On the diophantine equations 2y2 = 7k + 1 and x2 + 11 = 3n

$$x=\left(\frac{r}{2}-\rho\right)\cos\omega+\frac{3r}{2}\cos\frac{\omega}{3},\qquad y=\left(\frac{r}{2}-\rho\right)\sin\omega+\frac{3r}{2}\sin\frac{\omega}{3} \tag{23}$$

beschrieben, die als Einhüllende der Spitzentangenten auftretende Astroide (vierspitzige Hypozykloide) durch

$$x=-\frac{m}{2}\left(\cos\omega+3\cos\frac{\omega}{3}\right),\ y=-\frac{m}{2}\left(\sin\omega-3\sin\frac{\omega}{3}\right)\quad\text{mit}\quad m=\frac{r}{2}-\rho. \tag{24}$$

Satz 3 steht überdies in gewissem Zusammenhang mit Untersuchungen von Fréchet [3], welche die Beweglichkeit einer starren Ellipse in einer sie dreifach berührenden Steiner-Zykloide erkennen lassen und die von Wunderlich [6], Meyer [5] und anderen verallgemeinert wurden. Ernst Ungethüm, Wien

LITERATURVERZEICHNIS

1 G. Berkhan und W.F. Meyer: Neuere Dreiecksgeometrie. Enzykl. Math. Wiss. III AB 10.
2 F. Dingeldey: Kegelschnitte und Kegelschnittsysteme. Enzykl. Math. Wiss. III C 1.
3 M. Fréchet: Sur quelques propriétés de l'hypocycloïde à trois rebroussements. Nouv. Ann. *61*, 206-217 (1902).
4 R. Henke und R. Heger: Schloemilchs Handbuch der Mathematik, I., 2. Aufl. Leipzig 1904.
5 P. Meyer: Über Hüllkurven von Radlinien. Arch. Math. *18*, 651-662 (1967).
6 W. Wunderlich: Über Gleitkurvenpaare aus Radlinien. Math. Nachr. *20*, 373-380 (1959).
7 W. Wunderlich: Ebene Kinematik. Hochschultaschenbücher, Bd. 447. Mannheim, Wien, Zürich 1970.

On the diophantine equations $2y^2=7^k+1$ and $x^2+11=3^n$

Certain diophantine equations have played an important role in the recent development of the mathematical theory of error-correcting codes. One of these equations is

$$2y^2=7^k+1, \tag{1}$$

for which Alter [1] has proved the following result.

Theorem 1. *The only solutions in positive integers y, k of the equation (1) are* (2, 1) *and* (5, 2).

Alter's proof, which is based on the theory of continued fractions, is quite long and complicated. Therefore, it may be of some interest that theorem 1 can be demonstrated very briefly by appealing to the following theorem of Ljunggren's [8].

Theorem 2. *The diophantine equation*

$$\frac{x^n-1}{x-1}=y^2 \quad (n>2)$$

is impossible in integers x, y, $|x|>1$ with the exception of the cases $n=4$, $x=7$ and $n=5$, $x=3$.

This theorem is based on a fairly comprehensive theory which is, however, completely elementary.

In order to prove theorem 1 it is enough to show that (1) is impossible for $k>2$. Suppose that (1) holds for some integers $y>0$, $k>2$. We distinguish three cases.

If k is odd, then $2|y$, i.e. $y=2y_1$ with a positive integer y_1. Now (1) can be written in the form

$$\frac{(-7)^k-1}{-7-1}=y_1^2.$$

By theorem 2 this is impossible.

If $k=2(2h+1)$ with h an integer >0, then $(7^2+1)|(7^k+1)$. Hence $5|y$, i.e. $y=5y_2$, and (1) takes the form

$$\frac{(-49)^{2h+1}-1}{-49-1}=y_2^2.$$

Again, by Ljunggren's theorem, this is impossible because of $h>0$. Lastly, let $k=4h$. Now (1) becomes $(7^h)^4+1=2y^2$. This equation is impossible, since $h>0$ and the only integer solutions of $x^4+y^4=2z^2$ with $(x,y)=1$ are given by $x^2=y^2=1$ (cf. e.g. [9], p. 18). This completes the proof of theorem 1.

