STICHTING
MATHEMATISCH CENTRUM
2e BOERHAAVESTRAAT 49
AMSTERDAM

AFDELING ZUIVERE WISKUNDE

ZW 1965-007

A note on the multiplicative semigroup of the residue classes modulo n

by

P.C. Baayen and D. Kruyswijk

November 1965

The Mathematical Centre at Amsterdam, founded the 11th of February, 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications, and is sponsored by the Netherlands Government through the Netherlands Organization for Pure Research (Z.W.O.) and the Central National Council for Applied Scientific Research in the Netherlands (T.N.O.), by the Municipality of Amsterdam and by several industries.

§1. Introduction

Given an arbitrary integer a, we have the following congruence:

$$a(a - 1) \equiv 0 \text{ modulo } 2.$$

Slightly less obvious is the following fact. Given an arbitrary pair of integers a_1, a_2, then at least one of the three numbers

$$a_1(a_1 - 1) \quad , \quad a_2(a_2 - 1) \quad , \quad a_1a_2(a_1a_2 - 1)$$

will be divisible by 3. Verification of this property, by distinguishing some cases, is not difficult and it follows then from our initial congruence, that the same number is divisible by 6.

By suchlike observations we were led to the following question:

Given a modulus n, does there exist a number Q such that any sequence of integers

(1) $$a_1 \, , \, a_2 \, , \, \ldots \, , \, a_Q$$

contains a subsequence of the form

(2) $$a_i, \; a_{i+1}, \ldots, a_j \quad (1 \leq i \leq j \leq Q),$$

for which

(3) $$a_i \; a_{i+1} \ldots a_j (a_i \; a_{i+1} \ldots a_j - 1) \equiv 0 \text{ modulo } n?$$

This is true for $n = 1$ and $n = 2$ with $Q = 1$, and for $n = 3$ and $n = 6$ with $Q = 2$, as we have stated already.

For $n = 4$, 5 and 10 it turns out to be true with $Q = 4$, but in neither case with $Q = 3$. Hence it seems of interest to look for the least possible value of Q which can be assigned to a given n in the above sense, if such a Q exists.

We shall demonstrate in this note that Q always exists.
Moreover we shall prove:

> The least possible value of Q, considered as a function of n, is a multiplicative function of n in the arithmetical sense[*)].

These proofs are given in §5 en §6. Our theorem 1 (§4) which contains all the information in a shortened dialect, will be applied in §7 to a divisor problem, connected with some puzzles on decimals (theorem 2).

Sections 2 and 8 are dedicated to the algebraic background of the problem. In our theorems and proofs, however, we employ the language of elementary number theory.

§2. Algebraic remarks

The existence of Q for a given n can be proved by algebraic methods, even without reference to finite rings or prime factorization. We have given such a proof, in co-operation with P. VAN EMDE BOAS, in [2] of our reference-list. The following theorem provided the key.

Theorem (not to be proved here):

> To each finite semigroup H a positive integer λ can be assigned, such that any word W of length λ over H contains a subword with idempotent value.

Here a subword is understood to consist of one or more consecutive letters of the given word W. It is easy to show, that this theorem implies the affirmative answer to our question as described in (1), (2), (3). To that end, we take for H the multiplicative semigroup of all the residue classes modulo n and denote it by R_n. Clearly each of the integers of (1) defines a class of R_n, namely, the class to which it belongs. Now let λ be the constant, figuring in the theorem just quoted, as determined for the semigroup R_n, and let $Q \geq \lambda$. Then the sequence (1) defines a word W of length Q over R_n, which, by our

[*)] As defined, for instance, in [3] §5.5

theorem, contains a subword w such that

$$|w|^2 = |w| \quad \text{in } R_n.$$

Here $|w|$ means the product of the letters of w. Consequently, the corresponding integers form a sequence (2) with the property, that the numbers $(\prod a_\nu)^2$ and $(\prod a_\nu)$ lie in the same class of R_n. This is equivalent to the assertion (3).

