# On one way of making automorphic numbers

By PÉTER KISS (Eger)

*To the memory of Professor Andor Kertész**

**1.** A natural number $a$ is called an *automorphic number* in the scale $n$ with index $k$ if

$$a^2 \equiv a \pmod{n^k}.$$

Essentially this means that in the scale $n$ the last $k$ digits of $a^2$ and of $a$ are equal.

This terminology was used first by R. L. GOODSTEIN [1] who dealt with automorphic numbers under the influence of the letter by C. D. LANGFORD. Goodstein proved that if $n=u\cdot v$ where $(u, v)=1$ and $u^q\equiv 1 \pmod{v}$ then the remainder of $u^{q\cdot v^{k-1}}$ divided by $n^k$ is an automorphic number in the scale $n$ with index $k$. Following from this, the remainder of $R^{v^{k-1}}$ divided by $n^k$ is an automorphic number in the scale $n$ with index $k$, provided that $u^q\equiv R \pmod{n}$ for the previous $q$.

Similar problems have been considered already by several authors. R. TÉDENAT [2] (see also [9], p. 454) discussed in 1814 the method of making automorphic numbers in the scale 10. Similar results are obtained by A. PALMSTRÖM [3] (see also [9], p. 459). The general case is dealt with by G. ANDREOLI [4] (see also [9], p. 464) who proved very circumstantially that the equality $x^2-x=A\cdot n^k$ can have no more different solutions than the number of the possibilities of writing $n$ as a product of two relatively prime factors.

C. HUBERT [5] obviously did not know the preceding results because in 1949 he raised the question of the case $n=10$. On the base of [5] the problem has been considered by D. POMPEIU [6], G. VRĂNCEANU [7] and P. POPOVICI [8]. They discussed the case $n=10$ too, repeating the results of Tédenat in [2] and giving also a new method of making automorphic numbers in the scale 10.

We join the present article to the results of R. L. GOODSTEIN [1] and P. POPOVICI [8]. In the following we get a more simple way of producing automorphic numbers from the point of view of numerical calculation. This method is also good for the determination of the numbers of different automorphic numbers. Furthermore we shall exhibit the relation between the pseudoprime and automorphic numbers.

* Dedicated 14 May 1974.

**2.** It is evident that if one of the natural numbers is automorphic in a scale $n$ with index $k$ then it is automorphic with index 1 too. Therefore first let us deal with the case $k=1$. It is enough to look for solutions of the congruence

$$a^2 \equiv a (\bmod n) \tag{1}$$

in form $0 \leqq a < n$, since if $a$ is a solution of (1) then $a+d \cdot n$ is also one as is easy to see ($d$ is an arbitrary natural number). $a=0$ and $a=1$ are trivial solutions of (1) for any $n$, therefore in the sequel we do not deal with these cases. If $n$ is a power of a prime: $n=p^\alpha$ then from (1)

$$a(a-1) \equiv 0 (\bmod p^\alpha).$$

But $(a, a-1)=1$, therefore $n|a$ or $n|a-1$, however this is contradicts the conditions $0<a<n$. For this reason if $n$ is a power of a prime (1) has only two trivial solutions.

If $n$ is a composite number: $n=p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ with $r \geqq 2$, then we can write $n$ as a product:

$$n = q_1 \cdot q_2 \quad \text{where} \quad (q_1, q_2) = 1.$$

We will prove the following theorem: For all such factorisations there is one and only one number $a$ which is automorphic in the scale $n$ with index 1.

According to the conditions $n|a(a-1)$ and $(a, a-1)=1$ if $a$ satisfies (1) then there exist $q_1'$ and $q_2'$ with $n=q_1' \cdot q_2'$, $(q_1', q_2')=1$, $q_1'|a$ and $q_2'|a-1$. That means that all values of $a$ are coupled to one of the factorisations $n=q_1 \cdot q_2$. We will prove also the inverse of this; there is an $a$ for all factorisations $n=q_1 \cdot q_2$ which satisfies (1) and

$$q_1|a, \quad q_2|a-1. \tag{2}$$

The numbers $1, 2, 3, \ldots, q_2$ form a total remainder system (mod $q_2$) and as $(q_1, q_2)=1$, the numbers $q_1, 2q_1, 3q_1, \ldots, q_2 q_1$ form also a total remainder system (mod $q_2$). So the later system contains exactly one element $t \cdot q_1$ for which

$$t \cdot q_1 \equiv 1 (\bmod q_2). \tag{3}$$

The number $a=t \cdot q_1$ is a solution of the congruence (1) because it satisfies the conditions (2) and since $t<q_2$, $a=t \cdot q_1<q_1 \cdot q_2=n$. Following from (3) $(t, q_2)=1$, hence among the prime factors of $a$ there are all the prime factors of $q_1$ which are also factors of $n$. So each factorisation $(n=q_1 \cdot q_2)$ determines exactly one $a$ ($q_1 \cdot q_2$ and $q_2 \cdot q_1$ are different factorisations). Hence (1) has the same number of solutions as the number of decomposition of $n$ as product of two relatively prime numbers. But $q_1$ may contain $1, 2, \ldots, r-1$ different prime factors of $n$ (where $r$ is the number of different prime factors of $n$). Thus the number of solutions is

$$\binom{r}{1}+\binom{r}{2}+\ldots+\binom{r}{r-1} = \sum_{i=0}^{r}\binom{r}{i}-\binom{r}{0}-\binom{r}{r} = 2^r-2.$$

So the number of solutions of (1) is $2^r-2$, or $2^r$ with the two trivial solutions. This result contains the case $n=p^\alpha$, too.

