) = 1$.

When the quadratic form $Q(x_i)$ in equation (3.5) contains terms of the type $x_i x_j$, we can reduce it by an invertible linear transformation to the type $\sum_{i=1}^m a_i X_i^2$, solve the equation $Q(X_i) = y^n$ as described above and thereby obtain a parametric solution for (3.5) in terms of polynomials that do not have a common polynomial factor but which may have coefficients given by rational numbers depending on the initial invertible linear transformation. As observed in Section 3.1, such a solution readily yields a solution in terms of polynomials with integer coefficients.

3.3   THE EQUATION $Q(x_i) = y^n$ WHEN $n$ IS EVEN

When $n$ is an even positive integer, we may write $n = 2^h(2k + 1)$ where $h$ is a positive and $k$ a nonnegative integer, and so equation (3.3) may be written as

$$
(3.13) \qquad\qquad Q(x_1, x_2, \ldots, x_m) = y^{2^h(2k+1)} \,.
$$

We will obtain a parametric solution of this equation if the condition of solvability stated in Theorem 1 is satisfied. Equation (3.13) is equivalent to the following two diophantine equations:

$$(3.14) \qquad Q(x_1, x_2, \ldots, x_m) = y_1^2,$$

$$(3.15) \qquad y_1 = y^{2^{(h-1)}(2k+1)}.$$

When equation (3.13) is solvable in integers, it follows from Theorem 1 that equation (3.14) also has a solution in integers. Any solution of equation (3.14) in integers yields, on appropriate scaling, another solution of (3.14) in rational numbers such that $y_1 = 1$. We use such a solution to obtain a parametric solution of (3.14), substitute the value of $y_1$ so obtained in equation (3.15), and solve the resulting equation.

If $x_i = \xi_i$ $(i = 1, 2, \ldots, m)$, $y_1 = 1$ is a solution in rational numbers of equation (3.14) so that $Q(\xi_i) = 1$, we obtain a parametric solution of this equation by writing

$$(3.16) \qquad \begin{aligned} x_i &= x_{i1}\theta + \xi_i, \qquad i = 1, 2, \ldots, m, \\ y_1 &= 1, \end{aligned}$$

where $x_{i1}$ $(i = 1, 2, \ldots, m)$ are arbitrary parameters. With these values, equation (3.14) gives

$$(3.17) \quad Q(x_{11}, x_{21}, \ldots, x_{m1})\theta^2 + \left\{ \sum_{i=1}^{m} x_{i1} \left( \frac{\partial Q(x)}{\partial x_i} \right)_{x_i=\xi_i} \right\} \theta + Q(\xi_i) = 1.$$

Since $Q(\xi_i) = 1$, we can readily solve (3.17) to get a nonzero value of $\theta$ which on being substituted in (3.16) gives a solution of equation (3.14) that may be written, after multiplying by $Q(x_{11}, x_{21}, \ldots, x_{m1})$, as follows:

$$(3.18) \qquad x_i = Q_i(x_{11}, x_{21}, \ldots, x_{m1}), \qquad i = 1, 2, \ldots, m,$$

$$(3.19) \qquad y_1 = Q(x_{11}, x_{21}, \ldots, x_{m1}),$$

where $Q_i(x_{11}, x_{21}, \ldots, x_{m1})$ $(i = 1, 2, \ldots, m)$ are certain quadratic forms in $m$ arbitrary parameters $x_{11}, x_{21}, \ldots, x_{m1}$. Substituting this value of $y_1$ in equation (3.15), we get the equation

$$(3.20) \qquad Q(x_{11}, x_{21}, \ldots, x_{m1}) = y^{2^{(h-1)}(2k+1)}.$$

Since $Q(x_{11}, x_{21}, \ldots, x_{m1})$ is a quadratic form in $m$ arbitrary variables $x_{i1}$ $(i = 1, 2, \ldots, m)$, equation (3.20) is exactly of the same type as equation (3.13) and is equivalent to the following two equations:

$$(3.21) \qquad Q(x_{11}, x_{21}, \ldots, x_{m1}) = y_2^2,$$

$$(3.22) \qquad y_2 = y^{2^{(h-2)}(2k+1)}.$$

We now obtain a solution of (3.21) in terms of $m$ new arbitrary parameters $x_{i2}$ ($i = 1, 2, \ldots, m$) and proceeding as before, we substitute the value of $y_2$ in equation (3.22) to obtain the equation