As to the dependence of λ on the order of H, the report [2] provides some upper bounds, which are reasonable enough for the general case. For the special semigroups R_n, however, they turned out to be inadequately large.

In order to find the best possible estimate for R_n, we shall have to apply some tools of number theory.

§3. *Some conventions*

When dealing with arithmetical congruences, it is sometimes difficult to decide, whether residue classes should be considered or integers which belong to these classes. Hence we make the following convention:

a. If we use an arithmetical congruence, it is meant as a relation between integers only (hence not between classes, or between classes and integers).

The following conventions and the subsequent definition might be noted as well. (They are adaptations of the general conventions in [2], which we have used in §2 of this note.)

b. A *word* is a finite sequence of *integers*. We leave the "empty word" out of consideration. The terms of a word will be called *digits*, whatever integers they may be.

c. A *subword* consists of consecutive digits, in their original order of succession.

d. The value of a word w, to be denoted by $|w|$, means the integer which is the product of all the digits of w. To give an example, if w is the word which consists of the single digit -25, we have:

$$|w| = -25.$$

e. Formal division of the word $a_0a_1\ldots a_t$ by the word $a_0a_1\ldots a_s$ $(0 \leq s < t)$ yields the word $a_{s+1}\ldots a_t$.

Definition A word w is called automorphic modulo n if $|w|^2 \equiv |w|$ modulo n.

Remark. We took the term "automorphic" from [1], where it serves as an arithmetical substitute for "idempotent". Our definition is slightly different from GOODSTEIN's, but confusion seems unlikely.

§4. Statement of the main result

The question of §1 is settled by the following theorem.

Theorem 1.

Let $\phi(n)$ be the Eulerian indicator of n. Define a function Q(n) as follows:

$Q(1) = 1$;
$Q(p^\alpha) = \alpha\phi(p^\alpha)$ if p^α is a prime-power $(\alpha \geq 1)$;
$Q(mn) = Q(m)Q(n)$ if m and n are coprime.

Then we have the following properties:

Property I. Any word of Q(n) digits contains a subword which is automorphic modulo n.

Property II. Given $n \geq 3$, there is a word of $Q(n)-1$ digits, which has no automorphic subwords modulo n.

Remarks. Let $p_1^{\alpha_1} \ldots p_t^{\alpha_t}$ be the canonical factorization of the modulus n ($n \geq 2$). Then we have

$$Q(n) = \left(\prod_{i=1}^{t} \alpha_i\right) \cdot \phi(n)$$

and in particular, for $n \leq 14$:

n	2	3	4	5	6	7	8	9	10	11	12	13	14
Q(n)	1	2	4	4	2	6	12	12	4	10	8	12	12

The best possible estimates for the critical wordlength, which could be obtained by the general methods of [2], are as follows:

n	2	3	4	5	6	7	8	9	10	11	12	13	14
$\lambda \leq$	1	2	4	8	4	24	36	54	128	108	256	192	576

We have tabulated them mainly in view of a certain conjecture, to be raised in §8.

§5. Proof of theorem 1, property I

Lemma 1. Let $\bar{n}$ be a number which has property I ($\bar{n} \geq 1$).

Choose a number $g \geq 2$ which is coprime with $\bar{n}$.

Let W^* be a word of $\phi(g)Q(\bar{n})$ digits, all of which are coprime with g.

Then W^* contains a subword which is automorphic modulo $g\bar{n}$.

Proof (Some complications of the following argument will vanish in case $\bar{n} = 1$. It might be advantageous to make that assumption at a first reading.)

