MATH. SCAND. 2 (1954), 29–32

ON THE DIOPHANTINE EQUATION $|Ax^n - By^n| = 1$, $n \geqq 5$

YNGVE DOMAR

In a recently published thesis by Häggmark [1], it is shown that the Diophantine equation $x^5 - My^5 = 1$, where M is an integer, has at most two integral solutions apart from the trivial solution $x = 1$, $y = 0$. Actually a considerably stronger theorem is true. It seems to have been overlooked that the Thue-Siegel method can give much more information about the maximum number of integral solutions. In fact, the following theorems are easily obtainable after simple modifications in the final phase of the proof of a theorem by Siegel [2]:

THEOREM 1. *The equation*

$$|Ax^n - By^n| = 1 , \tag{1}$$

where A and B are positive integers and $n \geqq 5$, has at most two solutions in positive integers (x, y).

THEOREM 2. *The equation*

$$|x^n - My^n| = 1 ,$$

where M is a positive integer and $n \geqq 5$, has at most one solution in positive integers (x, y) except possibly for $M = 2$ and if $n = 5$ or 6 for $M = 2^n \pm 1$.

Siegel considers the inequality $|Ax^n - By^n| \leqq C$, $n \geqq 3$, where the variables and the constants are positive integers, and he assumes that two different solutions exist. By means of an approximation to the function $(1-z)^{1/n}$ in the interval $(0, 1)$ by rational functions with integral coefficients, and with the help of some simple inequalities, he shows that if certain conditions are imposed on the coefficients A, B, C, the above assumption involves a contradiction, so that two solutions cannot exist.

Let us suppose that (1) has two different solutions (x, y) and (x_1, y_1) in positive integers and let $x \leqq x_1$. It is easily seen that $x \leqq x_1$ implies $y \leqq y_1$. It is convenient to introduce $w = Ax^n$, $w_1 = Ax_1^n$ if $Ax^n > By^n$, otherwise $w = By^n$, $w_1 = By_1^n$. In both cases we obtain $w_1 \geqq w \geqq 2$.

Received April 19, 1953.

In the following we disregard the trivial case $A = B = 1$.

Siegel introduces the constants

$$s_r = \binom{2r}{r} q_r n^r , \qquad t_r = q_r n^r \prod_{m=1}^{r} (1 - m^{-1} n^{-1}) ,$$

where r is a positive integer and q_r denotes the product of all factors of the prime number decomposition of r which divide n.

If we take $C = 1$ in Siegel's proof, it is easy to see that the two assumed solutions of (1) cannot exist if two inequalities

$$6(n, 2) n^2 w^2 \leqq n^{-1} M^{1/n} w^{-1/n} w_1^{(n-1)/n} , \tag{2}$$

$$M w^{(r+1)(n-2)-2} \geqq t_r^{n-1} s_{r+2} n (1 - 1/n)^{1-n} , \tag{3}$$

where $M = AB$, are simultaneously true, the latter for every positive r. (Siegel's inequalities (40) and (47).)

Supposing that $n \geqq 5$, we can obtain the following inequalities, which are stronger than the corresponding relations (26) and (36) in Siegel's proof:

$$t_r^{n-1} s_{r+2} n (1 - 1/n)^{1-n} \leqq \lambda_n^{r+1-1/(n-2)} , \qquad r \geqq 1 , \tag{4}$$

where

$$\lambda_n = 4 n^n \prod_{p \mid n} p^{n/(p-1)} , \qquad p \text{ prime} ,$$

and

$$w_1 > M n^n (w - 1)^{n-1} . \tag{5}$$

The proof of inequality (4) involves only simple refinements of Siegel's equations, which are possible since $n \geqq 5$. Inequality (5) can be proved in the following way:

We may suppose that $w = Ax^n$, that is, $By^n = w - 1$, $Ax_1^n = w_1$, $By_1^n = w_1 \pm 1$.

Since $Ax^n - By^n = 1$, we have

$$(A^{1/n} x - B^{1/n} y)^{-1} = (Ax^n)^{(n-1)/n} + \ldots + (By^n)^{(n-1)/n} > n (Ax^n)^{(n-1)/(2n)} (By^n)^{(n-1)/(2n)} ,$$

and hence

$$|1 - (BA^{-1})^{1/n} y x^{-1}| < n^{-1} (Ax^n)^{-(n+1)/(2n)} (By^n)^{-(n-1)/(2n)} = D .$$

In a similar way

$$|1 - (BA^{-1})^{1/n} y_1 x_1^{-1}| < n^{-1} (Ax_1^n)^{-(n+1)/(2n)} (By_1^n)^{-(n-1)/(2n)} = D_1 .$$