**3.** After this we will prove the following **theorem**.

*All different numbers which are automorphic numbers in the scale $n$ with index* 1 *determine exactly one number which is less than $n^k$ and is an automorphic number in the scale $n$ with index $k$.*

It is enough to examine the case $a<n^k$ because if

$$a^2 \equiv a \pmod{n^k}$$

then

$$(a+d\cdot n^k)^2 = a^2+c\cdot n^k \equiv a \equiv a+d\cdot n^k \pmod{n^k},$$

where $d$ and $c$ are natural numbers. Thus if $a$ is an automorphic number in the scale $n$ with index $k$ then $a+d\cdot n^k$ too is one.

We saw, that there are $2^r$ automorphic numbers in the case $k=1$, hence it is enough to prove that all different automorphic numbers with index $i$ determine exactly one automorphic number with index $i+1$. If $a$ is an automorphic number with index $i$ and $b$ is one with index $i+1$, then

$$a^2 \equiv a \pmod{n^i} \tag{4}$$

and

$$b^2 \equiv b \pmod{n^{i+1}}. \tag{5}$$

But $b$ satisfies (4) too, hence $b=c\cdot n^i+a$ where $c<n$ from the condition $b<n^{i+1}$. If $a$ has the following form in the scale $n$:

$$a = a_{i-1}\cdot n^{i-1}+a_{i-2}\cdot n^{i-2}+\ldots+a_1\cdot n+a_0 \tag{6}$$

and according to (4)

$$a^2 = A\cdot n^{i+1}+b_i\cdot n^i+a,$$

then

$$a^2 \equiv b_i\cdot n^i+a \pmod{n^{i+1}}.$$

Now put $b=c\cdot n^i+a$ in congruence (5) and use the fact that $i>1$ implies $2i>i+1$

$$(c\cdot n^i+a)^2 = c^2\cdot n^{2i}+2a\cdot c\cdot n^i+a^2 \equiv 2a\cdot c\cdot n^i+b_i\cdot n^i+a \equiv c\cdot n^i+a \pmod{n^{i+1}}.$$

Dividing by $n^i$

$$2a\cdot c+b_i \equiv c \pmod{n}.$$

From (6)

$$a \equiv a_0 \pmod{n},$$

hence

$$2a_0\cdot c+b_i \equiv c \pmod{n}$$

and consequently

$$(2a_0-1)\cdot c+b_i \equiv 0 \pmod{n}. \tag{7}$$

We will prove that the congruence has one and only one solution. The number $a$ satisfies the congruence (4) and so $a_0$ satisfies congruence (1) hence with the help of (3)

$$a_0 = t\cdot q_1 \quad \text{and} \quad a_0-1 = m\cdot q_2,$$

where $m$ is a natural number, $q_1\cdot q_2=n$ and $(q_1, q_2)=(t, q_2)=(m, q_1)=1$. That is why

$$(n, 2a_0-1) = 1.$$

Thus the solution of (7) is exactly one remainder class (mod $n$) and by the condition $c<n$ we can find exactly one value of $c$. Thus we get different solutions of (5) from different solutions of (4) and conversely. So the numbers of solutions of (4) and of (5) are equal. But (1) has $2^r$ solutions hence the number of the automorphic numbers in a system $n$ with index $k$ is $2^r$ (with the two trivial solutions and the condition $a<n^k$).

Omitting the condition $a<n^k$ we get infinitely many automorphic numbers hence all $a$ automorphic numbers determine infinitely many $a+d\cdot n^k$ numbers (where $d$ is any natural number) which are also automorphic numbers.

**4.** With the help of the above results we can obtain the automorphic numbers in a recursive way. Let us see for example the case $n=10$. $n=10=2\cdot 5$ and so $r=2$. We shall look for the solutions (except the two trivial solutions) the number of which is for any index $2^r-2=2$. In the case $k=1$, $q_1=2$ and $q_2=5$ we must solve for (3) the congruence

$$2t \equiv 1 \pmod 5.$$

From this we get the value $t=3$ and so $a=t\cdot q_1=6$. If $q_1=5$ and $q_2=2$ then from

$$5t \equiv 1 \pmod 2$$

$t=1$ and so $a=1\cdot 5=5$.

