Séminaire Delange-Pisot-Poitou. Théorie des nombres

H. W., Jr. Lenstra

Perfect arithmetic codes

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 19, n° 1 (1977-1978), exp. n° 15, p. 1-14

<http://www.numdam.org/item?id=SDPP_1977-1978__19_1_A12_0>

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1977-1978, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

Numdam
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire DELANGE-PISOT-POITOU
(Théorie des Nombres)
19e année, 1977/78, n° 15, 14 p.

12 décembre 1978

PERFECT ARITHMETIC CODES

by H. W. LENSTRA Jr

1. Cyclic AN-codes.

Let r and n be integers with $r \geqslant 2$ and $n \geqslant 3$. For x, $y \in \underset{\sim}{Z}/(r^n - 1)\underset{\sim}{Z}$, the arithmetic distance $d(x, y)$ is defined to be the smallest integer $t \geqslant 0$ for which there exists a representation

$$x - y = (\sum_{i=1}^{t} c_i \, r^{n(i)} \mod (r^n - 1)),$$

with c_i, $n(i) \in \underset{\sim}{Z}$, $|c_i| < r$, $n(i) \geqslant 0$, for $1 \leqslant i \leqslant t$. It is easily seen that d is a metric on $\underset{\sim}{Z}/(r^n - 1)\underset{\sim}{Z}$.

An arithmetic code, or more precisely a cyclic AN-code of word length n in base r, is a subgroup C of $\underset{\sim}{Z}/(r^n - 1)\underset{\sim}{Z}$. The "AN" in the terminology is explained by the observation that every such code can be represented as

$$C = \{AN \mod (r^n - 1) \; ; \; 0 \leqslant N < B\},$$

for a unique pair A, B of positive integers, with $AB = r^n - 1$. The adjective "cyclic" does not refer to the group structure of the code, but to the following property. Let the elements of $\underset{\sim}{Z}/(r^n - 1)\underset{\sim}{Z}$ be represented by their digits in base r, i. e. let the "word" $(c_i)_{i=0}^{n-1}$ represent the element $\sum_{i=0}^{n-1} c_i \, r^i \mod (r^n - 1)$; only $0 \mod (r^n - 1)$ has two such representations. Then, for every cyclic AN-code C, and every word $(c_i)_{i=0}^{n-1} \in C$, also the cyclically permuted word $(c_{i-1})_{i=0}^{n-1}$, with $c_{-1} = c_{n-1}$, belongs to C, since

$$\sum_{i=0}^{n-1} c_{i-1} \, r^i \equiv r \sum_{i=0}^{n-1} c_i \, r^i \mod (r^n - 1).$$

Arithmetic codes are used for checking additions and subtractions of numbers written in base r, see ([9], [11], [12]). The procedure is roughly as follows. To add two numbers N_1, N_2, one encodes them as AN_1, AN_2, and one adds the encoded numbers in $\underset{\sim}{Z}/(r^n - 1)\underset{\sim}{Z}$; let the result be S. Next, one determines $AN_3 \in C$, with $d(AN_3, S)$ least possible. If no errors have been made, then $AN_3 = S$, and N_3 is the sum of N_1 and N_2 (mod B). Generally, $d(AN_3, S)$ is a lower bound for the number of errors which have been made, and N_3 is the most likely result of the addition $N_1 + N_2$ (mod B).

In this way, all combinations of e, or fewer, errors, can be corrected if, and only if, for every $x \in \underset{\sim}{Z}/(r^n - 1)\underset{\sim}{Z}$, there is at most one $c \in C$, with $d(x, c) \leqslant e$. A code having this property is called e-error-correcting. If, for every $x \in \underset{\sim}{Z}/(r^n - 1)\underset{\sim}{Z}$, there exists exactly one $c \in C$, with $d(x, c) \leqslant e$, the code is called perfect. If we put

$$S_e = \{s \in \underset{\sim}{Z}/(r^n - 1)\underset{\sim}{Z} \; ; \; d(s, 0) \leqslant e\},$$

then a subgroup $C \subset \underline{Z}/(r^n - 1)\underline{Z}$ is a perfect e-error-correcting arithmetic code if, and only if, every $x \in \underline{Z}/(r^n - 1)\underline{Z}$ has a unique representation $x = s + c$, with $s \in S_e$ and $c \in C$. We will be interested in the case $e = 1$, cf. ([1], [3], [4], [5]).

2. Perfect one-error-correcting arithmetic codes.

Example. - Let $r = n = 3$, then $r^n - 1 = 26$. We have

$$S_1 = \{0 , \pm 1 , \pm 2 , \pm 3 , \pm 6 , \pm 9 , \pm 18\} \subset \underline{Z}/26\underline{Z} .$$

It is easily checked that, for every $x \in \underline{Z}/26\underline{Z}$, we have either $x \in S_1$, or $x \in 13 + S_1$. Hence the subgroup $C = \{0 , 13\}$ is a perfect one-error-correcting cyclic 13N-code of word length 3 in base 3. This code can be used to check additions modulo 2 (= B) on a ternary computer.