Since $w_1 \geqq 2$, $n \geqq 5$, it follows that $D_1 \leqq w_1^{-1}$; and from the two above inequalities we obtain

$$(xx_1)^{-1}(BA^{-1})^{1/n} \leqq |(yx_1 - xy_1)(xx_1)^{-1}(BA^{-1})^{1/n}| < D + D_1 ,$$

which implies

$$(6)\quad 1 < w_1^{1/n} n^{-1} M^{-1/n} w^{-(n-1)/(2n)} (w-1)^{-(n-1)/(2n)} + w^{1/n} M^{-1/n} w_1^{-(n-1)/n} .$$

The right-hand member of (6) is a convex function of $w_1^{1/n}$, and the inequality does not hold for $w_1 = w$, since $w \geqq 2$, $M \geqq 2$. If it does not hold for $w_1 = M n^n (w-1)^{n-1}$ either, inequality (5) must be true. Putting this value of w_1 into the right-hand member of (6) we obtain:

$$\begin{aligned}(1 - 1/w)^{(n-1)/2n} + w^{1/n} M^{-1} n^{-(n-1)} (w-1)^{-(n-1)^2/n} \\ < (1 - 1/w)^{(n-1)/(2n)} + n^{-1} w^{-(n-2)} \\ < 1 - (n-1)(2n)^{-1} w^{-1} + n^{-1} w^{-(n-2)} \\ < 1 .\end{aligned}$$

Hence (5) is true.

Inequality (3) holds because of (4) if for every $r \geqq 1$

$$(7)\qquad M w^{(r+1)(n-2)-2} \geqq \lambda_n^{\,r+1-1/(n-2)} ,$$

that is, if

$$(8)\qquad w \geqq \lambda_n^{\,1/(n-2) + 1/(2(n-2)(n-3))} .$$

It is easy to see that (7) is also valid if

$$(9)\qquad \max(A, B) \geqq \lambda_n^{\,1/(n-2)} .$$

Consider for instance the case when the maximum equals A so that $A \geqq \lambda_n^{\,1/(n-2)}$. Since $w = Ax^n$ or $w = Ax^n + 1 > Ax^n$ inequality (7) is implied by

$$B x^{n(r+1)(n-2) - 2n} \geqq 1 ,$$

which is obviously true. The case $\max(A, B) = B$ can be treated similarly.

According to (5), inequality (2) is valid if

$$(10)\qquad 6 n^{4-n} (n, 2) \leqq M w^{-2-1/n} (w-1)^{(n-1)^2/n} .$$

From (8) or (9) it follows that $w^{n-2} \geqq \lambda_n$. Now λ_n is obviously $> n^n$ and $n \geqq 5$; thus $w > 5$. The right-hand side of (10) can be written

$$M \{(w-1) w^{-3/4}\}^{(2+1/n)4/3} (w-1)^{n - 14/3 - 1/(3n)} ,$$

which is $\geqq 2$ since $M \geqq 2$ and the two last factors are $\geqq 1$ for $w > 5$. The left-hand side of (10) is $\leqq \frac{6}{5}$. Thus (10) is proved and from this inequality it follows that (2) is true if (8) or (9) holds. Hence (8) and (9)

are alternative sufficient conditions for the non-existence of the two assumed solutions of (1).

We are now in a position to prove theorem 1. If three solutions exist, at least two of them should correspond to values of w exceeding n^n because of (5). But this implies that (8) is valid, which yields the theorem.

To prove theorem 2, we put $A = 1$, whence $B = M$. In this case w has to be of the type a^n or a^n+1, where $a \geqq 1$. A comparison with (8) shows that the only possibilities are $a = 1$ and, if $n = 5$ or 6, $a = 2$. (If the right hand side of (8) is denoted by k^n simple calculations show that $2 < k < 3$ when $n = 5$, 6 and $1 < k < 2$ when $n = 7$. By the help of the inequality $\lambda_n \leqq 2^{2+2/n} n^{3n/2}$ it follows that $1 < k < 2$ for $n > 7$.) Theorem 2 follows.

Consider equation (1), and suppose that $A \geqq B$. By application of (8) and (9) it is easy to specify the cases where two solutions could possibly exist. Simple calculations show that the number of such equations is for every $n \geqq 5$ less than $n + c \log n$, where c is a constant, independent of n.

BIBLIOGRAPHY

1. P. Häggmark, *On a class of quintic Diophantine equations in two unknowns*, Dissertation, Uppsala, 1952.
2. C. L. Siegel, *Die Gleichung* $ax^n - by^n = c$, Math. Ann. 114 (1937), 57–68.

UNIVERSITY OF UPPSALA, SWEDEN