REPRERESENTATIONS OF AUTOMORPHIC NUMBERS

NICHOLAS P. CALLAS
Office of Scientific Research, U.S.A.F., McLean, Virginia

An n-place automorphic number $x > 1$ is a natural number with n digits such that the last n digits of x^2 are equal to x (see, for example [1]). In number-theoretic notation, this definition can be expressed quite compactly as $x - x^2 \equiv 0 \pmod{10^n}$. An example of a 3-place automorphic number is 625. A recent report [2] indicates that automorphic numbers with 100,000 digits have been computed.

It is a simple matter to prove that automorphic numbers with any number of digits exist. Further, if x is an automorph of n digits, then it follows that $y = 10^n + 1 - x$ is also. In other words, n-place automorphic numbers occur in pairs. (This statement is not quite accurate. For example, the "two" 4-place automorphs are 9376 and 0625. If we accept the convention that a leading zero is distinctive, then 0625 may be considered a 4-place automorph different from the 3-place automorph 625).

The purpose of this paper is to present the following representations for automorphic numbers:

Theorem. If x is an n-place automorphic number, then $y \pmod{10^{tn}}$, defined by

$$(1) \qquad y = x^t \sum_{k=0}^{t-1} (-1)^k \binom{t+k-1}{k} \binom{2t-1}{t+k} x^k$$

is a tn-place automorphic number, $t = 1, 2, 3, \cdots$. Moreover,

$$(2) \qquad y = \frac{t}{2} \binom{2t}{t} \int_0^x (u - u^2)^{t-1} du \ .$$

Remarks. a. In the case $t = 1$, the theorem gives the trivial identity $y = x$.

b. These representations, for the case $t = 2$, are presented in [3, page 257] and in [2].

c. Apparently (due to multiple-precision requirements on digital computers) these representation formulas do not give any special advantage to their user in computing automorphic numbers with large numbers of digits. Even other alternatives for doing the necessary arithmetic with large integers, e.g., modular arithmetic, seem also to present major problems in appying these formulas.

d. The following definition and binomial coefficient identities are used in the proof of the theorem.

$$\binom{r}{k} \equiv \begin{cases} \dfrac{r(r-1)\cdots(r-k+1)}{k(k-1)\cdots(1)}, & \text{integer } k \geq 0, \\ 0, \quad \text{integer } k < 0; \end{cases}$$

(3) $$\binom{r}{k} = \frac{r}{k}\binom{r-1}{k-1}, \quad \text{integer } k \neq 0 ;$$

(4) $$\binom{r+s}{n} = \sum_{k=0}^{n} \binom{r}{k}\binom{s}{n-k}, \quad \text{integer } n ;$$

(5) $$\binom{r}{m}\binom{m}{k} = \binom{r}{k}\binom{r-k}{m-k}, \quad \text{integers } m, k ;$$

(6) $$\sum_{k=0}^{n} (-1)^k \binom{r}{k} = (-1)^n \binom{r-1}{n}, \quad \text{integer } n \geq 0 .$$

Proof of Theorem. First, by divisibility properties of primes, a necessary and sufficient condition that $x > 1$ is an n-place automorphic number is that either

(7) $$\begin{gathered} x \equiv 0 \pmod{2^n} \quad \text{and} \quad x \equiv 1 \pmod{5^n} \\ \text{or} \\ x \equiv 1 \pmod{2^n} \quad \text{and} \quad x \equiv 0 \pmod{5^n} . \end{gathered}$$

Hence $x = qp^n + r$, where $p = 2$ or 5 and $r = 0$ or 1. By the binomial expansion formula,

$$x^k = \sum_{m=0}^{k} \binom{k}{m} (qp^n)^{k-m} r^m, \quad \text{where } k = 1, 2, \cdots .$$

Suppose now that it is possible to find integers a_k, independent of x, such that