For shortness' sake let us write $\phi(g) = \phi$ and $Q(\bar{n}) = Q$. Let W^* be the word

$$c_1 \, c_2 \ldots c_{\phi Q},$$

where the c_i are digits. We consider the sequence of words

(4) $$c_0 \ , \ c_0c_1 \ , \ c_0c_1c_2 \ , \ \dots \ , \ c_0c_1c_2\dots c_{\phi Q},$$

where c_0 is a supplementary digit, which may be chosen arbitrarily, but should be coprime with g. Sequence (4) consists of $\phi Q+1$ terms, each of which is a word, which has a value coprime with g.
By the pigeon-hole principle one may select Q+1 terms from (4), such that the values of all these terms belong to one and the same residue class modulo g. Otherwise there would be more than $\phi(g)$ different classes in the reduced residue-class system modulo g.
These Q+1 terms form a subsequence of (4), which we shall denote by S.
If the second term of S is divided, formally, by the first one, we obtain a word

(5) $$w_1 = c_{i+1}c_{i+2}\dots c_j \quad (1 \leq i+1 \leq j),$$

such that $|w_1| \equiv 1$ modulo g, whilst w_1 is a subword of W^*.

If S contains more than two terms, we divide the third term (formally) by the second one and obtain a word

(6) $$w_2 = c_{j+1}c_{j+2}\dots c_k \quad (j+1 \leq k),$$

such that $|w_2| \equiv 1$ modulo g. It should be noted now, that the index j in (6) is the same one as in (5); hence $c_{i+1}c_{i+2}\dots c_k$ is a subword of W^*.

By continuing the same procedure, the whole sequence S can be exhausted. One will find, finally, a string of adjacent subwords of W^*, viz:

(7) $$w_1 \ , \ w_2 \ , \ \dots \ , \ w_{Q(\bar{n})},$$

such that $|w_\nu| \equiv 1$ modulo g for $1 \leq \nu \leq Q(\bar{n})$.
From this string we shall select a subword of W which is automorphic modulo $g\bar{n}$.

To that end we consider the word

$$|w_1|\ |w_2|\ \ldots\ |w_{Q(\bar{n})}|, \tag{8}$$

which consists of $Q(\bar{n})$ digits, each digit being a well-defined integer (as required in convention b of §3).

One of our assumptions says that I is valid for the modulus $\bar{n}$. Hence (8) contains a subword, say

$$|w_r|\ |w_{r+1}|\ \ldots\ |w_{s-1}|\ |w_s| \quad (1 \leq r \leq s \leq Q(\bar{n})),$$

which is automorphic modulo $\bar{n}$. It follows easily that

$$|w_r\ w_{r+1}\ldots w_{s-1}\ w_s|^2 \equiv |w_r\ w_{r+1}\ldots w_{s-1}\ w_s| \text{ mod } \bar{n}. \tag{9}$$

Since all the words w_ν have the property that $|w_\nu| \equiv 1$ modulo g, it will be clear that (9) remains valid if we replace the modulus $\bar{n}$ by g. As $\bar{n}$ is coprime with g, the congruence (9) will now hold modulo $g\bar{n}$ and this proves the lemma, with

$$w_r\ w_{r+1}\ \ldots\ w_{s-1}\ w_s$$

as the promised subword.

Lemma 2. Given an integer $k \geq 1$, let us assume that property I has been established for all those $n \geq 1$, each of which has less than k different prime-divisors. Then I holds true for any n which has exactly k different prime-divisors.

Proof Choose a number n which has exactly k different prime-divisors, then we have

$$n = p_1^{\alpha_1}\ p_2^{\alpha_2}\ \ldots\ p_k^{\alpha_k} \quad (k \geq 1),$$

where the p_i are different prime-numbers and where each $\alpha_i \geq 1$.