In the case $k=2$ we first use the value $a=6=a_0$ which is a solution of the case $k=1$. Here $a^2=36$ so $b_1=3$. Substituting in (7)

$$11c+3 \equiv 0 \pmod{10}$$

from this $c=7$ and so $b=7\cdot 10+6=76$. We get similarly, starting from $a=5$, the result $b=25$.

If $k=3$ and $a=76$ (from this $a_0=6$) then because of $76^2=5776$, $b_2=7$ and so on the basis of (7)

$$11c+7 \equiv 0 \pmod{10}.$$

From this $c=3$, thus $b=3\cdot 10^2+76=376$ is an automorphic number in the scale 10 with index 3. If we start from $a=25$ then we get the number 625.

We can continue the procedure until an arbitrary value of $k$. For any $k$ we get 0 and 1 as the two trivial solutions evidently satisfying the conditions.

**5.** The following remark shortens the calculations.

If the number $a$ is an automorphic number in the scale $n$ with index $k$ then $n^k+1-a$ is also one. Hence

$$a^2 \equiv a (\mathrm{mod}\, n^k) \quad \text{and} \quad n^{2k} \equiv n^k \equiv 0 \pmod{n^k}$$

and so

$$(n^k+1-a)^2 \equiv 1+a^2-2a \equiv 1-a \equiv n^k+1-a \pmod{n^k},$$

and that proves our statement.

We saw previously that in case $k=1$ the solution is of the form $a=t\cdot q_1$, where $n=q_1\cdot q_2$ and $(q_1, q_2)=1$. This implies that there are no common factors among the prime factors of $n+1-a=q_1\cdot(q_2-t)+1$ and $q_1$. But because of (3) $a-1=m\cdot q_2$ (where $m$ is a natural number), hence $n+1-a=q_1\cdot q_2-m\cdot q_2=M\cdot q_2$ (where $M$ is a natural number). Thus if the solution $a$ belongs to $q_1$ in the factorisation $n=q_1\cdot q_2$ then $n+1-a$ belongs to $q_2$.

Thus it is enough to deal with one of the factorisations $n=q_1 \cdot q_2$ and $n=q_2 \cdot q_1$ since we get the solution for the other factorisation by $n^k+1-a$. For example we saw that the number 376 is automorphic in the scale 10 with index 3. But then the number $10^3+1-376=625$ is automorphic, too.

**6.** It is worth to mention the relation between the automorphic and the pseudoprime numbers.

A composite number $n$ is called a pseudoprime with respect to $a$ if

$$a^n \equiv a \pmod{n}.$$

It is easy to see that if a natural number $a$ is automorphic in the scale $n$ with index 1 then $n$ is a pseudoprime number with respect to $a$. Namely if

$$a^2 \equiv a \pmod{n}$$

then in the case $n>2$

$$a^n = a^2 \cdot a^{n-2} \equiv a \cdot a^{n-2} = a^{n-1} \equiv \ldots \equiv a^2 \equiv a \pmod{n}.$$

We already saw that for all composite numbers $n$ there are $2^r-2$ (where $r$ is the number of different prime factors of $n$) automorphic numbers $a$ in the scale $n$ $(a<n)$, therefore for all composite numbers $a$ there are at least $2^r-2$ numbers $a$ so that $n$ is a pseudoprime with respect to $n$ and $1<a<n$. Of course these are principal values because if the number $n$ is a pseudoprime with respect to $a$ then with respect to $a+d \cdot n$ it is pseudoprime, too, where $d$ may be any natural number.

## Bibliography

[1] R. L. Goodstein, Automorphic numbers in a general scale, *Math. Gaz.*, **43** (1959), 270—272.

[2] M. Tédenat, Solutions du probléme d'arithmétique, *Ann. de Math.*, **5** (1814—5), 309—321.

[3] A. Palmström, Einige zahlentheoretische Probleme, *Skrifter udgivne af videnskabs… , Kristiania*, 1900, No 3, 3—16.

[4] G. Andreoli, Sopra alcuni speciali numeri sui sistemi di numeracione in cui essi sono possibili, *Giornale di Math.*, **52** (1914), 53—57.

[5] Constant Hubert, Le curieux nombre 9376, *La Nature*, sept., 1949, 282.

[6] D. Pompeiu, O ecuatie aritmetica, *Bul. stii., sect. de stii. mat. si fiz.*, tom IV. (1952), 1—5.

[7] G. Vrănceanu, Asupra unei ecuatii aritmetica, *Com. Acad. Rep. Pop. Romane*, tom. III (1953), 5—8.

[8] C. P. Popovici, Sur une équation arithmétique de D. Pompeiu, *Bull. Math. de la Soc. Sci. Math. de la R.S.R.*, tom. **9** (57) (1967), 91—97.

[9] L. E. Dickson, History of the theory of numbers, Vol. I, *New York*, 1952.

*(Received September 12, 1973.)*