In the general case, we have

$$S_1 = \{0 , \pm c.r^j \mod r^n - 1 ; \ 1 \leqslant c \leqslant r - 1 , \ 0 \leqslant j < n\} ,$$

$$\#S_1 = 1 + 2(r - 1).n$$

(here, we use that $n \geqslant 3$). Let $C \subset \underline{Z}/(r^n - 1)\underline{Z}$ be generated by $A \mod (r^n - 1)$, where A divides $r^n - 1$. This is a perfect one-error-correcting code if, and only if, every $x \in \underline{Z}/(r^n - 1)\underline{Z}$ is uniquely representable as

$$x = AN , \text{ or } x = AN \pm cr^j ,$$

with $AN \in C$, $1 \leqslant c \leqslant r - 1$, $0 \leqslant j < n$. If this condition is satisfied, then

$$r^n - 1 = \#C \, \#S_1 = \frac{r^n - 1}{A} (1 + 2(r - 1)n) ,$$

so A and n determine each other by

$$A - 1 = 2(r - 1)n .$$

Passing to $(\underline{Z}/(r^n - 1)\underline{Z})/C \cong \underline{Z}/A\underline{Z}$, we see that C is perfect one-error-correcting if, and only if, every $x \in \underline{Z}/A\underline{Z}$ can be written in a unique way as

$$x = (0 \mod A) , \text{ or } x = (\pm cr^j \mod A) ,$$

with $1 \leqslant c \leqslant r - 1$, $0 \leqslant j < n$. It was observed by GOTO and FUKUMURA [4], and by BOJARINOV and KABATJANSKIJ [1] that this condition implies that A is prime. To see this, suppose that $A = ab$, with $a < A$, $b < A$. With $x = (a \mod A)$, we find $a \equiv \pm cr^j \mod A$, so a divides cr^j; but a is coprime with r, since it divides $r^n - 1$, so a divides c, hence $a < r$. Similarly $b < r$. Then $A < r^2$, so A has in base r at most two digits : $A = c_1 r + c_0$, $0 \leqslant c_i < r$. But then $x = (c_0 \mod A)$ has two representations,

$$x = (c_0 \mod A) , \ x = (- c_1 r \mod A) ,$$

contradicting our uniqueness assumption. We conclude that A is prime.

Observing that $\{1 , r , \dots , r^{n-1}\}$ is a subgroup of $\underset{\sim}{F}_A^*$, we arrive at the following proposition.

(2.1) PROPOSITION. - Let A be a positive integer. Then A generates a perfect one-error-correcting cyclic AN-code in base r if, and only if, A is prime, and (i) and (ii) hold :

(i) The subgroup $\langle r \mod A\rangle$ of $\underset{\sim}{F}_A^*$ has index 2 in the subgroup $\langle r \mod A , -1 \mod A\rangle$;

(ii) The subgroup $\langle r \mod A , -1 \mod A\rangle$ has index $r - 1$ in $\underset{\sim}{F}_A^*$, with $1 , 2 , \dots , r - 1 \pmod A$ as a complete system of representatives.

The word length n of the code is determined by

$$n = \frac{A - 1}{2(r - 1)} = \#\langle r \mod A\rangle ;$$

it is necessarily odd, since $(-1 \mod A) \notin \langle r \mod A\rangle$, by (i). Notice that, in (ii), we may replace $1 , 2 , \dots , r - 1$ by $2 , 3 , \dots , r - 1 , r$, since $r \equiv 1 \mod \langle r \mod A , -1 \mod A\rangle$.

Example [11]. - Let $r = 2$. In this case (i) and (ii) mean

$$\langle 2 \mod A\rangle \subsetneq \langle 2 \mod A , -1 \mod A\rangle = \underset{\sim}{F}_A^* ,$$

and this is easily seen to be equivalent to

$$A \equiv 7 \mod 8 \text{ and } -2 \text{ is a primitive root } \mod A .$$

Examples are $A = 7 , 23 , 47 , 71 , 79 , 103 , 167 , \dots$. If Artin's conjecture on primes, with a prescrived primitive root, is true, the condition is satisfied for 18,69779... % of all prime numbers. We remark that this conjecture is known to be a consequence of the generalized Riemann hypothesis [6].

Example [5]. - Let $r = 3$. In this case, $(3 \mod A)$ must have odd order $(A - 1)/4$ in $\underset{\sim}{F}_A^*$. Then, $A \equiv 5 \mod 8$, and $-1 \notin \langle 3 \mod A\rangle$, and $2 \notin \langle 3 \mod A , -1 \mod A\rangle$ are automatically satisfied. Examples are $A = 13 , 109 , 181 , 229 , 277 , 421 , \dots$. Modulo the Riemann hypotheses, 3,739558 % of all primes satisfy the condition.

In the general case, we are interested in conditions on r which are necessary and probably sufficient for the existence of perfect one-error-correcting codes in base r .