Next, let W be a word of Q(n) digits. We have to ascertain that W contains a subword w for which

$$|w|^2 \equiv |w| \text{ modulo } n. \tag{10}$$

If $|W|$ happens to be $\equiv 0$ modulo n, (10) is true with $w = W$.
If $|W| \not\equiv 0$ mod n, there must be an index i such that

(11) $$|W| \not\equiv 0 \bmod p^{\alpha} \text{ for } p = p_i,\ \alpha = \alpha_i.$$

By the definition of the function $Q(n)$ we have:

$$Q(n) = \alpha\phi(p^{\alpha})Q(\frac{n}{p^{\alpha}}) ,$$

so that we may subdivide the word W into α disjunct subwords, each of length $\phi(p^{\alpha})Q(np^{-\alpha})$.

In view of (11) at least one of these α subwords must have the property that none of its digits is divisible by p. Denote such a subword by W^* and apply lemma 1 with $g = p^{\alpha}$, $\bar{n} = np^{-\alpha}$. One will find that W^* (hence a fortiori W) contains a subword w satisfying (10). This completes the proof.

Lemma 2 provides the proof of property I for all n, by induction with regard to k. One has to start with the observation that property I is true for $n = 1$, this being the only positive integer which has less than one prime-divisor.

§6. Proof of theorem 1, property II

For each value of $n \geq 1$ let us define $q(n)$ as the least possible integer Q which has the property that any word of Q digits contains a subword which is automorphic modulo n. By property I, $q(n)$ exists for all n and $q(n) \leq Q(n)$ for all n.

Hence, if we can prove:

(12) $$q(n) \geq Q(n) \quad \text{for all } n,$$

property II will be certainly valid. The reader will see at once, that the following two lemma's imply the truth of (12):

Lemma 3. If n is a prime-power, we have

$$q(n) \geq Q(n).$$

Lemma 4. Let m,n be a pair of coprime positive integers. Suppose that $q(m) \geq Q(m)$ and $q(n) \geq Q(n)$. Then we have

$$q(mn) \geq Q(mn).$$

Proof of lemma 3 The case n=2 has already been dealt with in our introduction, whence we may assume that $n = p^\alpha \geq 3$, which implies that $\phi(p^\alpha) \geq 2$. Regrettably, we may not assume that $p \geq 3$.

First, let us construct an auxiliary word W with the following properties:

(i) W consists of $\phi(p^\alpha)-1$ digits;
(ii) Each digit of W is coprime with p^α;
(iii) W does not contain a subword w for which $|w| \equiv 1$ modulo p^α.

An easy method of construction of such a word W (not only for p^α but for any $n \geq 3$), is implied by a theorem on finite groups in [2]. The following construction is slightly more difficult, but it leads to more surveyable words W.

If p is odd, let us take an integer r which is a primitive root of p^α and define the word W by

$$W = rrr....rr \quad (\text{length } \phi(p^\alpha)-1).$$

Then W has clearly the three properties (i), (ii) and (iii).

If p = 2, define the word W by

$$W = \mu 5 \mu 5 ... 5 \mu 5 \mu \quad (\text{length } \phi(2^\alpha)-1,\ \alpha \geq 2),$$

where the digit μ is the number -1. Here any subword has either a value of the form -5^k, which cannot be $\equiv 1 \bmod 2^\alpha$ because it is $\equiv -1$ modulo 4, or its value is of the form $+5^k$ with $1 \leq k \leq 2^{\alpha-2}-1$.
It is well-known (and rather easy to prove) that the order of 5 modulo 2^α for $\alpha \geq 2$ is precisely $2^{\alpha-2}$, and it follows at once that

W has no subwords w for which $|w| \equiv 1 \bmod 2^\alpha$; hence W has clearly the properties (i), (ii) and (iii).

The auxiliary word W will help us to prove that $q(p^\alpha) \geq Q(p^\alpha)$. We consider the word

$$Wp_1Wp_2\ldots Wp_{\alpha-1}W \;, \tag{13}$$

where $p_1 = p_2 = \ldots = p_{\alpha-1} = p$; (13) should be interpreted as a single word W if α happens to be 1.