We shall now deal with the equation

$$x^2+11=3^n, \tag{2}$$

for which the following result holds.

Theorem 3. *The only positive integer solution of equation (2) is given by* $(x,n)=(4,3)$.

It seems that the first proof for this theorem is given by Alter and Kubota [2]. [An error in the proof of the case $n\equiv 7 \pmod{10}$ was later corrected by the second author [5]. By the way, we may note that the correction can be demonstrated very briefly as follows: Since $3|n$, we have $n\equiv -3 \pmod{30}$ and so, by (2) and Fermat's theorem, $3^3x^2\equiv 3^{n+3}+4\cdot 11\equiv -48 \pmod{31}$ or $(3x)^2+4^2\equiv 0 \pmod{31}$, which is impossible, since $(-1/31)=-1$.]

Very recently Cohen [4] has proved theorem 3 using the interesting method developed by Hasse [6]. However, an earlier proof given by Cohen and Ljunggren [3] is much simpler. Our following proof is slightly dissimilar to the latter.
Firstly we show that $3 \mid n$. The equation (2) can be written in the forms

$$x^2+8=3(3^{n-1}-1), \qquad x^2+2=9(3^{n-2}-1).$$

The right-hand side is divisible by 3^3-1 $(=2\cdot 13)$ in the first equation for $n\equiv 1 \pmod 3$ and in the second one for $n\equiv 2 \pmod 3$. But $(-2/13)=-1$ and thus the cases $n\equiv 1,\ 2 \pmod 3$ are excluded. Now (2) has the form $x^2+11=y^3$. We do not wish to make use of the well-known result [7] that the only solutions in positive integers of this equation are given by (4, 3) and (58, 15), but we carry through the proof completely.
In the quadratic field $Q(\sqrt{-11})$ unique factorization holds, the only units are ± 1, and g.c.d. $(x+\sqrt{-11}, x-\sqrt{-11})=1$, whence

$$x+\sqrt{-11}=\left(\frac{a+b\sqrt{-11}}{2}\right)^3, \qquad 4y=a^2+11b^2, \tag{3}$$

where a, b are rational integers. From these equations it follows that

$$3a^2b-11b^3=8, \qquad a^2b-by=2.$$

Hence $|b|=1$ or 2 and so $a^2=1$ or 16, respectively. The second equation in (3) then gives $y=3$, $x=4$ and $y=15$, $x=58$ as only solutions of $x^2+11=y^3$. Since y is a power of 3 in the case we are considering, it follows that $x=4$, $n=3$ is the only solution of (2).

K. Inkeri, University of Turku, Finland

REFERENCES

1 R. Alter: On the nonexistence of close-packed double Hamming error-correcting codes on $q=7$ symbols. J. Comput. Syst. Sci. *2*, 169–176 (1968).
2 R. Alter and K.K. Kubota: The diophantine equation $x^2+11=3^n$ and a related sequence. J. Number Theory *7*, 5–10 (1975).
3 E.L. Cohen: Sur l'équation diophantienne $x^2+11=3^k$. C.r. Acad. Sci. Paris (A) *275*, 5–7 (1972).
4 E.L. Cohen: The diophantine equation $x^2+11=3^k$ and related questions. Math. Scand. *38*, 240–246 (1976).
5 E.L. Cohen: Review of [2], MR 51, No.344, p.48 (1976).
6 H. Hasse: Über eine diophantische Gleichung von Ramanujan-Nagell und ihre Verallgemeinerung. Nagoya Math. J. *27*, 77–102 (1966).
7 O. Hemer: On the diophantine equation $y^2-k=x^3$. Doct. Diss., Uppsala 1952.
8 W. Ljunggren: Noen setninger om ubestemte likninger av formen $(x^n-1)/(x-1)=y^q$. Norsk. Mat. Tidsskr. *1*, H. 25, 17–20 (1943).
9 L.J. Mordell: Diophantine equations. Academic Press, New York, London 1969.