REMARKS ON TERNARY DIOPHANTINE EQUATIONS

KURT MAHLER, University of Manchester

Let $F(x, y)$ be a binary form of order $n \geqq 3$ with integral coefficients, $k \neq 0$ an integer, $P_1, \cdots, P_t$ a finite set of different prime numbers. The following results have been proved:*

THEOREM 1. *If the equation*

$$F(x, y) = k$$

has an infinity of integral solutions x, y, then $F(x, y)$ is a power of a linear form or of an indefinite quadratic form.

THEOREM 2. *If the equation*

$$F(x, y) = \mp P_1^{z_1} \cdots P_t^{z_t}$$

has an infinity of integral solutions $x, y, z_1, \cdots, z_t$, where x and y are relatively prime, and $z_1 \geqq 0, \cdots, z_t \geqq 0$, then $F(x, y)$ is a power of a linear or quadratic form.

Now consider a ternary form $F(x, y, z)$ of order $n \geqq 3$ with integral coefficients, and the representations of integers $k \neq 0$ by this form. If $F(x, y, z)$ is decomposable into a product of linear forms with algebraic coefficients and if n is sufficiently large, then results analogous to Theorem 1 and 2 are true.† On the other hand, very little is known about the more general case when $F(x, y, z)$ is irreducible in the field of all constants. In this note, I construct examples of ternary forms of every order with the property of representing at least one integer $k \neq 0$, or even every integer, in an infinity of different ways. I further show how to form positive definite ternary forms of every even order with the property that for an infinity of different sets of relatively prime integers x, y, z the greatest prime factor of $F(x, y, z)$ is bounded. Special cases of forms with these properties are well known; *e.g.*, the equation

$$x^3 + y^3 + z^3 = 1$$

has an infinity of integral solutions, since identically in t,

$$(9t^4)^3 + (3t - 9t^4)^3 + (1 - 9t^3)^3 = 1;$$

and the equation

$$x^4 + y^4 + z^4 = 2 \cdot 7^{z_1}$$

has an infinity of integral solutions with relatively prime x, y, z, since identically in x and y,‡

* A. Thue, Norske Vid. Selsk. Skr. 1908, Nr. 7. K. Mahler, Math. Ann. 107, 1933, pp. 691–730.

† C. L. Siegel, Math. Z. 10, 1921, pp. 173–213.

E. T. Parry, Journal of the London Mathematical Society, 1940, vol. 15, pp. 293–305.

‡ The equation $x^2+xy+y^2=7^z$ has an infinity of integral solutions with relatively prime x, y.

$$x^4 + y^4 + (x + y)^4 = 2(x^2 + xy + y^2)^2.$$

The stated results are obtained by the construction of simple identities. In a similar way, it is possible to show the following theorem: "*If $F(x, y, z)$ is an irreducible cubic form with integral coefficients, such that the equation $F(x, y, z) = 0$ has at least one solution in integers not all zero, then $F(x, y, z)$ either represents all integers in a suitable linear progression $at+b$* ($t=0, \mp 1, \mp 2, \cdots$) *or it represents a certain integer $k \neq 0$ in an infinity of different ways.*" Let g, h, k be three integers not all zero such that

$$F(g, h, k) = 0,$$

and denote with F_g, F_h, F_k the values of the three first partial derivatives $\partial F/\partial x$, $\partial F/\partial y$, $\partial F/\partial z$ for $x=g$, $y=h$, $z=k$. There are three integers not all zero such that

$$GF_g + HF_h + KF_k = 0.$$

Let now t be a parameter; then

$$F(gt + G, ht + H, kt + K) = At^3 + Bt^2 + Ct + D$$

is a cubic polynomial in t. This polynomial cannot vanish identically, since $F(x, y, z)$, by hypothesis, is irreducible. It is however at most of the first degree. For the assumptions about g, h, k; G, H, K are equivalent to $A=B=0$. According as to whether $C\neq 0$ or $C=0$, F represents all integers of the progression $Ct+D$, or is equal to D for all values of t. In the second case $D\neq 0$, since $F\not\equiv 0$.