(8) $$y = \sum_{k=0}^{s} a_k x^k$$

is an tn-place automorph for any n-place automorph x. Then

(9) $$y \equiv r \pmod{p^{tn}}, \quad p = 2 \text{ or } 5, \quad r = 0 \text{ or } 1 .$$

By replacing x^k with its binomial expansion and interchanging orders of summation,

$$y \equiv \sum_{j=0}^{t-1} A_j (qp^n)^j \equiv r \pmod{p^{tn}} ,$$

where

$$A_j \equiv \sum_{k=j}^{s} \binom{k}{j} a_k r^{k-j} .$$

Due to our assumption that y is automorphic for any automorph x, it follows that

$$A_j = \delta_0^j r, \qquad j = 0, 1, 2, \cdots, t-1 .$$

Hence, for $r = 0$, it follows that

$$a_k = 0, \qquad k = 0, 1, 2, \cdots, t-1 \tag{10}$$

Further, for $r = 1$, the remaining $s - t + 1$ coefficients are related in t linear equations. If we choose $s = 2t - 1$, then the necessary conditions on the remaining t coefficients in the representation y are the t linear equations

$$\sum_{k=t}^{2t-1} \binom{k}{j} a_k = \delta_0^j, \qquad j = 0, 1, 2, \cdots, t-1 . \tag{11}$$

We now verify that this system has a solution, indeed

$$a_k = (-1)^{k-t} \binom{k-1}{t-1} \binom{2t-1}{k}, \qquad k = t, \cdots, 2t-1 \tag{12}$$

defines a set of solutions of the linear system (11). Having proven this result, then $y \equiv r$ (mod p^{tn}), i.e., y (mod 10^{tn}) is a tn-place automorph.

First, consider the cases $j = 1, \cdots, t-1$. Let

$$S \equiv \sum_{k=t}^{2t-1} (-1)^{k-t} \binom{k}{j} \binom{k-1}{t-1} \binom{2t-1}{k} .$$

So, by using binomial identities (4) and (5)

$$S = \binom{2t-1}{j} \sum_{k=t}^{2t-1} (-1)^{k-t} \binom{2t-1-j}{k-j} \sum_{i=0}^{t-1} \binom{j-1}{i} \binom{k-j}{t-1-i} .$$

By again using binomial coefficient identity (5), we get

$$S = \binom{2t-1}{j} \sum_{i=0}^{j-1} \binom{j-1}{i} \binom{2t-1-j}{t-1-i} T ,$$

where

$$T \equiv \sum_{k=t}^{2t-1} (-1)^{k-t} \binom{t-j+i}{k-t-j+1+i}$$

$$\equiv (-1)^{j-i-1} \left[\sum_{k=t+j-i-1}^{2t-1} (-1)^{k-t-j+i+1} \binom{t-j+i}{k-t-j+i+1} - \sum_{k=t+j-i-1}^{t-1} (-1)^{k-t-j+i+1} \binom{t-j+1}{k-t-j+i+1} \right] .$$

with the first sum in the brackets equal to zero (by a special case of identity (6)). Then, by binomial coefficient identity (6) again,

$$T = \binom{t-j+i-1}{i-j} .$$

Hence $T = 0$, since $i - j < 0$. Therefore $S = 0$ for $j = 1, 2, \cdots, t-1$.

In case $j = 0$,

$$S = (2t-1) \binom{2t-2}{t-1} \sum_{k=t}^{2t-1} \frac{(-1)^k}{k} \binom{t-1}{k-t}$$

by first applying identity (3), then (5). Hence replacing $k - t$ by t gives

$$S = (2t-1) \binom{2t-2}{t-1} \sum_{k=0}^{t-1} \frac{(-1)^k}{t+k} \binom{t-1}{k} = 1 ,$$

since for the Beta function B,

$$B(t,t) \equiv \int_0^1 v^{t-1}(1-v)^{t-1} dv = \frac{1}{t\binom{2t-1}{t-1}} ,$$

and expanding $(1-v)^{t-1}$ and integrating each term yields

[Continued on page 402.]