Assume that A as in (2.1) exists. Then

(2.2) r is no square,

since if $r = s^2$, say, then $s^{(A-1)/(r-1)} = s^{2n} = r^n \equiv 1 \mod A$, so $s \equiv t^{r-1} \mod A$, for some t , contradicting that s , by condition (ii), represents a non-trivial element in the group $\underset{\sim}{F}_A^*/\langle r \mod A , -1 \mod A\rangle \cong \underset{\sim}{Z}/(r - 1)\underset{\sim}{Z}$.

By (ii), the canonical map

$$\{2\ ,\ 3\ ,\ \ldots\ ,\ r-1\ ,\ r\} \longrightarrow \underset{\sim}{F}_A^*/\langle r \mod A\ ,\ -1 \mod A\rangle$$

is bijective, and this gives :

(2.3) There exists a group multiplication $*$ on $V = \{2\ ,\ 3\ ,\ \ldots\ ,\ r-1\ ,\ r\}$ such that :

(2.4) $(V\ ,\ *)$ is a cyclic group of order $r-1$ with neutral element r ;

(2.5) $a * b = ab$ whenever $a\ ,\ b \in V$ are such that $ab \in V$;

(2.6) If p is prime and $2p$ divides $r-1$, then p is a square in $(V\ ,\ *)$;

(2.7) If $r \equiv -1 \mod 4$, then 2 is no square in $(V\ ,\ *)$.

To prove (2.6), notice that $A = 1 + 2(r-1)n \equiv 1 \mod 4p$, so the Legendre symbol (p/A) equals 1, and $(p \mod A) \in \underset{\sim}{F}_A^{*2}$. This proves (2.6). Similarly, if $r \equiv -1 \mod 4$, then $A \equiv 5 \mod 8$, since n is odd, so $(2/A) = -1$, which implies that 2 is not a square in $(V\ ,\ *)$. This proves (2.7).

Example. - Let $r = 10$, and suppose that $V = \{2\ ,\ 3\ ,\ \ldots\ ,\ 9\ ,\ 10\}$ has a cyclic group structure satisfying (2.4) and (2.5). Since $2^3 = 8 \neq 10$ (= unit element), the order of 2 in V is 9, so 2 generates the group, and

$$2^1 = 2\ ,\ \ 2^2 = 4\ ,\ \ 2^3 = 8\ ,\ \ 2^9 = 10\ ,\ \ 2^8 = 5 \quad \text{(since } 2.5 = 10\text{)}.$$

Let $3 = 2^x$. Clearly, $x \neq 1\ ,\ 2\ ,\ 3\ ,\ 8$ or 9 . If $x = 4\ ,\ 5$ or 6, then $9 = 3^2 = 2^8\ ,\ 2^1$ or $2^3 = 5\ ,\ 2$ or 8, a contradiction. Also $x = 7$ leads to a contradiction : $6 = 2^{x+1} = 2^8 = 5$. We conclude that no perfect one-error-correcting arithmetic code in base 10 exists, cf. ([4] (for the case $A < 10^6$), [3]).

The following theorem shows that the necessary conditions (2.2), (2.3), (2.4), (2.5), (2.6), (2.7), for the existence of a perfect one-error-correcting arithmetic code in base r , are, conversely, sufficient for the existence of infinitely many such codes, if certain Riemann hypotheses are true. If M is a set of prime numbers, the limit

$$\lim_{x\to\infty} \frac{\#\{p\ ;\ \ p \in M\ ,\ \ p \leqslant x\}}{\#\{p\ ;\ \ p \text{ prime},\ p \leqslant x\}}\ ,$$

if it exists, is called the density of M , and denoted by $d(M)$.

(2.8) THEOREM. - Let r be an integer $\geqslant 2$ satisfying (2.2)-(2.7), and suppose that, for every squarefree integer m , the ζ-function of the field $\mathbb{Q}(\zeta_{2m(r-1)}\ ,\ \sqrt[m(r-1)]{r})$ satisfies the generalized Riemann hypothesis. Here ζ_k denotes a primitive k-th root of unity. Then, there exist infinitely many prime numbers A which generate a perfect one-error-correcting cyclic AN-code inbase r ; more precisely the set S of these prime numbers has strictly positive density.

The proof of this theorem is outlined in the following section. We shall also give a precise formula for $d(S)$, under the assumptions of the theorem.

3. Proof of the theorem.

Denote by L the infinite Galois extension of $\mathbb{Q}$ obtained by adjoining ζ_k and $\sqrt[k]{a}$ to $\mathbb{Q}$, for all $k \in \mathbb{Z}$, $k \geqslant 1$, $a \in \mathbb{Q}$, $a > 0$, with ζ_k as in (2.8). We translate the conditions (2.1) (i) and (2.1) (ii) on A in conditions about the behaviour of the prime A in $L/\mathbb{Q}$.

Let A be prime, and let $(A, L/\mathbb{Q})$ denote the set of all $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ for which there exists a prime $\mathfrak{A}$ of L lying over A such that $\sigma(\alpha) \equiv \alpha^A \bmod \mathfrak{A}$, for all algebraic integers $\alpha \in L$. Let $\sigma \in (A, L/\mathbb{Q})$.

