102

Square classes of $(a^n-1)/(a-1)$ and a^n+1

Sichuan Daxue Xuebao, 26, 1989, 196-199.

四川大学学报（自然科学版）
Journal of Sichuan University Natural Science Edition Vol.26 Special Issue

Square Classes of $\frac{a^n-1}{a-1}$ and a^n+1

Paulo Ribenboim

(Queen's University, Kingston, Ontario, Canada)

ABSTRACT

Let $a>1$, $n\geq 1$ and $U_n=\frac{a^n-1}{a-1}$, $V_n=a^n+1$. In this paper, the author investigate whether U_mU_n, respectively V_mV_n, may be a square when $m\neq n$, and gives a completed answer.

Key Words Linear recurring sequences of order 2, Diophantine equations, Effectively computable constant.

(1980 AMS Subject Classification (1985 Revision) 11D41, 11B37)

1. In 1960/4, Professor Chao Ko solved a long standing open problem, when he showed that if $n>3$, the Diophantine equation $X^2-Y^n=1$ has no solution in non-zero integers.

In the present paper, just like in [Ri1], I shall use his result.

Let $a>1$, $n\geq 1$ and $U_n=\frac{a^n-1}{a-1}$, $V_n=a^n+1$. Thus $U_0=0$, $U_1=1$ and $U_n=(a+1)U_{n-1}-aU_{n-2}$ for $n\geq 2$. Similarly $V_0=2$, $V_1=a+1$, $V_n=(a+1)V_{n-1}-aV_{n-2}$ for $n\geq 2$.

In this paper, I shall investigate whether U_mU_n, respectively V_mV_n, may be a square when $m\neq n$. This is just a special case of the problem of determination of the square classes of linear recurring sequences of order 2. It is said that U_n, U_m (respectively V_n, V_m) are in the same square class if there exist non-zero integers k,h, such that $U_nk^2=U_mh^2$, or equivalently $U_mU_n=\square$ (respectively $V_nh^2=V_mh^2$, $V_mV_n=\square$).

For the determination of the square classes of the sequences of Fibonacci numbers and Lucas numbers, see [Ri2].

Besides the aforementioned result of Chao Ko, the following facts will be required.

As it is well-known, $\gcd(U_m,U_n)=U_d$, where $d=\gcd(m,n)$.

Received March 12, 1990

For the sequence $(V_n)_{n>0}$ a similar result was only partially known, until the recent (still unpublished) result of McDaniel [McD]:

Denoting by v_2 the 2-adic valuation,

$$\gcd(V_m,V_n)=\begin{cases} V_d, & \text{if } v_2(m)=v_2(n), \text{ with } d=\gcd(m,n), \\ 1 \text{ or } 2, & \text{if } v_2(m)\neq v_2(n). \end{cases}$$

Nagell [Na] and Ljunggren [Lj] proved:

If $n>2$, $|x|>1$, $y\geqslant 1$ are integers and $\dfrac{x^n-1}{x-1}=y^2$, then $(x,n,y)=(7,4,\pm 20)$ or $(3,5,\pm 11)$.

Fermat stated that if a,x,y are integers, $a\geqslant 1$, and $\begin{cases} a+1=2x^2 \\ a^2+1=2y^2, \end{cases}$ then $(a,x,y)=(1,\pm 1,\pm 1)$ or $(7,\pm 2,\pm 5)$. This result was proved by Genocchi [Ge].

Finally, I shall also require the following theorem of Schinzel & Tijdeman [S-T]:

Let $f\in \mathbb{Q}[X]$ be a polynomial with at least two simple zeroes. Then there exists an effectively computable constant $C>0$ (depending only on f), such that if x,y,z are integers with $|y|\geqslant 2$, $z\geqslant 3$ and $f(x)=y^z$, then $|x|,|y|,z<C$.

2. Now I prove the new results.

A) If $1\leqslant m,n$ and U_mU_n is a square, then $m=n$.

Proof Assume that $\dfrac{a^n-1}{a-1}\cdot\dfrac{a^m-1}{a-1}$ is a square. Let $d=\gcd(m,n)$, so $\dfrac{a^d-1}{a-1}=\gcd\left(\dfrac{a^m-1}{a-1},\ \dfrac{a^n-1}{a-1}\right)$, hence $\dfrac{a^m-1}{a^d-1}$, $\dfrac{a^n-1}{a^d-1}$ are relatively prime and their product is a square. Let $n=dt$, $m=du$ (with t,u integers), let $b=a^d$. So

$$\frac{b^t-1}{b-1}=\square,\quad \frac{b^u-1}{b-1}=\square.$$

By the result of Nagell and Ljunggren, $(b,t)=(7,4)$ or $(3,5)$, hence $d=1$, $b=a$, $n=t$, $m=u$, thus $(a,n)=(7,4)$ or $(3,5)$. So $\dfrac{7^m-1}{6}=\square$, thus $m=4=n$, or $\dfrac{3^m-1}{2}=\square$, thus $m=5=n$.

B) If $n\geqslant 1$ there does not exist m, different from n, with $v_2(m)=v_2(n)$ and such that V_mV_n is a square.