Any subword w of (13) has a value of the form $p^\lambda\nu$, where ν is coprime with p and where $0 \leq \lambda \leq \alpha-1$. If $\lambda = 0$, w must be a subword of W. If $\lambda \geq 1$, we have $|w| \equiv 0 \bmod p$ but $|w| \not\equiv 0 \bmod p^\alpha$. Hence we have in both cases:

$$|w| \not\equiv 1 \bmod p^\alpha \quad \text{and} \quad |w| \not\equiv 0 \bmod p^\alpha \;,$$

which statement is equivalent to $|w|^2 \not\equiv |w| \bmod p^\alpha$.

This means that (13) has no automorphic subwords mod p^α. The number of digits of (13) is $\alpha\phi(p^\alpha)-1$ so that we have, finally:

$$q(p^\alpha) \geq \alpha\phi(p^\alpha) = Q(p^\alpha).$$

<u>Proof of lemma 4</u> To the assumptions of lemma 4 we may safely add:

$$m \geq 2, \quad n \geq 3.$$

If m=2, n must be odd and we have $Q(2n) = Q(2)Q(n) = Q(n)$. By the definition of q(n) it is moreover easy to check that $q(2n) \geq q(n)$, or even that $q(2n) = q(n)$. Hence we have

$$q(2n) \geq q(n) \geq Q(n) = Q(2n).$$

We may assume from now on that both m and n are ≥ 3, which implies that q(m) and q(n) are each ≥ 2.

Let $a_1a_2\ldots a_{q(m)-1}$ be a word without subwords which are automorphic modulo m. Choose, for each index i, an integer b_i such that

$$(14) \qquad \begin{cases} b_i \equiv 1 \mod n \\ b_i \equiv a_i \mod m. \end{cases}$$

This is certainly possible; one may take for instance:

$$b_i = m^{\phi(n)} + a_i n^{\phi(m)}.$$

Then the word

$$(15) \qquad B = b_1 b_2 \ldots b_{q(m)-1}$$

does not contain automorphic subwords modulo m, and it has moreover the property that any one of its subwords has a value $\equiv 1$ modulo n.

Furthermore, let $c_1 c_2 \ldots c_{q(n)-1}$ be a word without automorphic subwords modulo n. Then the word

$$(16) \qquad Bc_1 Bc_2 \ldots Bc_{q(n)-1} B$$

consists of exactly $q(m)q(n) - 1$ digits; we shall prove that none of its subwords w satisfies the congruence $|w|^2 \equiv |w|$ modulo mn.

If a subword w of (16) is contained in one of the subwords of the form B, it is not automorphic modulo m and hence, a fortiori, not automorphic modulo mn.

If a subword w of (16) is not contained in a word B, it will contain one or more digits c_i of (16). In that case we have:

$$|w| \equiv |c_t c_{t+1} \ldots c_{u-1} c_u| \quad \text{modulo } n$$

for a certain pair of indices t,u with $1 \leq t \leq u \leq q(n)-1$; this follows from the fact that the whole word B and any of its subwords have a value $\equiv 1$ modulo n; they are completely "sieved out" when the value of w is calculated modulo n. It follows that w is not automorphic modulo n and hence, a fortiori, not automorphic modulo mn.

We have proved by now, that $q(mn) \geq q(m)q(n)$. Hence, by our assumptions:

$$q(mn) \geq q(m)q(n) \geq Q(m)Q(n) = Q(mn),$$

which proves lemma 4.

§7. A theorem on divisors

The following statement and subsequent remark can be read without regard to our previous text.

Theorem 2. Denote by $\tau(m)$ the number of divisors of m. Then any number A for which

$$\tau(A) > 2^{(n-1)\tau(n)-n} \qquad (n \geq 2) \tag{17}$$

will have a divisor $d \geq 2$ such that

$$d(d-1) \equiv 0 \quad \text{modulo } n.$$

Remark This theorem implies that any positive integer which has more than 2^{791} divisors, certainly possesses a divisor ≥ 2, which ends on

00 , 01 , 25 or 76 ,

if expanded in the decimal scale.