If (2.1) (i) and (2.1) (ii) hold, then $\mathbb{F}_A^*$ has a subgroup of index $2(r-1)$, so $A \equiv 1 \bmod 2(r-1)$. This is equivalent to

$$\sigma(\zeta_{2(r-1)}) = \zeta_{2(r-1)}^{A}, \tag{3.1}$$

if $A > r$. The requirement that $\mathbb{F}_A^{*2(r-1)}$ contains $(r \bmod A)$, but not $(-1 \bmod A)$, is expressed by

$$\sigma(\sqrt[2(r-1)]{r}) = \sqrt[2(r-1)]{r}, \tag{3.2}$$

$$\sigma(\sqrt[2(r-1)]{-1}) \neq \sqrt[2(r-1)]{-1}. \tag{3.3}$$

Notice that (3.1) and (3.3) are together equivalent to

$$\sigma(\zeta_{4(r-1)}) = -\zeta_{4(r-1)}^{A}. \tag{3.4}$$

Condition (2.1) (ii) implies that no two of $2, 3, \ldots, r-1, r \pmod A$ are congruent modulo the subgroup $\mathbb{F}_A^{*(r-1)}$, which is expressed by

$$\sigma(\sqrt[r-1]{(a/b)}) \neq \sqrt[r-1]{(a/b)}, \text{ for all } a, b \in \mathbb{Z},\ 2 \leqslant a < b \leqslant r. \tag{3.5}$$

We have not yet expressed the condition that $\mathbb{F}_A^{*(r-1)}$ is generated by $(r \bmod A)$ and $(-1 \bmod A)$. This is equivalent to the non-existence of a prime ℓ dividing the index $[\mathbb{F}_A^{*(r-1)} : \langle r \bmod A, -1 \bmod A\rangle]$, i. e. for which $A \equiv 1 \bmod 2(r-1)\ell$ and $(r \bmod A) \in \mathbb{F}_A^{*(r-1)\ell}$. This leads to

$$\sigma|\{\zeta_{2(r-1)\ell}, \sqrt[(r-1)\ell]{r}\} \neq \mathrm{id}, \text{ for every prime number } \ell, \tag{3.6}$$

in the case $\ell = A$, this may be wrong for some, but not all, $\sigma \in (A, L/\mathbb{Q})$.

We conclude that a prime number A satisfies (2.1) (i) and (2.1) (ii) if, and only if, $A > r$ and

$$(A, L/\mathbb{Q}) \cap \mathcal{U} \neq \emptyset,$$

where

$$\mathcal{U} = \{\sigma \in \mathrm{Gal}(L/\mathbb{Q}) ;\ \sigma \text{ satisfies } ((3.2), (3.4), (3.5), (3.6))\}. \tag{3.7}$$

Let μ denote the Haar measure on $\mathrm{Gal}(L/\mathbb{Q})$, normalized such that $\mu(\mathrm{Gal}(L/\mathbb{Q})) = 1$.

(3.8) PROPOSITION. - Let the hypotheses and notations be as in (2.9), (3.7). Then $d(S) = \mu(\mathcal{U})$.

Proof. - The proposition would be an immediate consequence of the Čebotarev den-

sity theorem ([10], Chap. 7, § 3) if (3.6) would only be required for finitely many primes ℓ. In our situation, the desired conclusion can be drawn by appealing to a suitably generalized form of Artin's conjecture on primes with prescribed primitive roots, which is known to be a consequence of the Riemann hypotheses mentioned in (2.9) (see [2], [6], [8]). This proves (3.8).

We remark that, without any unproved hypothesis, it can be proved that $d^+(S) \leq \mu(\mathcal{U})$, where

$$d^+(S) = \limsup_{x\to\infty} \frac{\#\{A\ ;\ A \in S\ ,\ A \leq x\}}{\#\{A\ ;\ A \text{ is prime},\ A \leq x\}}\ .$$

To prove the theorem, it suffices to show that $\mu(\mathcal{U}) > 0$ if (2.2), (2.3), (2.4), (2.5), (2.6), (2.7) are satisfied. In [8], it is proved that, for sets $\mathcal{U}$ of the type, we are considering it is true that

$$\mu(\mathcal{U}) > 0 \text{ if, and only if, } \mathcal{U} \neq \emptyset\ .$$

We give an outline of the proof that $\mathcal{U} \neq \emptyset$ if (2.2)-(2.7) hold.

We begin with an explicit description of $\mathrm{Gal}(L/\underset{\sim}{Q})$. Choose $\zeta_k = \exp(2\pi i/k)$, $\sqrt[k]{a} = \exp((\log a)/k)$, for $k \in \underset{\sim}{Z}$, $k \geq 1$, $a \in \underset{\sim}{Q}$, $a > 0$, and let $\hat{\underset{\sim}{Z}}$ be the profinite completion of $\underset{\sim}{Z}$, with group of units $\hat{\underset{\sim}{Z}}^*$.