$$(3.23) \qquad Q(x_{12}, x_{22}, \ldots, x_{m2}) = y^{2^{(h-2)}(2k+1)},$$

where $x_{12}, x_{22}, \ldots, x_{m2}$ are $m$ arbitrary parameters. Equation (3.23) is again of the same type as equation (3.13), and by repeating this process $h$ times, we will obtain the equation

$$(3.24) \qquad Q(x_{1h}, x_{2h}, \ldots, x_{mh}) = y^{2k+1},$$

where $x_{1h}, x_{2h}, \ldots, x_{mh}$ are $m$ arbitrary parameters.

We can obtain a parametric solution of equation (3.24) as described in Section 3.2, and working backwards, we successively obtain parametric solutions of all intermediate equations such as (3.23) and (3.20), and eventually we obtain a parametric solution of equation (3.13). In general, the values of $x_i$ ($i = 1, 2, \ldots, m$) and $y$ given by this solution are in terms of polynomials that do not have a common polynomial factor. Further, these polynomials may have rational coefficients but, as already noted, we can readily use such a solution to obtain a solution in terms of polynomials with integer coefficients.

As an example, a parametric solution of the equation

$$(3.25) \qquad X_1^2 + 2X_2^2 + 3X_3^2 = Y^8,$$

obtained by the above method, is as follows:

$$
\begin{aligned}
(3.26) \quad
X_1 &= -x_1^8 + 56x_1^6x_2^2 + 84x_1^6x_3^2 - 280x_1^4x_2^4 - 840x_1^4x_2^2x_3^2 \\
&\quad - 630x_1^4x_3^4 + 224x_1^2x_2^6 + 1008x_1^2x_2^4x_3^2 + 1512x_1^2x_2^2x_3^4 \\
&\quad + 756x_1^2x_3^6 - 16x_2^8 - 96x_2^6x_3^2 - 216x_2^4x_3^4 - 216x_2^2x_3^6 - 81x_3^8, \\
X_2 &= 8x_1x_2(-x_1^2 + 2x_2^2 + 3x_3^2) \\
&\quad \times (x_1^4 - 12x_1^2x_2^2 - 18x_1^2x_3^2 + 4x_2^4 + 12x_2^2x_3^2 + 9x_3^4), \\
X_3 &= 8x_1x_3(-x_1^2 + 2x_2^2 + 3x_3^2) \\
&\quad \times (x_1^4 - 12x_1^2x_2^2 - 18x_1^2x_3^2 + 4x_2^4 + 12x_2^2x_3^2 + 9x_3^4), \\
Y &= x_1^2 + 2x_2^2 + 3x_3^2,
\end{aligned}
$$

where $x_1, x_2$ and $x_3$ are arbitrary parameters. Taking $x_1 = 1, x_2 = 4, x_3 = 2$, we get the following solution of (3.25) in coprime integers:

$$x_1 = -1497233, \quad x_2 = 2302048, \quad x_3 = 1151024, \quad Y = 45.$$

We also note that if we substitute in (3.26) the values of $x_1, x_2$ and $x_3$

obtained by taking $a = 1$, $b = 2$, $c = 3$ in (3.10), we will get a parametric solution of the diophantine equation

$$(3.27) \qquad X_1^2 + 2X_2^2 + 3X_3^2 = Y^{56} .$$

While this solution is cumbersome to write, substituting in (3.26) the numerical values of $x_1$, $x_2$ and $x_3$ stated in (3.12), we find the following solution of equation (3.27) in coprime integers:

$X_1 = -113196439558029506112128478909351707306431 8753427441 ,$

$X_2 = -271146391211682226276577890818469441 4526742521916520,$

$X_3 = -361528521615576350354371877579592552702323362555360,$

$Y = 67.$

The above method does not always yield solutions in coprime integers of a given equation of type (3.13). This is not surprising since, as seen in Section 3.1, solutions in coprime integers do not always exist. We give below an example where the parametric solution obtained as described above does not give a solution in coprime integers.

