The length of the shortest period of rests of numbers n^n

by R. Hampel (Warszawa)

W. Sierpiński proves[1]) that the last figures of the numbers n^n form the periodical sequence whose shortest period consists of 20 terms, and that for every natural m the rests mod m of the numbers n^n $(n=1,2,3,\ldots)$ form an infinite periodical sequence.

My aim in this paper[2]) is to calculate the length of the shortest period mod m.

Let us suppose that

$$m=\prod_{i=1}^{k} p_i^{a_i}, \qquad a_i\geqslant 1, \qquad 2\leqslant p_i<p_{i+1} \qquad (i=1,2,\ldots,k-1).$$

I shall prove that

$$n^n\equiv r_n^{(m)} \pmod m$$

the rests $r_n^{(m)}$ forming the periodical sequence whose shortest period S_m satisfies the relation

$$S_m \mid \varphi(m)\prod_{i=1}^{k} p_i; \tag{1}$$

exactly

$$S_m=\{p_i\varphi(p_i^{a_i})\} \quad \text{i. e.} \quad S_m=\{m;p_i-1\} \qquad (i=1,2,\ldots,k), \tag{2}$$

$\varphi(m)$ denotes the well known function of Gauss and $\{\ \}$ — the least common multiple of corresponding numbers.

It is obvious that to prove the relation (1) we have to show for $n\geqslant n_0$ (n_0 denotes the well determined natural number given below) the validity of the congruence

$$[n+\varphi(m)\prod_{i=1}^{k} p_i]^{n+\varphi(m)\prod_{i=1}^{k} p_i}\equiv n^n \pmod m. \tag{3}$$

[1]) W. Sierpiński, *Sur la périodicité* mod m *de certaines suites infinies d'entiers*, Annales de la Soc. Pol. Math. 23 (1950), p. 256.

[2]) Communication presented to the Polish Mathematical Society, Section of Warsaw, March 13, 1953.

Considering

$$m\mid\varphi(m)\prod_{i=1}^{k} p_i=m\prod_{i=1}^{k}(p_i-1)$$

we get from (3)

$$n^n[n^{\varphi(m)\prod_{i=1}^{k} p_i}-1]\equiv 0 \pmod m. \tag{4}$$

1° $(n,m)=1$. On applying the theorem of Euler we immediately see that the congruence (3) is valid.

2° $(n,m)\neq 1$. Suppose that

$$(n,m)=\prod_{i=1}^{r} p_{l_i}^{\beta_{l_i}}, \qquad r\leqslant k, \quad 1\leqslant\beta_{l_i}\leqslant a_{l_i}, \quad 1\leqslant l_1<l_2<\ldots<l_r\leqslant k.$$

We begin the calculation of the period from the least natural number $n=n_0$ which satisfies the inequalities $n\beta_{l_i}\geqslant a_{l_i}$, $t=1,2,\ldots,r$ *i. e.* from such n_0 that

$$n_0\geqslant\max\frac{a_{l_t}}{\beta_{l_t}} \qquad \text{and} \qquad n_0-1<\max\frac{a_{l_t}}{\beta_{l_t}} \qquad (t=1,2,\ldots,r).$$

Applying the symbol E (entier) we get

$$n_0=-\mathrm{E}\left(-\max\frac{a_{l_t}}{\beta_{l_t}}\right).$$

We shall prove the validity of the congruence (4) for every $n\geqslant n_0$. Applying the multiplicativeness of the function $\varphi(m)$ and considering that the two obtained factors are mutually prime we may write this congruence in the form

$$n^n(n^\nu-1)\equiv 0 \pmod m \tag{5}$$

where

$$\nu=\varphi\Big(m/\prod_{t=1}^{r} p_{l_t}^{a_{l_t}}\Big)\varphi\Big(\prod_{t=1}^{r} p_{l_t}^{a_{l_t}}\Big)\prod_{t=1}^{k} p_t;$$

but $n^n\equiv 0 \pmod{\prod_{t=1}^{r} p_{l_t}^{a_{l_t}}}$ because for $n\geqslant n_0$

$$n\beta_{l_t}\geqslant a_{l_t} \qquad (t=1,2,\ldots,r).$$

Applying the theorem of Euler to the expression in brackets in (5) and taking into account that

$$\left(\frac{m}{\prod_{t=1}^{r} p_{l_t}^{a_{l_t}}};n\right)=1$$

we prove immediately the theorem.

It is sufficient to take $n=n_0=\max \alpha_i$, $i=1,2,\ldots,k$.

Before proving that the shortest period $S_m=\{m;p_i-1\}$ I shall discuss some special cases.