(3.9) PROPOSITION. - *Let $\sigma \in \mathrm{Gal}(L/\underset{\sim}{Q})$. Then, there is a unique element $u \in \hat{\underset{\sim}{Z}}^*$, and a unique sequence $(v(p))_{p \text{ prime}}$, with $v(p) \in \hat{\underset{\sim}{Z}}$, for p prime, such that*

(3.10) $$\sigma(\zeta_k) = \zeta_k^u \text{, for all } k \in \underset{\sim}{Z},\ k \geq 1\ ;$$

(3.11) $$\sigma(\sqrt[k]{p}) = \zeta_k^{v(p)}\sqrt[k]{p} \text{, for all } k \in \underset{\sim}{Z},\ k \geq 1, \text{ and all primes } p\ ;$$

(3.12) $$(-1)^{v(p)} = \left(\frac{p}{u}\right) \text{ (Jacobi-symbol), for all primes } p\ .$$

Conversely, if $u \in \hat{\underset{\sim}{Z}}^*$, $v(p) \in \hat{\underset{\sim}{Z}}$ (for p prime) satisfy (3.12), then there is a unique element $\sigma \in \mathrm{Gal}(L/\underset{\sim}{Q})$ satisfying (3.10), (3.11).

Proof. - The existence of unique u, $v(p)$ such that (3.10), (3.11) hold is obvious, and (3.12) is proved by calculating $\sigma(\sqrt{p})/\sqrt{p}$ in two ways : using (3.11), or using (3.10), with $\sqrt{p}$ expressed as a Gauss sum.

The converse follows by Kummer theory over the base field $K = \underset{\sim}{Q}(\zeta_k\ ;\ k = 1,2,3,\ldots)$ if we know that

(3.13) For all $u \in \hat{\underset{\sim}{Z}}^*$, there exists $\sigma \in \mathrm{Gal}(K/\underset{\sim}{Q})$ such that (3.10) holds ;

(3.14) $$\{\sqrt[k]{a}\ ;\ k \in \underset{\sim}{Z},\ k \geq 1,\ a \in \underset{\sim}{Q},\ a > 0\} \cap K = \{\sqrt[2]{a}\ ;\ a \in \underset{\sim}{Q},\ a > 0\}\ .$$

Here (3.13) follows from the irreducibility of the cyclotomic polynomials, the inclusion $\supset$ in (3.14) is proved by expressing square roots as Gauss sums, and the opposite inclusion is proved as follows. Let $\sqrt[k]{a} \in K$, with $k \in \underset{\sim}{Z}$, $k \geq 1$, $a \in \underset{\sim}{Q}$, $a > 0$, let $\tau \in \mathrm{Gal}(K/\underset{\sim}{Q})$ be complex conjugation, and let $\rho \in \mathrm{Gal}(K/\underset{\sim}{Q})$ be arbitrary. Then, $\rho(\sqrt[k]{a}) = \eta\sqrt[k]{a}$, for some η, with $\eta^k = 1$, and $\tau(\eta) = \eta^{-1}$,

$\tau(\sqrt[k]{a}) = \sqrt[k]{a}$. Since $Gal(K/\underset{\sim}{Q})$ is abelian, we have

$$\rho(\sqrt[k]{a}) = \rho\tau(\sqrt[k]{a}) = \tau\rho(\sqrt[k]{a}) = \tau(\eta\sqrt[k]{a}) = \eta^{-1}\sqrt[k]{a} .$$

Multiplying by $\rho(\sqrt[k]{a}) = \eta\sqrt[k]{a}$, we find $\rho(\sqrt[k]{a^2}) = \sqrt[k]{a^2}$, for all ρ , so $b = \sqrt[k]{a^2}$ belongs to $\underset{\sim}{Q}$, and $\sqrt[k]{a} = \sqrt[2]{b}$, as required. This proves (3.9).

If $(v(p))_{p \text{ prime}}$ is as in (3.9), then, for $m \in \underset{\sim}{Z}$, $m > 0$, we define $v(m)$ by

$$(3.15) \qquad v(p_1 p_2 \cdots p_h) = v(p_1) + v(p_2) + \cdots + v(p_h) \in \hat{\underset{\sim}{Z}}$$

(p_1 , p_2 , $\cdots$, p_h prime). Notice that we then have $\sigma(\sqrt[k]{m}) = \zeta_k^{v(m)}\sqrt[k]{m}$, for all $k \in \underset{\sim}{Z}$, $k \geqslant 1$, in the situation of (3.9).

Suppose now that (2.2)-(2.7) are satisfied, and let $\psi : (V, *) \longrightarrow \underset{\sim}{Z}/(r-1)\underset{\sim}{Z}$ be a group isomorphism. Here, we use (2.4). We claim that, for an element σ of $Gal(L/\underset{\sim}{Q})$ to belong to $\mathcal{U}$, it suffices that the numbers u , $v(p)$ from (3.9) satisfy

$$(3.16) \qquad v(r) \equiv 0 \mod 2(r-1) ;$$

$$(3.17) \qquad u \equiv 1 + 2(r-1) \mod 4(r-1) ;$$

$$(3.18) \qquad v(p) \equiv \psi(p) \mod (r-1) \text{ , for all primes } p < r ;$$

(3.19) For no prime number ℓ , we have both

$$u \equiv 1 \mod 2(r-1)\ell , \quad v(r) \equiv 0 \mod (r-1)\ell .$$

The properties (3.2), (3.4), (3.6) of σ are obviously equivalent to (3.16), (3.17), (3.19), respectively. From (3.18), (3.15), (2.5) and the fact that ψ is a group homomorphism, we see that $v(a) \equiv \psi(a) \mod (r-1)$, for all $a \in \underset{\sim}{Z}$, $2 \leqslant a \leqslant r$, so the fact that ψ is bijective gives (3.5). This proves our claim.