A parametric solution of the diophantine equation

$$(3.28) \qquad 2x_1^2 + 3x_2^2 + 7x_3^2 = y^8 ,$$

obtained by the above method, is as follows:

$$\begin{aligned}
x_1 = &- 21552u_1^8 - 3234147u_3^8 - 3619728u_1^3u_2^4u_3 + 76952736u_1^3u_2^2u_3^3 \\
&+ 25873176u_1^2u_3^6 - 177147u_2^8 + 26046048u_1^5u_3^3 - 18480840u_1^4u_3^4 \\
&- 91161168u_1^3u_3^5 + 2112096u_1^6u_3^2 - 51152472u_1^2u_2^4u_3^2 \\
&+ 137433240u_1^2u_2^2u_3^4 + 7715736u_1u_2^6u_3 - 5630688u_1^5u_2^2u_3 \\
&+ 966168u_1^4u_2^4 - 33030900u_2^2u_3^6 + 45580584u_1u_3^7 + 6062364u_2^6u_3^2 \\
&+ 1547910u_2^4u_3^4 - 1063104u_1^7u_3 - 16532208u_1^4u_2^2u_3^2 \\
&- 59344488u_1u_2^4u_3^3 - 25412184u_1u_2^2u_3^5 + 1102248u_1^2u_2^6 + 143136u_1^6u_2^2 ,
\end{aligned}$$

$$\begin{aligned}
x_2 = &\, 24u_2(2u_1 + 7u_3)(-10u_1^2 + 56u_1u_3 - 27u_2^2 + 35u_3^2) \\
&\times (124u_1^4 + 2240u_1^3u_3 - 108u_1^2u_2^2 - 2604u_1^2u_3^2 \\
&\quad + 6048u_1u_2^2u_3 - 7840u_1u_3^3 - 729u_2^4 + 7182u_2^2u_3^2 + 1519u_3^4) ,
\end{aligned}$$

$$x_3 = 37968u_1^8 + 5697573u_3^8 + 4953312u_1^3u_2^4u_3 - 24018624u_1^3u_2^2u_3^3$$
$$- 45580584u_1^2u_3^6 - 177147u_2^8 + 4224192u_1^5u_3^3 + 32557560u_1^4u_3^4$$
$$- 14784672u_1^3u_3^5 - 3720864u_1^6u_3^2 - 14410872u_1^2u_2^4u_3^2$$
$$+ 84280392u_1^2u_2^2u_3^4 + 5353776u_1u_2^6u_3 + 737856u_1^5u_2^2u_3 + 476280u_1^4u_2^4$$
$$+ 2309076u_2^2u_3^6 + 7392336u_1u_3^7 + 9369108u_2^6u_3^2 - 35316162u_2^4u_3^4$$
$$- 172416u_1^7u_3 - 17675280u_1^4u_2^2u_3^2 - 67305168u_1u_2^4u_3^3$$
$$+ 88037712u_1u_2^2u_3^5 + 157464u_1^4u_2^6 + 252000u_1^6u_2^2,$$

$$y = 9(2u_1^2 + 3u_2^2 + 7u_3^2),$$

where $u_1$, $u_2$ and $u_3$ are arbitrary parameters. Here the values of $x_1$, $x_2$ and $x_3$ are always divisible by 3 but not necessarily by a larger factor. Taking $u_1 = 1$, $u_2 = 2$, $u_3 = 3$ in the above solution, we get the following solution of (3.28):

$$x_1 = -20601098187, \quad x_2 = 86152445040, \quad x_3 = 65551346853, \quad y = 693,$$

for which $\gcd(x_1, x_2, x_3) = 3$.

REFERENCES

[1]    DICKSON, L. E. *History of the Theory of Numbers. Vol. II : Diophantine Analysis.* Chelsea Publishing Co., New York, 1966. (Unaltered reprint of the 1920 original.)

[2]    JACOBSON, N. *Basic Algebra. I.* W. H. Freeman and Co., San Francisco, Calif., 1974.

[3]    MORDELL, L. J. *Diophantine Equations.* Pure and Applied Mathematics *30.* Academic Press, London-New York, 1969.

*(Reçu le 2 février 2010)*

Ajai Choudhry, Dean

Foreign Service Institute
Old J. N. U. Campus
Baba Gang Nath Marg
New Delhi 110067
India
*e-mail :* ajaic203@yahoo.com