Proof Assume that $v_2(m)=v_2(n)$ and $V_mV_n=\square$. Let $d=\gcd(m,n)$, $n=dt$, $m=du$, so t,u are odd. Since $V_d=\gcd(V_m,V_n)$, then

$$\frac{a^n+1}{a^d+1}=\square \text{ and } \frac{a^m+1}{a^d+1}=\square.$$

Let $b=a^d>1$. Since $m\neq n$ then, say, $t>1$. Since t is odd and $\dfrac{b^t+1}{b+1}=\square$, hence

$$\frac{(-b)^y-1}{(-b)-1}=\square.$$

According to the result of Nagell and Ljunggren, this is impossible.

C) If a is even and if $n\geqslant 1$, there does not exist m, different from n, such that V_mV_n is a square.

Proof I may assume that $v_2(n)\neq v_2(m)$. Since a is even, by the result of McDaniel, $\gcd(a^m+1, a^n+1)=1$, hence $a^m+1=\square$, $a^n+1=\square$. Necessarily m,n are different from 2. Since $v_2(1)=v_2(3)=0$, then $(m,n)=(1,3)$ and $(3,1)$ have been excluded. Therefore $m,n\geqslant 3$ and, say $m>3$. By Ko's result, $a^m+1\neq\square$ is impossible.

D) There exists an effectively computable constant $C>0$ such that if a is odd, if m,n are different and $V_mV_n=\square$, then $a,m,n<C$.

Proof Consider the polynomial $f=2X^2-1$, which has two simple roots. By the theorem of Schinzel and Tijdeman, there exists an absolute constant $C>7$ such that if $a>1$, $m\geqslant 3$, $|x|\geqslant 1$ and $2x^2-1=a^m$, then $|x|,a,m\leqslant C$.

Now assume that a is odd, $m\neq n$, and $V_mV_n=\square$. By (B), $v_2(m)\geqslant v_2(n)$, hence $\gcd(V_m,V_n)=2$. Thus $\frac{a^m+1}{2}=\square$ and $\frac{a^n+1}{2}=\square$.

Thus there exist positive integers x,y such that $\begin{cases} 2x^2-1=a^m, \\ 2y^2-1=a^n. \end{cases}$

Assume, for example, that $1\leqslant n<m$. The following possibilities are arised:

a) $n=1$, $m=2$, hence $\begin{cases} a+1=2x^2, \\ a^2+1=2y^2. \end{cases}$

By Fermat-Genocchi's result, either $a=1$ (which is against the hypothesis) or $a=7$, hence $x=2$, $y=5$.

b) $m\geqslant 3$. Then $a,n,m\leqslant C$.

E) Let $a>1$ be odd, let C be defined as in (D). For every $n, 1\leqslant n\leqslant C$, the number of integers $m\neq n$, such that $V_mV_n=\square$, is at most equal to $\left[\frac{\log C}{\log 2}\right]$.

Proof Let $m\neq n$ be such that $V_mV_n=\square$. By the above results, $m\leqslant C$ and $v_2(m)\neq v_2(n)$.

Let $k=\left[\frac{\log C}{\log 2}\right]$, and consider the mapping $m\longmapsto v_2(m)\in\{0,1,\cdots,k\}\setminus\{v_2(n)\}$.

This mapping is injective: if $m\neq m'$ and $V_nV_m=\square$, $V_nV_{m'}=\square$ (with m,m' different from n) then $V_n^2V_mV_{m'}=\square$, so $V_mV_{m'}=\square$; hence by (B), $v_2(m)\neq v_2(m')$.

Thus, the number of $m\neq n$, such that $V_mV_n=\square$ is at most $\left[\frac{\log C}{\log 2}\right]$.

BIBLIOGRAPHY

[Ge] Genocchi A., Démonstration d'un théorème de Fermat, *Nouv. Ann. Math. Ser.* 3, 2(1883), 306—310.

[Ko1] Ko C., On the diophantine equation $x^2=y^n+1$, *Acta. Sci. Natur. Univ. Szechuan* 2(1960), 57—64.

[Ko2] Ko C., On the diophantine equation $x^2=y^n+1$, *Scientia Sinica* (*Notes*) 14(1964), 457—460.

[Lj] Ljunggren W., New propositions about the indeterminiate equation $\frac{x^n-1}{x-1}=y^q$, *Norske Mat. Tidsskrift* 25(1943), 17—20.

[McD] McDaniel W. L., The g.c.d. in Lucas sequences and Lehmer number sequences, preprint.

[Na] Nagell T., Sur l'équation indéterminée $\frac{x^n-1}{x-1}=y^2$, *Norsk Mat. For. Skr., Ser.* I 3(1921), 17 pages.

[Ri1] Ribenboim P., Remarks on exponential congruences and powerful numbers, *J. Nb. Th.* 29(1988), 251—263.

[Ri2] Ribenboim P., Square classes of Fibonacci and Lucas numbers, *Port. Math.* 46(1989), 159—175.

[S-T] Schinzel A. & Tijdeman R., On the equation $y^m=P(x)$, *Acta. Arithm.* 31(1976), 199—204.

$\frac{a^n-1}{a-1}$ 和 a^n+1 的平方类

P. Ribenboim

(Queen's 大学，加拿大)

摘　要

设 $a>1$, $n\geqslant 1$, $U_n=\frac{a^n-1}{a-1}$, $V_n=a^n+1$. 本文研究当 $m\neq n$, U_mU_n(V_mV_n) 是否能够是一个完全平方的问题，得到了完全解决。

关键词 二阶线性循环序列，丢番图方程，可有效计算的常数。