By (2.6), (2.7), we have

(3.20) If p is prime and $2p \mid r-1$, then $\psi(p)$ is even ;

(3.21) If $r \equiv 3 \mod 4$, then $\psi(2)$ is odd.

To finish the proof that $\mathcal{U} \neq \emptyset$, and hence the proof of the theorem, it suffices to see that the conditions (3.12), (3.16), (3.17), (3.18), (3.19) are compatible if (2.2), (3.20), (3.21) hold. This is an entirely straightforward combinatorial exercise, which we leave to the reader ; notice that (3.20), (3.21) are forced by (3.12), (3.17), (3.18). This concludes our outline of the proof of theorem (2.9).

With slightly more effort, one can determine the number $\mu(\mathcal{U})$, which by (3.8) equals $d(S)$ if the Riemann hypotheses are true. The result is as follows.

(3.22) PROPOSITION. - Let r be an integer $\geqslant 2$ which is no square, and define

$$q = \#\{p ; \ p \text{ prime}, \ p \leqslant r\} ,$$

$$t = \#\{p ; \ p \text{ prime}, \ 2p \mid r-1\} ,$$

$$w = \max\{m \in \mathbb{Z} \ ; \ r \text{ is an } m\text{-th power}\} \ .$$

Let $\mathfrak{U}$ be as in (3.7), and W the set of group multiplications $*$ on $V = \{2 , 3 , \dots , r - 1 , r\}$ satisfying (2.4), (2.5), (2.6), (2.7). Further, if r is even, put

$$c = \frac{1}{4(r-1)^q} \prod^{I}(1 - \frac{1}{\ell^2}) \prod^{II}(1 - \frac{1}{\ell(\ell-1)}) \ ,$$

with $\prod^{I}$ ranging over the primes ℓ with $\ell | r - 1$, $\ell \nmid w$, and $\prod^{II}$ over those with $\ell \nmid 2(r-1)$. If r is odd, then, for $* \in W$, put

$$c_* = \frac{2^{t-2}}{(r-1)^q} \prod^{III}(1 - \frac{1}{\ell^2}) \prod^{IV}(1 - \frac{2}{\ell(\ell-1)}) \prod^{V}(1 - \frac{1}{\ell(\ell-1)}) \ ,$$

with $\prod^{III}$ ranging over the primes ℓ with $\ell | r - 1$, $\ell \nmid 2w$, the product $\prod^{IV}$ over those primes $\ell \leqslant r$, $\ell \nmid r - 1$, which are squares in $(V , *)$, and $\prod^{V}$ over the primes $\ell > r$. Then, we have :

(a) If $r = r_0 r_1^2$, with r_0 odd and squarefree, and r_1 even, then

$$\mu(\mathfrak{U}) = \#W.c(1 + (-1)^{(r_0-1)/2} \prod \frac{-1}{\ell^2 - \ell - 1}) \ ,$$

with $\prod$ ranging over the primes ℓ dividing r_0 ,

(b) If r is even, but not as in (a), i. e. 2 occurs to an odd power in r , then

$$\mu(\mathfrak{U}) = \#W.c \ ;$$

(c) If $r \equiv 1 \mod 4$, then

$$\mu(\mathfrak{U}) = \frac{1}{2} \sum_{* \in W} c_* \ ;$$

(d) If $r \equiv 3 \mod 4$, then

$$\mu(\mathfrak{U}) = \sum_{* \in W} c_* \ .$$

4. Perfect negacyclic codes.

A negacyclic AN-code of word length n in base r is a subgroup $C \subset \mathbb{Z}/(r^n + 1)\mathbb{Z}$, where n is an integer $\geqslant 2$. Arithmetic distance and perfectness are defined as in the cyclic case.

Example. - Let $r = 2$, $n = 5$, then $r^n + 1 = 33$. The elements of $\mathbb{Z}/33\mathbb{Z}$, with arithmetic distance $\leqslant 1$ to 0 , are

(4.1) $0 \ , \pm 1 \ , \pm 2 \ , \pm 4 \ , \pm 8 \ , \pm 16$.

Every $x \in \mathbb{Z}/33\mathbb{Z}$ is of exactly one of the three forms $x = s$, $x = s + 11$, $x = s + 22$, with s one of the elements (4.1). It follows that $C = \{0 , 11 , 22\}$ is a perfect one-error-correcting negacyclic code.

The results of the preceding sections all have analogues for perfect one-error-correcting negacyclic AN-codes. The modifications are as follows.