1. Ternary equations with an infinity of solutions. The general ternary form $F(x, y, z)$ of order n has

$$N = \frac{(n + 1)(n + 2)}{2}$$

coefficients. If

$$p_1(t), \quad p_2(t), \quad p_3(t) \qquad \left(\sum_{h=1}^{3} |\, p_h(t)\,| > 0 \text{ for all } t\right)$$

are three polynomials in a parameter t with integral coefficients and of degree less than or equal to ν, then

$$F(p_1(t), p_2(t), p_3(t)) = \phi(t)$$

is a polynomial in t of degree not greater than $n\nu$; its coefficients are linear forms in the coefficients of $F(x, y, z)$ with integral numerical coefficients; say

$$\phi(t) = \sum_{h=0}^{n\nu} L_h(F)t^h.$$

If $\phi(t)$ is to be a constant, then the coefficients of $F(x, y, z)$ must satisfy the $n\nu$ linear equations

$$L_h(F) = 0 \qquad (h = 1, 2, \cdots, n\nu).$$

For $N > n\nu$, this system has always a non-trivial solution in integers; there is therefore then a ternary form of order n with integral coefficients not all zero such that

$$F(p_1(t), p_2(t), p_3(t)) = L_0(F)$$

is independent of t. The so constructed form $F(x, y, z)$ may, however, be reducible, and the constant $L_0(F)$ on the right-hand side may vanish. In the special case $\nu = 1$ of linear polynomials $p_h(t)$ both complications can always be avoided, and it is possible to determine irreducible forms $F(x, y, z)$ of every order n such that the constant $\phi(t) = L_0(F) \neq 0$.*

The form $F(x, y, z)$ constructed in this manner is *not* definite; it assumes the values $k = L_0(F)$ for every integral value $t = 0, \mp 1, \mp 2, \cdots$. I give here a few examples of this kind:

$x^3 + y^3 + z^3 + \lambda xyz = \lambda^3 + 27$ identically in t for $x = t + \lambda$, $y = -t$, $z = 3$;

$y^2 z - 12x^3 + 3z^3 = 12$ identically in t for $x = t + 1$, $y = 3t$, $z = t + 2$;

$2x^4 - y^4 - z^4 + 2x^2y^2 + 2x^2z^2 - 4y^2z^2 = -6$ identically in t for $x = t$, $y = t + 1$, $z = t - 1$;

$2(x^4 + y^4) - (x - y)^2 z(3x - 3y + z) = 4$ identically in t for $x = t + 1$, $y = t - 1$, $z = t^2$.

2. Forms which represent every integer. Let α, β, γ be three integers and assume that the form $F(x, y, z)$ of order n has the following property:

"On replacing z by $\alpha x + \beta y + \gamma$, we get identically in x and y,

$$(1) \qquad F(x, y, \alpha x + \beta y + \gamma) = p(x) + ay,$$

where a is a constant and $p(x)$ a polynomial in x both depending on F."

Assume the form has this property, and let

$$\xi_1, \xi_2, \cdots, \xi_s$$

be the different residues of $p(x)$ mod a; since

$$p(x) \equiv p(x') \bmod a \quad \text{for} \quad x \equiv x', \bmod a,$$

each congruence

$$p(x) \equiv \xi_\sigma \bmod a \qquad (\sigma = 1, 2, \cdots, s)$$

has an infinity of integral solutions x. Hence if k is any integer in one of the residue classes

$$k \equiv \xi_\sigma \bmod a \qquad (\sigma = 1, 2, \cdots, s),$$

then

$$p(x) + ay = k$$

* This corresponds to the fact that there are irreducible algebraic curves of every order n which intersect a given straight line only in n coinciding points.

has an infinity of integral solutions x, y, and therefore the equation $F(x, y, z)=k$ has an infinity of integral solutions, x y, z.

The following forms satisfy the identity (1):

$$\begin{aligned} F_l(x, y, z) &= x^{n-l}(z - \beta y)^l \qquad (l = 0, 1, \cdots, n-1); \\ F_n(x, y, z) &= y(z - \alpha x - \beta y)^{n-1}, \end{aligned} \tag{2}$$

as is evident on putting $z=\alpha x+\beta y+\gamma$. A further and less obvious solution is obtained in the following way:

We assume that this solution can be written as

$$\begin{aligned} F_{n+1}(x, y, z) = z^n &+ yf_1(x, y)z^{n-2} + yf_2(x, y)z^{n-3} + \cdots \\ &+ yf_{n-2}(x, y)z + yf_{n-1}(x, y), \end{aligned} \tag{3}$$

where $f_k(x, y)$, for $k=1, 2, \cdots, n-1$, is a binary form in x, y of order k with integral coefficients. Evidently none of the forms (2) is of this type.