Let us take $m=p^\alpha$. According to the relation (1) we have

$$S_m \leqslant p^\alpha(p-1). \tag{6}$$

I shall prove that

$$S_m=p\varphi(p^\alpha)=p^\alpha(p-1).$$

We distinguish two cases:

1° $\alpha=1$, *i. e.* $m=p$, $S_p=p(p-1)$.

I report the proof of W. Sierpiński given in his letter of 6.5.1953.

It was proved above that $S_p|p(p-1)$. Therefore it is sufficient to show that the period $S<p(p-1)$ does not exist. But for the prime mod p we have $n^n\equiv 0 \pmod p$, if and only if $n\equiv 0 \pmod p$, which involves $p|S$, *i. e.* $S=pk$ (k — natural number).

Let us suppose now that $S<p(p-1)$, it means that $k<p-1$, *i. e.* since S is a period, we may write

$$(n+S)^{n+s}\equiv n^n \pmod p$$

for natural n; hence, regarding $S=pk$, it follows that

$$n^n n^{pk}\equiv n^n \pmod p;$$

the last congruence for $(n,p)=1$ gives immediately $n^{pk}\equiv 1 \pmod p$. But according to the theorem of Fermat we have

$n^{p-1}\equiv 1 \pmod p$ for $(n,p)=1$, hence $n^{(p-1)k}\equiv 1 \pmod p$ for $(n,p)=1$.

Since $n^{pk}=n^{(p-1)k}n^k$, we obtain

$$n^k\equiv 1 \pmod p \quad \text{for} \quad (n,p)=1.$$

Particularly let us assume $n=g$, where g denotes the primitive root of the prime number p; then we have

$$g^k\equiv 1 \pmod p \quad \text{where} \quad k<p-1,$$

contrary to the property of the primitive root. Therefore $S\geqslant p(p-1)$.

2° $\alpha\geqslant 2$. I shall prove the impossibility of the conjecture

$$S_m=p^{\alpha-1}(p-1) \quad \text{for} \quad (n,p)=1. \tag{7}$$

Let us suppose the contrary. Admitting (7), we have

$$[n+p^{\alpha-1}(p-1)]^{n+p^{\alpha-1}(p-1)}\equiv n^n \pmod{p^\alpha} \tag{8}$$

i. e.

$$n^n[(n^{p^{\alpha-1}(p-1)}-1)-n^{p^{\alpha-1}(p-1)}p^{\alpha-1}]\equiv 0 \pmod{p^\alpha}. \tag{9}$$

Using

$$n^{p^{\alpha-1}(p-1)}-1=n^{\varphi(p^\alpha)}-1\equiv 0 \pmod{p^\alpha},$$

we get

$$n^{p^{\alpha-1}(p-1)}p^{\alpha-1}\equiv 0 \pmod{p^\alpha} \qquad ((n,p)=1),$$

which is impossible. It means that

$$p^\alpha | S_m \quad \text{where} \quad S_m | p^\alpha(p-1).$$

We have therefore $S_m=p^\alpha k$.

I shall prove that $k=p-1$. Let us suppose $k<p-1$, then we have

$$(n+S_m)^{n+S_m}\equiv n^n \pmod{p^\alpha}$$

or

$$n^{n+p^\alpha k}\equiv n^n \pmod{p^\alpha}; \tag{10}$$

it follows from (10) that

$$n^{p^\alpha k}=n^{p^{\alpha-1}(p-1)k}n^{p^{\alpha-1}k}\equiv 1 \pmod{p^\alpha} \qquad ((n,p)=1).$$

Let us take $n=g$ where g denotes the primitive root of the number p^α. We have

$$n^{\varphi(m)}=n^{p^{\alpha-1}(p-1)}\equiv 1 \pmod{p^\alpha},$$

i. e.

$$n^{p^{\alpha-1}k}\equiv 1 \pmod{p_a} \qquad (k<p-1),$$

contrary to the definition of the primitive root of a number. It means that $k\geqslant p-1$ and

$$S_m\geqslant p^\alpha(p-1); \tag{11}$$

from (6) and (11) we get immediately

$$S_m=p^\alpha(p-1) \qquad \text{q. e. d.}$$

Taking now $m=2p^\alpha$, $p\neq 2$ we have, as before,

$$S_m=p^\alpha(p-1) \qquad (S_{2p^\alpha}=S_{p^\alpha},\ p\neq 2). \tag{12}$$

Indeed, according to the theorem just proved we have

$$n^n(n^{p^\alpha(p-1)}-1)\equiv 0 \pmod{p^\alpha} \qquad ((n,p)=1).$$

If $n\equiv 0 \pmod 2$, *the relation* (12) *is obvious.*

If $n\equiv 1 \pmod 2$, $n^{p^\alpha(p-1)}-1\equiv 0 \pmod 2$ *and* $\pmod{p^\alpha}$ *if* $(n,p)\neq 1$ *i. e.* $p|n$ *the relation* (12) *is valid* (see later) *at any rate for* $n\geqslant\alpha$.