In proposition (2.1), condition (i) is replaced by

(i') $\langle r \mod A \rangle = \langle r \mod A , -1 \mod A \rangle$.

The word length $n = (A - 1)/2(r - 1) = (1/2)\#\langle r \mod A \rangle$ is not necessarily odd, and the proof that conditions (2.2) and (2.7) are necessary breaks down. No new conditions take their place, and we have the following theorem.

(4.2) THEOREM. - Let r be an integer ≥ 2 satisfying (2.3), (2.4), (2.5), (2.6) and suppose that, for every squarefree integer m, the ζ-function of the field $\mathbb{Q}(\zeta_{2m(r-1)}, \sqrt[m(r-1)]{r})$ satisfies the generalized Riemann hypothesis. Then, there exist infinitely many prime numbers A which generate a perfect one-error-correcting negacyclic AN-code in base r ; more precisely, the set S' of these prime numbers has strictly positive density.

In the proof of this theorem, the role of $\mathcal{U}$ is played by

$\mathcal{U}' = \{\sigma \in \mathrm{Gal}(L/\mathbb{Q})$; σ satisfies (3.1), (3.5), (3.6) and $\sigma(\sqrt[r-1]{r} = \sqrt[r-1]{r}\}$.

The Riemann hypotheses imply that

$$d(S') = \mu(\mathcal{U}') ,$$

and $\mu(\mathcal{U}')$ is given by the following proposition.

(4.3) PROPOSITION. - Let r be an integer ≥ 2, and q, t, w as in (3.22). Let $\mathcal{U}'$ be as just defined, and W' the set of group multiplications on $V = \{2 , 3 , \ldots , r - 1 , r\}$ satisfying (2.4), (2.5), (2.6). Define c, if r is even, and c_*, if r is odd, for $* \in W'$, as in (3.22). Then, we have :

(a) If $r = r_0 r_1^2$, with r_0 squarefree, $r_0 \equiv 1 \mod 4$ and r_1 even, then

$$\mu(\mathcal{U}') = 2 \#W' \cdot c \left(1 - \prod \frac{-1}{\ell^2 - \ell - 1}\right) ,$$

with ℓ ranging over the primes ℓ dividing r_0 ;

(b) If r is even, but not as in (a), then

$$\mu(\mathcal{U}') = x \#W' . c ;$$

(c) If r is an odd square, then

$$\mu(\mathcal{U}') = 2 \sum_{* \in W'} c_* ;$$

(d) If r is odd, but not a square, then

$$\mu(\mathcal{U}') = \sum_{* \in W'} c_* .$$

5. Examples.

(5.1) PROPOSITION. - No perfect one-error-correcting cyclic or negacyclic AN-codes in base r exist if r assumes one of the following values :

(a) $r = 5 , 9 , 10 , 13 , 25$;

(b) $r = s^w$, with $w \nmid r - 1$.

In addition, no perfect one-error-correcting cyclic AN-code in base r exists if r is a square.

Proof. - For $r = 10$, see (2.8). The other four cases are similar to each other ; we only treat $r = 25$. Let $V = \{2 , 3 , \dots , 24 , 25\}$ have a group multiplication $*$ satisfying (2.4), (2.5), (2.6). By (2.6), the numbers 2 and 3 are squares in $(V , *)$, and since 5 has order two, it is also a square. This gives fifteen squares in V :

$$2 , 3 , 4 , 5 , 6 , 8 , 9 , 10 , 12 , 15 , 16 , 18 , 20 , 24 , 25 ,$$

contradicting that, in a cyclic group of order 24 , there are only twelve squares.

For the last statement of (5.1), see (2.2). This proves (5.1).

Notice that powers of two fall under (5.1) (b) : If $r = 2^w$, $w > 1$, and w divides $2^w - 1$, then let q be the smallest prime dividing w . From $(q - 1 , w) = 1$, $2^{q-1} \equiv 1 \mod q$, $2^w \equiv 1 \mod q$, it then follows that $2^1 \equiv 1 \mod q$, a contradiction. Hence, there exist no perfect one-error-correcting arithmetic codes in base 2^w , $w > 1$. The result is due to BOJARINOV and KABATJANSKIJ [1].

I do not know whether, for all r , other than those in (5.1) perfect arithmetic codes do exist. Modulo the Riemann hypotheses, this problem comes down to constructing group multiplications $*$ as in (2.3). I can only do this in certain special cases.

One way to proceed is as follows. Suppose one finds a map

$$\psi : \{p ; p \text{ prime}, p \leq r\} \longrightarrow \mathbb{Z}/(r - 1)\mathbb{Z}$$

such that ψ , when extended to $V = \{2 , 3 , \dots , r\}$ by the rule

$$\psi(ab) = \psi(a) + \psi(b) ,$$

becomes a bijection satisfying

(5.2) $\psi(r) = 0$;

(5.3) $\psi(p)$ is even if p is prime and $2p \mid r - 1$;

(5.4) $\psi(2)$ is odd if $r \equiv 3 \mod 4$.

Then, a group multiplication $*$ on V satisfying (2.4), (2.5), (2.6), (2.7) is given by $a * b = \psi^{-1}(\psi(a) + \psi(b))$.