From (1) and (3), we get

$$\begin{aligned} F_{n+1}(x, y, \alpha x + \beta y + \gamma) &= (\alpha x + \beta y + \gamma)^n + yf_1(x, y)(\alpha x + \beta y + \gamma)^{n-2} + \cdots \\ &\quad + yf_{n-1}(x, y) \\ &= p(x) + ay. \end{aligned}$$

Hence, on developing both sides into sums of binary forms in x, y and comparing forms of equal order,

$$\begin{aligned}
&(\alpha x+\beta y)^n+yf_1(x, y)(\alpha x+\beta y)^{n-2}+\cdots+yf_{n-2}(x, y)(\alpha x+\beta y)+yf_{n-1}(x, y) &&=c_nx^n,\\
&\binom{n}{1}(\alpha x+\beta y)^{n-1}+\binom{n-2}{1}yf_1(x, y)(\alpha x+\beta y)^{n-3}+\cdots+\binom{1}{1}yf_{n-2}(x, y) &&=c_{n-1}x^{n-1},\\
&\binom{n}{2}(\alpha x+\beta y)^{n-2}+\binom{n-2}{2}yf_1(x, y)(\alpha x+\beta y)^{n-4}+\cdots+\binom{2}{2}yf_{n-3}(x, y) &&=c_{n-2}x^{n-2},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&\binom{n}{n-2}(\alpha x+\beta y)^2+\binom{n-2}{n-2}yf_1(x, y) &&=c_2x^2,\\
&\binom{n}{n-1}(\alpha x+\beta y) &&=c_1x+\binom{n}{n-1}ay.
\end{aligned}$$

Here the c's are suitable constants; their values are found by putting $y=0$, namely:

$$c_n = \alpha^n,\ c_{n-1} = \binom{n}{1}\alpha^{n-1},\ c_{n-2} = \binom{n}{2}\alpha^{n-2}, \cdots, c_1 = \binom{n}{n-1}\alpha.$$

Let

$$d_k(x, y) = d_k = (\alpha x)^k - (\alpha x + \beta y)^k \quad (k = 2, 3, \cdots, n).$$

Then the last equations take the form,

$$\begin{aligned}
&yf_1(x, y)(\alpha x+\beta y)^{n-2}+yf_2(x, y)(\alpha x+\beta y)^{n-3}+\cdots+yf_{n-1}(x, y)=d_n,\\
&\binom{n-2}{1}yf_1(x, y)(\alpha x+\beta y)^{n-3}+\binom{n-3}{1}yf_2(x, y)(\alpha x+\beta y)^{n-4}+\cdots+\binom{1}{1}yf_{n-2}(x, y)=\binom{n}{1}d_{n-1},
\end{aligned}$$

$$\binom{n-2}{2} yf_1(x, y)(\alpha x+\beta y)^{n-4}+\binom{n-3}{2} yf_2(x, y)(\alpha x+\beta y)^{n-5}+\cdots+\binom{2}{2} yf_{n-3}(x, y)=\binom{n}{2} d_{n-2},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\binom{n-2}{n-2} yf_1(x, y) \qquad\qquad = \binom{n}{n-2} d_2.$$

This system of linear equations for

$$yf_1(x, y),\ yf_2(x, y), \cdots, yf_{n-1}(x, y)$$

is easily solved just in the required form; for the expressions on the right-hand side are all divisible by y. We find for small values of n:

$$n = 1: F_2(x, y, z) = z;$$

$$n = 2: F_3(x, y, z) = z^2 + d_2;$$

$$n = 3: F_4(x, y, z) = z^3 + 3d_2z + (d_3 - 3(\alpha x + \beta y)d_2);$$

$$\begin{aligned} n = 4: F_5(x, y, z) &= z^4 + 6d_2z^2 + 4(d_3 - 3(\alpha x + \beta y)d_2)z + (d_4 - 4(\alpha x + \beta y)d_3 \\ &\quad + 6(\alpha x + \beta y)^2d_2); \end{aligned}$$