Thus we have, beginning from some n,

$$n^{n+p^\alpha(p-1)}\equiv n^n \pmod{2p^\alpha} \qquad \text{q. e. d.}$$

For instance

$$m=2^a, \qquad S_m=2^a=m,$$

$$m=10, \qquad S_m=5\cdot(5-1)=20.$$

Now I shall discuss when the period is proper and when it is mixed in the cases $m=p^a$ and $m=2p^a$, $p\neq 2$.

Let us take first

$$m=p^a. \tag{13}$$

When $p\geqslant a$, the period is proper. Indeed, for $(n,m)=1$ the period begins from $n=1$.

Let us suppose $(n,m)\neq 1$ *i. e.* $(n,m)=p^\beta$; $1\leqslant\beta\leqslant a\leqslant p$; *i. e.* $n=p^\beta\cdot t$. We have

$$(n+S_m)^{n+S_m}\equiv n^n=(p^\beta t)^{p^\beta t}\equiv 0 \pmod{p^a},$$

for every natural t and β.

If $p<a$, the period is necessarily mixed because

$$(p+S_m)^{p+S_m}\equiv p^{p+S_m}\not\equiv p^p \pmod{p^a},$$

it is sufficient but not necessary to begin the period from $n=a$.

We shall find the necessary and sufficient condition as follows. It is evident that we have to discuss only the case $(n,p)\neq 1$ *i. e.* $n=p^\beta$, $1\leqslant\beta\leqslant a$. We seek the least natural number k such that

$$(kp)^{kp}\equiv 0 \pmod{p^a}$$

i. e.

$$kp\geqslant a; \qquad (k-1)p<a, \qquad -\frac{a}{p}-1<-k\leqslant-\frac{a}{p}, \qquad k=-\mathrm{E}\left(-\frac{a}{p}\right).$$

Denoting by $n_0=n_{ap}$ the natural number from which the period begins we get immediately

$$n_0=n_{ap}=(k-1)p+1=1-p\left[1+\mathrm{E}\left(-\frac{a}{p}\right)\right]. \tag{14}$$

Particularly if $a\leqslant p$, we obtain from (14) the result given above. I omit the case $m=2p^a$ which leads to quite the same result *e. g.*

$p=7$, $a=15$, $n_0=a=15$; $p=7$, $a=14$, $n_0=8$; $p=2$, $a=3$, $n_0=3$ etc.

Before proceeding to the general case I shall give two quite evident relations:

1° If $m_1\mid m$, then $S_{m_1}\leqslant S_m$. Indeed, denoting $u_k=k^k$, if $u_{k+S_m}\equiv u_k \pmod m$, then, all the more, $u_{k+S_m}\equiv u_k \pmod{m_1}$.

2° If S_1 and S_2 are two different periods of the rests of numbers mod m then $(S_1,S_2)=$(g. c. d. of the numbers S_1 and S_2) forms also the period mod m. Let us take $n\geqslant n_0$. According to our supposition

$$u_{n+S_1}\equiv u_n \pmod m, \qquad u_{n+S_2}\equiv u_n \pmod m$$

and

$$u_{n+kS_1+tS_2}\equiv u_n \pmod m \quad (k,t \text{ integers } n+kS_1+tS_2\geqslant n_0);$$

but the equation (indefinite) $kS_1+tS_2=(S_1,S_2)$ has an infinity of solutions (k,t), so that we may write

$$[n+(S_1,S_2)]^{n+(S_1,S_2)}\equiv n^n \pmod m$$

for every sufficiently great n.

Remark 1. Considering $S_m\geqslant 2$ $(m\geqslant 2)$, the relation $(S_1,S_2)=1$ is impossible; *i. e.* there do not exist two relatively prime periods.

Remark 2. It is obvious that the last two assertions may be applied to the rests of terms of every periodical sequence mod m.

Let us proceed to the general case $m=\prod_{l=1}^{k} p_l^{a_l}$.

