On the solution in natural numbers of the equation $x^m - y^n = 1$ *

by R. HAMPEL (Warszawa)

In this article I intend to demonstrate the impossibility in natural numbers of the equation $x^m - y^n = 1$ for the case $|x-y|=1$. In other words I shall prove that the equalities

$$n^{a+s} - (n+1)^a = \pm 1 \quad \text{for} \quad n \geqslant 2, \quad a \geqslant 2, \quad s \geqslant 1$$

have only the trivial solution $n=2$, $a=2$, $s=1$.

Let us take first $n^{a+s} - (n+1)^a = 1$ or

$$n^{a+s} - \sum_{k=0}^{a-1} \binom{a}{k} n^{a-k} - 2 = 0. \tag{1}$$

The only possible natural solution (>1) of (1) is 2 and we get

$$2^{a+s} - 3^a = 1, \quad a \geqslant 2, \quad s \geqslant 1. \tag{2}$$

Using the dual system of computation we may write equation (2) in the form

$$2^{a+s} - 1 = \underbrace{(11\ldots1)_2}_{a+s \text{ ciphers}} = 3^a = (11)_2^a. \tag{3}$$

(The number of figures on the right side of (3) is $[a \log_2 3]+1$, the figure c_r on the r-place from the end amounts to

$$c_r = [3^a 2^{1-r}] - 2[3^a 2^{-r}] \quad (r = 1, 2, \ldots, [a \log_2 3]+1),$$

$a+s \geqslant 3$, *i. e.* we have at least 3 ciphers on both sides of equality (3).)

If $a \equiv 0 \pmod 2$ then $(11)_2^a = (\ldots 001)_2$; if $a \equiv 1 \pmod 2$ then $(11)_2^a = (\ldots 011)_2$. It means that the last three figures on both sides of (3) cannot be equal, equality (3) being thus impossible[1]).

Let us prove three lemmas.

---

* Presented to the Polish Mathematical Society, Section of Warsaw, 11. I. 1952.

[1]) For other demonstrations see *e. g.* W. Sierpiński, *Teoria liczb*, Warszawa-Wrocław 1950, p. 44, exercise 9.

LEMMA 1. *For every natural L and p*

$$(L,p+1)\prod_{k=1}^{p}(L-k)\equiv 0 \pmod{(p+1)!},$$

(a,b) denoting the greatest common divisor of corresponding numbers.

Proof. Let us suppose that

$$L=(L,p+1)u, \quad p+1=(L,p+1)s, \quad (u,s)=1.$$

It is obvious that the number

$$\frac{\prod_{k=0}^{p}(L-k)}{(p+1)!}=\frac{L}{p+1}\cdot\frac{\prod_{k=1}^{p}(L-k)}{p!}=\frac{u}{s}\binom{L-1}{p}$$

is an integer; considering $(u,s)=1$ we obtain $s\left|\binom{L-1}{p}\right.$ *i. e.*

$$(L,p+1)\binom{L-1}{p}\equiv 0 \pmod{(p+1)};$$

finally

$$(L,p+1)\prod_{k=1}^{p}(L-k)\equiv 0 \pmod{(p+1)!}.$$

If $(L,p+1)=1$, we get $\prod_{k=1}^{p}(L-k)\equiv 0 \pmod{(p+1)!}$.

LEMMA 2. *For natural numbers ϱ,s,p,n $(s\geqslant p\geqslant 2)$*

$$(\varrho n^s,p+1)=(\varrho n^{p-1},p+1). \tag{4}$$

Proof. For $p=2$ we have $(\varrho n^s,3)=(\varrho n,3)$, which is obvious.

For $p\geqslant 3$ supposing that $p+1=Ar^k$ $(r\geqslant 2,\ A\not\equiv 0 \pmod r)$ we may write

$$k=\ln(p+1)/\ln r-\ln A/\ln r\leqslant \ln(p+1)/\ln r\leqslant \ln(p+1)/\ln 2\leqslant p-1.$$

The last inequality proves the lemma.

Remark. For $n\equiv 1 \pmod 2$ equality (4) is valid already for $s\geqslant d\geqslant 1$; indeed in this case we have $(\varrho n^s,2)=(\varrho,2)$.

