COLLOQUIUM MATHEMATICUM

VOL. X 1963 FASC. 1

# *REMARQUE AU TRAVAIL DE W. SIERPIŃSKI SUR LES NOMBRES* $a^{2^n}+1$

PAR

A. SCHINZEL (VARSOVIE)

Les théorèmes du travail qui précède* peuvent être généralisés comme suit.

THÉORÈME 1. *Si* $1 < a < 8(2^4+1)(2^8+1)(2^{12}+1)$, *il existe un nombre composé de la forme* $a^{2^n}+1$ *où* $1 \leqslant n \leqslant 15$.

THÉORÈME 2. *S'il existe une infinité de nombres premiers de Fermat, il existe pour tout* $a > 1$ *naturel qui n'est pas de la forme* $a = 2^{2^k}$ *une infinité de nombres composés de la forme* $a^{2^n}+1$.

Démonstration du théorème 1. Si l'on a $F_i \nmid a(a^2-1)$ pour un $i \leqslant 4$ naturel, on a aussi $F_i \mid a^{F_i-1}-1$ en vertu du théorème d'Euler et comme

$$a^{F_i-1} = (a^2-1)\prod_{j=1}^{2^i-1}(a^{2^j}+1),$$

on conclut que $F_i \mid a^{2^j}+1$ pour un $j \leqslant 2^i-1 \leqslant 15$.

Si $F_i \neq a^{2^j}+1$, le nombre $a^{2^j}+1$ est composé et si $F_i = a^{2^j}+1$, on a $a = 2^{2^{i-j}}$ pour $j \leqslant i$ et le nombre $a^{2^{5-i+j}}+1 = F_5$ est composé.

Il reste à examiner les $a > 1$ naturels tels que

$$F_1F_2F_3F_4 \mid a(a^2-1). \tag{1}$$

Remarquons d'abord que la divisibilité $F_1F_2 \mid a(a^2-1)$ entraîne pour $a$ naturels que $a = 1$, ou bien $a = 16$, ou bien $a \geqslant 34$. En admettant donc pour $a \geqslant 1$ que

$$F_1F_2F_3 \mid a(a^2-1), \tag{2}$$

on a $a = F_3t+\varepsilon$ (pour $t \geqslant 0$ et $\varepsilon = 0$ ou $\varepsilon = \pm 1$) et vu que $F_3 \equiv 2 \pmod{F_1F_2}$, on conclut que $F_1F_2 \mid (2t+\varepsilon)[(2t+\varepsilon)^2-1]$.

---

* W. Sierpiński, *Sur les nombres composés de la forme* $a^{2^n}+1$, ce fascicule, p. 133-135.

D'après la remarque qui précède, il y a par suite 3 cas possibles, à savoir $2t+\varepsilon=1$, $2t+\varepsilon=16$ et $2t+\varepsilon\geqslant 34$, qui donnent respectivement $t=0$, $\varepsilon=1$ et $a=1$, ou bien $t=1$, $\varepsilon=-1$ et $a=F_3-1=2^8$, ou bien $t=8$, $\varepsilon=0$ et $a=8F_3$, ou bien $t\geqslant 17$, $\varepsilon\geqslant 0$ et $a\geqslant F_2F_3$, ou enfin $t\geqslant 18$ et $a\geqslant 18F_3-1$. Donc, (2) entraîne pour $a\geqslant 1$ que

(3) $a=1$, ou bien $a=2^8$, ou bien $a=8F_3$, ou bien $a\geqslant F_2F_3$.

Ceci établi, examinons les $a>1$ naturels assujettis à (1). On a $a = F_4t+\varepsilon$ (où $t\geqslant 1$ et $\varepsilon=0$ ou $\varepsilon=\pm 1$) et vu que $F_4\equiv 2 \pmod{F_1F_2F_3}$, on conclut que $F_1F_2F_3\,|\,(2t+\varepsilon)[(2t+\varepsilon)^2-1]$.