$$\begin{aligned} n = 5: F_6(x, y, z) &= z^5 + 10d_2z^3 + 10(d_3 - 3(\alpha x + \beta y)d_2)z^2 + 5(d_4 - 4(\alpha x + \beta y)d_3 \\ &\quad + 6(\alpha x + \beta y)^2d_2) + (d_5 - 5(\alpha x + \beta y)d_4 + 10(\alpha x + \beta y)^2d_3 \\ &\quad - 10(\alpha x + \beta y)^3d_2). \end{aligned}$$

It is also clear that the following formulae hold:

$$\begin{aligned} F_l(x, y, \alpha x + \beta y + \gamma) &= x^{n-l}(\alpha x + \gamma)^l \qquad (l = 0, 1, \cdots, n - 1); \\ F_n(x, y, \alpha x + \beta y + \gamma) &= \gamma^{n-1}y; \qquad\qquad (4) \\ F_{n+1}(x, y, \alpha x + \beta y + \gamma) &= (\alpha x + \gamma)^n + n\beta\gamma^{n-1}y. \end{aligned}$$

Assume in particular that

$$\alpha \neq 0, \qquad \beta \neq 0, \qquad \gamma \neq 0.$$

Then the $n+2$ forms (2) and (3) are linearly independent; for the polynomials in x

$$x^{n-l}(\alpha x + \gamma)^l \qquad (l = 0, 1, \cdots, n - 1)$$

are clearly linearly independent, since no two of them vanish to the same order at $x=0$ or at $x=-\gamma/\alpha$. Therefore the form of order n,

$$F(x, y, z) = \sum_{l=0}^{n+1} C_lF_l(x, y, z), \tag{5}$$

where $C_0, C_1, \cdots, C_{n+1}$ are arbitrary integers not all zero, does not vanish identically; it is again a solution of (1).

Take

$$\gamma = 1, \qquad C_n + C_{n+1}n\beta = 1$$

and choose F such that $F(x, 0, \alpha x+\gamma)$ is a polynomial in x exactly of degree n. Then by the remark at the beginning of this paragraph, $F(x, y, z)$ represents every integer in an infinity of different ways. We furthermore have

$$F(x, y, \alpha x + \beta y + \gamma) = F(x, 0, \alpha x + \gamma) + y,$$

and conclude that $F(x, y, z)$ is an irreducible form in x, y, z, since the expression on the right-hand side is irreducible in x and y and of exact degree n in x. It is again clear, as in the preceding paragraph, that the so constructed form, $F(x, y, z)$ is indefinite.

3. Forms with bounded greatest prime factor. A positive definite ternary form of order n, $F(x, y, z)$, represents every integer k in at most a finite number of ways. Since $F(x, y, z)$ is positive definite, its order is even, say $n=2m$. The values of F on the sphere $x^2+y^2+z^2=1$ are always positive; since F is continuous, they have a minimum value $V>0$ on this sphere. Hence

$$f(x, y, z) = \frac{F(x, y, z)}{(x^2 + y^2 + z^2)^m} \geqq V$$

for all points of this sphere, and therefore for all points of space, since $f(x, y, z)$ is homogeneous of order zero. Hence, if $k>0$ is given and $F=k$, then

$$k = F(x, y, z) \geqq V(x^2 + y^2 + z^2)^m, \quad i.e. \quad |x|, |y|, |z| \leqq (k/V)^{1/2m},$$

so that there are at most a finite number of integral solutions x, y, z.

Suppose in particular, that this form can be written as

$$F(x, y, z) = aQ(x, y)^m + (z - x - y)G(x, y, z), \tag{6}$$

where $a\neq 0$ is an integer and

$$Q(x, y) = \alpha x^2 + \beta xy + \gamma y^2$$

is a quadratic form in x and y, and $G(x, y, z)$ a form of order $n-1$ in x, y, z, both with integral coefficients. Since

$$F(x, y, x + y) = aQ(x, y)^m, \tag{7}$$

the form $Q(x, y)$ must be positive or negative definite; otherwise there would be real x, y, z not all zero such that $F(x, y, z)=0$.