LEMMA 3. *For natural ϱ,s,p $(>1),n$*

$$\frac{\prod_{k=0}^{p}(\varrho n^s-k)}{n^{s-p+1}}=\varrho n^{p-1}\prod_{k=1}^{p}(\varrho n^s-k)\equiv 0 \pmod{(p+1)!}. \tag{5}$$

Proof. Congruence (5) is obvious for $s<p$; let us suppose that $s\geqslant p>1$. On applying the first and second lemmas we get

$$(\varrho n^s,p+1)\prod_{k=1}^{p}(\varrho n^s-k)=(\varrho n^{p-1},p+1)\prod_{k=1}^{p}(\varrho n^s-k)\equiv 0 \pmod{(p+1)};$$

hence $\varrho n^{p-1}\prod_{k=1}^{p}(\varrho n^s-k)\equiv 0 \pmod{(p+1)!}$, q. e. d.

Remark. The first and third lemmas give generalizations of the well known property $\prod_{k=1}^{p}(L-k)\equiv 0 \pmod{p!}$.

Let us proceed to the demonstration of the impossibility of the equality

$$n^{\alpha+s}+1=(n+1)^{\alpha}. \tag{6}$$

Let us first discuss the cases $n\equiv 0,1$ or $3 \pmod 4$. Applying the n-system of computation to (6) we see that the last three ciphers on the left side of (6) are 0, 0 and 1 $(n\geqslant 2,\ \alpha\geqslant 2,\ s\geqslant 1)$. Denoting by c_i the ciphers on the right side of (6) we get $c_1=1$; if $c_2=0$, we must have $\alpha\equiv 0 \pmod n$, *i. e.* $\alpha=\varrho n$; further, if $n\equiv 1$ or $3 \pmod 4$, we have

$$c_3=\frac{\alpha}{n}+\frac{\alpha(\alpha-1)}{2}=\varrho+\frac{\varrho n(\varrho n-1)}{2}\equiv \varrho \pmod n$$

because $\varrho(\varrho n-1)\equiv 0 \pmod 2$, if $n\equiv 0 \pmod 4$

$$c_3=\varrho-\tfrac{1}{2}\varrho n\equiv \varrho+\tfrac{1}{2}\varrho n\equiv \varrho(1+\tfrac{1}{2}n) \pmod n$$

and vice versa.

Generally we have

THEOREM. *A necessary and sufficient condition for the existence of p successive zeros in the development $(11)_n^{\alpha}$ is*

$$\alpha=\varrho n^p, \quad \varrho\not\equiv 0 \pmod n.$$

Proof. The condition is sufficient. Let us suppose that

$$\alpha=\varrho n^p, \quad \varrho\not\equiv 0 \pmod n, \quad p\geqslant 2$$

(the case $p=1$ was discussed above).

$$c_1=0,$$

$$c_2\equiv\binom{\alpha}{1}=\varrho n^p\equiv 0 \pmod n,$$

$$c_3=\binom{\alpha}{1}\frac{1}{n}+\binom{\alpha}{2}\equiv 0 \pmod n,$$

generally:

$$c_{t+1}\equiv\sum_{l=0}^{t-1}\frac{\prod_{k=0}^{l}(\varrho n^p-k)}{(l+1)!\,n^{t-l-1}} \pmod n, \quad 3\leqslant t\leqslant p.$$

According to the third lemma we have $c_{t+1}\equiv 0 \pmod n$ $(t=1,2,\ldots,p)$.

The condition is necessary. Let us suppose that

$$c_{t+1}\equiv \sum_{k=0}^{t-1}\binom{\alpha}{t-k}\frac{1}{n^k}\equiv 0 \pmod n, \qquad 1\leqslant t. \tag{7}$$

It immediately follows from (7) that

$$c_{t+1}\equiv \binom{\alpha}{1}\frac{1}{n^{t-1}}\equiv 0 \pmod n \quad i.\,e. \quad c_{p+1}\equiv \frac{\alpha}{n^{p-1}}\equiv 0 \pmod n \quad (t=1,2,\ldots,p)$$

or $\alpha=\varrho n^p$, q. e. d.

Now we are able to finish the demonstration of the impossibility of

$$(10)_n^{\alpha+s}+1=n^{\alpha+s}+1=(n+1)^\alpha=(11)_n^\alpha. \tag{8}$$

On the left side of (8) there are at least $\alpha+s-1\geqslant 2$ zeros; let us suppose that on the right side of (8) we have exactly p $(\geqslant 2)$ zeros, *i. e.* according to the theorem $\alpha=\varrho n^p$, $\varrho\not\equiv 0 \pmod n$ the number of zeros on the left side of (8) is $\alpha+s-1=\varrho n^p+s-1\geqslant \varrho n^p\geqslant n^p>p$, *i. e.* c_{p+2} equals zero on the left side of (8) and differs from zero on the right side of (14), equality (6) being thus excluded.