THEOREM. *Denoting as before by the symbol $\{a_i\}$ the l. c. m. of the numbers $a_1,a_2,\ldots,a_k$ we have*

$$S_m=\{p_i\varphi(p_i^{a_i})\}=\{m;p_i-1\} \qquad (i=1,2,\ldots,k). \tag{15}$$

Proof.

$$[n+\{m;p_i-1\}]^{n+\{m;p_i-1\}}\equiv n^n \pmod{p_i^{a_i}}, \quad i=1,2,\ldots,k, \quad \text{for} \quad n\geqslant n_{a_ip_i}$$

and since all the natural numbers $p_1^{a_1},p_2^{a_2},\ldots,p_k^{a_k}$ are relatively prime, we conclude that

$$[n+\{m;p_i-1\}]^{n+\{m;p_i-1\}}\equiv n^n \pmod m, \quad \text{for} \quad n\geqslant \max(n_{a_ip_i}) \tag{16}$$

it means that

$$S_m\leqslant\{p_i\varphi(p_i^{a_i})\}. \tag{17}$$

Let us suppose that

$$S_m<\{p_i\varphi(p_i^{a_i})\},$$

then we have $p_i\varphi(p_i^{a_i})\nmid S_m$ at least for some $i=i_0$, and, according to the second assertion mentioned above, the number

$$L=(S_m;p_{i_0}^{a_{i_0}}(p_{i_0}-1))<p_{i_0}^{a_{i_0}}(p_{i_0}-1)=S_{p_{i_0}^{a_{i_0}}}$$

would be a period mod $p_{i_0}^{a_{i_0}}$ which is impossible. Therefore

$$S_m=\{p_i\varphi(p_i^{a_i})\}, \tag{18}$$

q. e. d.

It follows immediately from (18) $m\mid S_m$.

It is interesting to answer the question when $m=S_m$. The necessary condition is $m\equiv 0 \pmod 2$, *e. g.*

$$m=2^\alpha, \quad m=2^\alpha\cdot 3^\beta, \quad m=2^\alpha 5^\beta \ (\alpha\geqslant 2), \quad m=2^\alpha 3^\beta 7^\gamma \ \text{ etc.}$$

for all these cases $S_m=m$.

It means that the number

$$\varphi(m)\prod_{l=1}^{k} p_l$$

given on the first page as the period, may be divided by

$$2^{a_1+\sum_{l=1}^{k}\gamma_l-\max(\gamma_i;a_i)} \quad \text{when} \quad p_1=2$$

and by

$$2^{\sum_{l=1}^{k}\gamma_l-\max\gamma_i} \quad \text{when} \quad p_1\geqslant 3 \qquad (i=1,2,\ldots,k),$$

where

$$p_i-1=2^{\gamma_i}c_i, \qquad c_i\not\equiv 0 \pmod 2 \qquad (i=1,2,\ldots,k),$$

and possibly by other (necessarily odd) divisors of the numbers c_i.

The period is proper if $p_i\geqslant a_i$, $i=1,2,\ldots,k$, and mixed if this is not the case. If we denote

$$n_{a_i,p_i}=1-p_i\left[1+\mathrm{E}\left(-\frac{a_i}{p_i}\right)\right],$$

the period begins in both cases from $n=\max(n_{a_ip_i})$, $i=1,2,\ldots,k$.

Problème du mouvement stationnaire dans une couche gazeuse rayonnante

par W. Pogorzelski (Warszawa)

Introduction. L'étude de l'équilibre ou du mouvement dans un grand milieu gazeux, comme l'atmosphère d'une planète ou d'une étoile, doit tenir compte du rayonnement intérieur en négligeant l'influence de la conductibilité.

K. Schwarzschild [4] le premier et ensuite R. Emden [2] ont étudié l'équilibre d'une couche gazeuse en tenant compte du rayonnement mais sous la supposition inexacte des courants d'énergie dans deux directions seulement.

C. Białobrzeski [1] a étudié le premier l'équilibre d'une sphère gazeuse en tenant compte de la pression de radiation.

W. Pogorzelski [3] a étudié l'équilibre d'une couche gazeuse en tenant compte du rayonnement polychromatique dans toutes les directions. Le problème conduit à un système d'équations intégrales non linéaires, assez compliquées; l'auteur a démontré l'existence de la solution si l'épaisseur de la couche est suffisamment petite.

Dans ce travail nous démontrerons l'existence d'un état stationnaire du mouvement dans une couche gazeuse en tenant compte du rayonnement polychromatique dans toutes les directions. Le problème consiste en l'étude d'un système d'équations intégrales non linéaires.

Les grandeurs et les équations fondamentales. Soit au point intérieur M d'un milieu gazeux un élément de surface $d\sigma$ avec la normale Mn. On admet que la quantité d'énergie, qui passe par l'élément $d\sigma$ dans le temps dt grâce au rayonnement de longueur d'onde dans l'intervalle $(\lambda,\lambda+d\lambda)$ dans la direction MR d'un angle solide $d\omega$, a pour valeur principale le produit

$$X\cos\Theta\, d\sigma\, d\lambda\, dt\, d\omega, \tag{1}$$

Θ étant l'angle que fait la direction MR avec la normale Mn. La grandeur X s'appelle l'intensité de rayonnement de longueur d'onde λ, au point M et dans la direction MR.