D'après (3), on a ici $2t+\varepsilon=1$, ou bien $2t+\varepsilon=2^8$, ou bien $2t+\varepsilon=8F_3$, ou enfin $2t+\varepsilon\geqslant F_2F_3$, ce qui donne 5 cas possibles suivants:

1. $t=1$, $\varepsilon=-1$, $a=F_4-1=a_1$;
2. $t=2^7$, $\varepsilon=0$, $a=2^7F_4=a_2$;
3. $t=4F_3$, $\varepsilon=0$, $a=4F_3F_4=a_3$;
4. $t=\frac{1}{2}(F_2F_3-1)$, $\varepsilon=1$, $a=\frac{1}{2}F_4(F_2F_3-1)+1=a_4$;
5. $t\geqslant\frac{1}{2}(F_2F_3+1)$, $a\geqslant\frac{1}{2}F_4(F_2F_3+1)-1=a_5$.

Or $a_1^2+1=F_5$, $13\,|\,a_2^2+1$, $37\,|\,a_3^2+1$, $2\,|\,a_4^2+1$ et $a_5=8(2^4+1)\times(2^8+1)(2^{12}+1)$, ce qui achève la démonstration.

Démonstration du théorème 2. Soient $a$ et $m$ des nombres naturels quelconques dont $a>1$. Il existe par hypothèse un nombre premier de Fermat $F_i$ tel que $F_i\nmid a(a^{2^m}-1)$. On a $F_i\,|\,a^{F_i-1}-1$ en vertu du théorème d'Euler et comme

$$a^{F_i-1}-1=(a^{2^m}-1)\prod_{j=m}^{2^i-1}(a^{2^j}+1),$$

on a $F_i\,|\,a^{2^j}+1$ pour un $j\geqslant m$.

Si $a^{2^j}+1=F_i$, il vient $a=2^{2^{i-j}}$, ce qui est incompatible avec l'hypothèse. On a donc $a^{2^j}+1\neq F_i$ et le nombre $a^{2^j}+1$ (où $j\geqslant m$) est composé.

*Reçu par la Rédaction le 29. 1. 1962*

COLLOQUIUM MATHEMATICUM

VOL. X 1963 FASC. 1

# *REMARK ON RATIONAL TRANSFORMATIONS*

BY

W. NARKIEWICZ (WROCŁAW)

In [1] and [2] it was proved that if a field $K$ is finitely generated over the rationals, and $X$ is an infinite subset of $K$, then every polynomial mapping $X$ onto itself must be linear. It seems to be true that every rational function mapping an infinite subset $X$ of such a field onto itself must be a homography. The purpose of this note is to prove this in the case of the field $R$ of rational numbers.

Let $R_\infty$ be the set obtained by adjoining an ideal element $\infty$ to $R$. For every rational function $F(t)$ we put $F(\infty)=\lim_{|t|\to\infty}|F(t)|$ and if $z$ is a pole of $F(t)$, then we put $F(z)=\infty$. We shall prove the following

THEOREM. *If $X$ is an infinite subset of $R_\infty$, and $F(t)$ a rational function, such that $X\subset F(X)$, then $F(t)=(at+b)/(ct+d)$ with suitable rational $a$, $b$, $c$, $d$.*

A. Schinzel posed the following problem (see [3]):

Let $f(x,y)$ be a polynomial with rational coefficients, and $X$ an infinite set of rational numbers with the property that for every $x$ in $X$ there exists such an $y$ in $X$ that $f(x,y)=0$. Prove that $f(x,y)$ must have a factor which is linear in $y$ or symmetrical in $x$, $y$.

As a corollary of our theorem we obtain a positive solution of that problem in the case of $f(x,y)=P(y)-Q(y)x$.

LEMMA 1. *Suppose that $X$ is a set and $T$ a transformation mapping a subset $X_0$ of $X$ onto $X$. Suppose moreover that there exists a function $s(x)$ defined on $X$ with values in the set of natural numbers subject to conditions:*

(i) *For every constant $c$ the equation $s(x)=c$ has only a finite number of solutions.*

(ii) *There exists a constant $C$ such that from $s(x)\geqslant C$ follows $s(Tx)>s(x)$.*

*Then the set $X$ is finite.*

Proof of the lemma. If $X=X_0$, then the finiteness of $X$ follows from lemma 1 in [1] if we put there $f(x)=s(x)$, $g(x)=1$ for all $x$ and