It can easily be proved in the same manner as above that if $n\equiv 2 \pmod 4$, the necessary (but not sufficient), condition for the existence of p successive zeros in the development $(n+1)^\alpha=(11)_n^\alpha$ is $\alpha=2\varrho(n/2)^p$.

Generalization. Instead of $|n^{\alpha+s}-(n+1)^\alpha|\neq 1$, $n\geqslant 2$, $\alpha\geqslant 2$, $s\geqslant 1$ I shall prove the inequality

$$|n^{\alpha+s}-(n+1)^\alpha|\geqslant \max(5,n+2), \qquad (n-2)^\alpha+(\alpha-2)^2+(s-1)^2\neq 0.$$

Proof.

$$|n^{\alpha+s}-(n+1)^\alpha|\neq 2 \quad \text{and} \quad \neq 4 \tag{9}$$

because $n^{\alpha+s}-(n+1)^\alpha\equiv 1 \pmod 2$. Considering $(n,n+1)=1$ we obtain the inequalities $|n^{\alpha+s}-(n+1)^\alpha|\neq n$ and $\neq n+1$.

We have to prove that $|n^{\alpha+s}-(n+1)^\alpha|\neq k$ $(1\neq k\leqslant n-1)$. In fact

$$|n^{\alpha+s}-(n+1)^\alpha|\equiv \pm 1 \,(\mathrm{mod}\,(n+1)), \tag{10}$$

since $1\neq k\leqslant n-1$; we must have $k\not\equiv \pm 1 \,(\mathrm{mod}\,(n+1))$. Taking into account (9), (10) we infer that

$$|n^{\alpha+s}-(n+1)^\alpha|\geqslant \max(5,n+2), \qquad \text{q. e. d.}$$

Sur l'équation $x^z-y^t=1$, où $|x-y|=1$

par A. Schinzel (Warszawa)

Dans la Note précédente R. Hampel a démontré le

Théorème. *L'équation*

$$x^z-y^t=1 \tag{1}$$

n'a pas, en nombres naturels x,y,z,t supérieurs à 1, d'autres solutions que $x=3$, $y=2$, $z=2$, $t=3$, si $|x-y|=1$.

Le but de la Note présente est de donner une démonstration plus courte de ce théorème.

Démonstration. Je démontrerai d'abord que l'équation (1) n'a pas de solutions en nombres naturels x,y,z,t supérieurs à 1, si

$$x-y=-1. \tag{2}$$

En effet, d'après (1) et (2) on a $(x+1)^t+1=x^z$. Le côté gauche, divisé par x, donne le reste 2 et le côté droit le reste 0 et, comme $x>1$, il en résulte que $x=2$, donc $y=3$ et d'après (1) on a $2^z-3^t=1$.

Or, B. A. Hausmann a démontré dans The American Mathematical Monthly 48 (1941), p. 482, que les nombres 2^m-1 où $m>1$ et 2^m+1 où $m>3$ ne sont pas des puissances de nombres naturels aux exposants naturels >1. Il en résulte que l'équation $2^z-3^t=1$ a en nombres naturels z et t une seule solution $z=2$, $t=1$[1]).

Il ne nous reste qu'a examiner le cas où

$$x-y=1. \tag{3}$$

Supposons que le système de nombres naturels x,y,z,t plus grands que 1 et différent que le système 3,2,2,3 est une solution de l'équation (1). S'il était ici $y=2$, on aurait $2^t+1=x^z$ et, vu que $z>1$, il résulterait du théorème mentionné de Hausmann que $t\leqslant 3$. Pour $t=3$ on aurait $9=x^z$, ce qui donne, d'après $z>1$, $x=3$, $z=2$, contrairement à l'hypothèse que le système x,y,z,t est distinct du système 3,2,2,3. Pour $t=2$ on aurait $5=x^2$, ce qui est impossible pour $z>1$. On a ainsi $y\neq 2$.

[1]) Voir aussi W. Sierpiński, *Teoria liczb*, Warszawa-Wrocław 1950, p. 44, exercice 9.