We conjecture, that here the estimate 2^{791} may be replaced by 2^{22}. This result would be best possible, for there exist numbers with exactly 2^{22} divisors, no divisors d of which ends on 00, 01, 25 or 76 ($d \geq 2$).

For introductory information concerning "automorphic" numbers in various scales, see R.L. GOODSTEIN's paper [1].

Proof of theorem 2 By our (former) definition of Q(n) we have for $n \geq 2$:

$$Q(n) = \phi(n)\prod \alpha_i \leq (n-1)\{\prod(\alpha_i+1) - 1\} = (n-1)\{\tau(n)-1\} ,$$

where $\prod \alpha_i$ denotes the product of the exponents in the canonical factorization of n. Hence we have, if we assume (17) to be true for a given A:

$$\tau(A) > 2^{Q(n)-1} .$$

This inequality implies that A can be written as the product of at least Q(n) prime numbers, which may be different from each other or not. (For whatever the case may be, a number which is the product of less than Q prime numbers has at most 2^{Q-1} divisors).

Now let us consider the formal product of all the prime-factors of A as a word, where each prime-factor is a digit and where the order of succession is arbitrary.

It follows from theorem 1 that this word has an automorphic subword modulo n. Denote its value by d, then d is a divisor of A and we have $d \geq 2$. Since moreover $d^2 \equiv d$ modulo n, theorem 2 has been proved.

Remark Readers who might be interested in the order of magnitude of the function Q(n), are invited to prove by elementary methods, as described in [3] Ch.XVIII:

a. $\frac{1}{2}\sqrt{n+1} < Q(n) \leq \frac{1}{2}n\sqrt{n+1}$ for all $n \geq 2$.

b. Given $\varepsilon > 0$, we have $n^{1-\varepsilon} < Q(n) < n^{1+\varepsilon}$ for all n which are sufficiently large.

c. Given $E > 0$, we have $Q(n) > n(\log n)^E$ for infinitely many values of n.

§8. Supplementary algebraic remarks

Let us return to the algebraic point of view, as abandoned at the end of §2. It is clear that the semigroup R_n contains for $n \geq 2$ at least two idempotent elements, zero and unity (for n=1 they coïncide). By simple considerations it can be shown that the exact amount of idempotents in R_n is

$$2^{\omega(n)},$$

where $\omega(n)$ is the number of different prime numbers which divide n.

In [2] an upper bound has been derived for the critical word-length for an abstract semigroup with n elements, θ of which are idempotent. This function (too complicated for quotation here) has extremal properties if $\theta = \left[\frac{n}{3}\right]$.

If we apply it on R_n, with $\theta = 2^{\omega(n)}$, we obtain for $n \leq 14$ the second tabulation of §4.

Here the numbers 7, 12 and 14 are of special interest, because they are the only positive integers n for which $\theta = \left[\frac{n}{3}\right]$ in R_n.

We conjecture that there are positive integers $N(n)$ $(5 \leq n \leq 14)$ such that $R_{N(n)}$ has a subsemigroup of order n with $2^{\omega(n)}$ idempotents, for which the critical wordlength, as given in our second tabulation of §4, is the best possible one. (If this conjecture is true there should exist, for some N, a multiplicative semigroup of residue-classes modulo N, consisting of 14 elements, over which a word of 575 letters can be constructed without subwords of idempotent value).

More generally, we put forward the question whether eachcommutative semigroup of order n can be embedded, isomorphically, in an arithmetical semigroup of the type R_N.

References

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

[2] P.C. BAAYEN, P. VAN EMDE BOAS and D. KRUYSWIJK, A combinatorial problem on finite semigroups. Mathematical Centre Report ZW 1965-006.

[3] G.H. HARDY and E.M. WRIGHT, An introduction to the theory of numbers (4th Edition, Oxford 1960).