By the theory of quadratic forms, it is possible to find for every integer $t\geqq 1$ a system of t different prime numbers

$$P_1, P_2, \cdots, P_t,$$

such that the equation

$$Q(x, y) = \mp P_1^{z_1} \cdots P_t^{z_t}$$

has an infinity of integral solutions $x, y, z_1, \cdots, z_t$, where x and y are relatively prime and $z_1\geqq 0, \cdots, z_t\geqq 0$. Hence, by (7), there exist an infinity of different sets of three relatively prime integers x, y, z, for which the greatest prime divisor of $F(x, y, z)$ is bounded.

It is possible to find positive definite forms $F(x, y, z)$ of every even order $n=2m$, which can be written as a sum (6). For instance, it suffices to take

$$G(x, y, z) = (z - x - y)H(x, y, z),$$

where $H(x, y, z)$ is a positive definite form of order $n-2=2(m-1)$. Or we may take $G(x, y, z)$ arbitrary, but such that $G(0, 0, 1)>0$, and then can make $F(x, y, z)$ positive definite by just choosing for a a sufficiently large positive integer.

In the excluded case that $Q(x,y)$ is indefinite, $F(x,y, z)$ evidently represents an infinity of different integers k in an infinity of different ways.

As there are many forms of the type (6), we may impose on them further conditions, *e.g.*, consider only forms which are quadratic or cubic forms in x^h, y^h, z^h. In the following examples, the sign "→" means that the right-hand side is derived from the left-hand side by the substitution $z=x+y$.

(a) Quadratic forms in x^2, y^2, z^2. A few examples are given by the identities, in which α is arbitrary:

$$(1 - \alpha)x^4 + \alpha x^2y^2 + \alpha x^2z^2 + \alpha^2y^2z^2 \to (x^2 + \alpha xy + \alpha y^2)^2;$$

$$\alpha x^4 + \alpha(4\alpha - 1)y^4 + \alpha z^4 + (1 - 2\alpha)x^2z^2 \to (x^2 + xy + 2\alpha y^2)^2.$$

(b) Quadratic forms in x^3, y^3, z^3. The following identities hold for arbitrary α:

$$(\alpha^2 - 4\alpha + 4)(x^6 + y^6) + (\alpha^2 - \alpha + 1)z^6 + (3\alpha^3 - 16\alpha^2 + 28\alpha - 16)x^3y^3$$
$$- (2\alpha^2 - 5\alpha + 2)(x^3 + y^3)z^3 \to 3(x^2 + \alpha xy + y^2)^3;$$

$$(\alpha^2 - 3\alpha + 3)x^6 + \alpha^2(y^6 + z^6) + (2\alpha^2 - 3\alpha)x^3(y^3 - z^3) + (3\alpha^3 - 2\alpha^2)y^3z^3$$
$$\to 3(x^2 + \alpha xy + \alpha y^2)^3;$$

$$\alpha(x^6 + z^6) + (3\alpha^3 - 3\alpha^2 + \alpha)y^6 + (2\alpha - 3\alpha^2)y^3(x^3 - z^3) + (3 - 2\alpha)x^3z^3$$
$$\to 3(x^2 + xy + \alpha y^2)^3.$$

(c) A quadratic form in x^4, y^4, z^4:

$$x^8 + y^8 + 17z^8 + 14(x^4 + y^4)z^4 \to 2(2x^2 + 3xy + 2y^2)^4.$$

(d) There is no irreducible cubic form in x^4, y^4, z^4 with rational coefficients, but there are four with coefficients in $K(\sqrt{3})$ which are conjugate in pairs with respect to this field.

Final remark. Analogous to (6), there are positive definite quaternary forms $F(x, y, z, w)$ of every even order $n=2m$ which can be written as

$$F(x, y, z, w) = aQ(x, y, z)^m + (w - x - y - z)G(x, y, z, w),$$

where $a\neq 0$ is an integer, $Q(x, y, z)$ a positive definite quadratic form and $G(x, y, z, w)$ a form of order $n-1$. For forms F of this kind, the equation $F(x, y, z, w)=k$ has evidently at least const. $|k|^{1/n}$ solutions for an infinity of k's.