For example, if $r = 6$, one can take $\psi(2) = 1$, $\psi(3) = 4$, $\psi(5) = 3 \pmod 5$, and if $r = 15$, then $\psi(2) = 1$, $\psi(3) = 4$, $\psi(5) = 10$, $\psi(7) = 12$, $\psi(11) = 7$, $\psi(13) = 9 \pmod{14}$ works. All $r \leq 60$, except those in (5.1), can be treated in this way.

The following heuristic argument leads one to expect that, for all sufficiently

large r with $w|(r-1)$ (cf. (3.22), (5.1) (b)), such a ψ can be found. The number of maps $\{p\ ;\ p \text{ prime},\ p \leqslant r\} \longrightarrow \underset{\sim}{Z}/(r-1)\underset{\sim}{Z}$ is $(r-1)^q$, with q as in (3.22). The probability that the extended map $V \longrightarrow \underset{\sim}{Z}/(r-1)\underset{\sim}{Z}$ satisfies (5.2), (5.3), (5.4) is $w.2^{-t}/(r-1)$ or $w.2^{-t-1}/(r-1)$, with t as in (3.22). If we further estimate the probability for the map to be bijective to be $(r-1)!/(r-1)^{r-1}$, then we find

$$\frac{w.(r-1)^{q-1}}{2^{t(+1)}}\ \frac{(r-1)!}{(r-1)^{r-1}}$$

as the number of maps ψ we may expect to satisfy our conditions. The reader easily checks that this espression tends to infinity with r.

(5.5) PROPOSITION. - Let r be an integer satisfying one of the following conditions :

(a) r is prime, and $r \equiv 1 \mod 8$;

(b) r is prime, and $r = x^2 + y^2 + 1$, for certain integers x, y, with $(x, y) = 1$;

(c) r is prime, and $2r - 1$ is prime ;

(d) $r = 3p$, where p, $2p - 1$ and $2r - 1$ are prime, and $p \geqslant 5$.

Further, let the Riemann hypotheses mentioned in (2.9) be satisfied. Then, there exist infinitely many perfect one-error-correcting cyclic AN-codes in base r, and the same is true for negacyclic codes.

Proof. - We define the group multiplication $*$ on V such that the following maps are group isomorphisms : In cases (a) and (b),

$$V \longrightarrow \underset{\sim}{F}_r^*\ ,\quad r \longmapsto (1 \mod r)\ ,\quad a \longmapsto (a \mod r)\quad (a \neq r)\ ;$$

in case (c),

$$V \longrightarrow \underset{\sim}{F}_{2r-1}^*/\{\pm 1\}\ ,$$

$$r \longmapsto \{\pm 1 \mod 2r - 1\}\ ,\quad a \longmapsto \{\pm a \mod 2r - 1\}\quad (a \neq r)\ ;$$

and in case (d)

$$V \longrightarrow \underset{\sim}{F}_{2r-1}^*/\{\pm 1\}\ ,$$

$$r \longmapsto \{\pm 1 \mod 2r - 1\}\ ,\quad p \longmapsto \{\pm 2p \mod 2r - 1\}\ ,$$

$$2p \longmapsto \{\pm (2p - 1) \mod 2r - 1\}\ ,\quad 2p - 1 \longmapsto \{\pm p \mod 2r - 1\}\ ,$$

$$a \longmapsto \{\pm a \mod 2r - 1\}\quad (a \neq r\ ,\ p\ ,\ 2p\ ,\ 2p - 1)\ .$$

Then $(V\ ,\ *)$ clearly satisfies (2.4), condition (2.5) is easily checked, and (2.6), (2.7) are proved by the quadratic reciprocity law. In case (b), notice that $r - 1$ has no divisors which are $3 \mod 4$. The proposition now follows from (2.9) and (4.2).

Examples.

(a) $r = 17 , 41 , 73 , 89 , 97$, and infinitely many others ;

(b) $r = 2 , 3 , 11 , 59 , 83 , 107$, and infinitely many others, cf. [7] ;

(c) $r = 2 , 3 , 7 , 19 , 31 , 37 , 79 , 97$, and probably infinitely many others;

(d) $r = 21 , 57 , 471 , 597 , 687 , 1137 , 1317 , 1731$, and probably infinitely many others.

Generators for perfect arithmetic codes in bases 2 and 3 are easily obtained from the tables of WESTERN and MILLER [13]. In table 1, one finds all primes $A < 10^5$ which generate a perfect one-error-correcting cyclic or negacyclic AN-code in base 6 or 7 , and all $A < 10^7$, for bases 11 and 12 . In each case, the word length n is given by $n = (A - 1)/(2r - 2)$. In table 2 , one finds, for all $r \leq 15$, not dealt with by (5.1), the densities (modulo the Riemann hypotheses) of the sets S , and S' defined in (2.9) and (4.2).

There are 9592 and 664579 primes less than 10^5 and 10^7 , respectively. The reader may decide for himself to which extent our results cast doubt on the validity of the Riemann hypotheses.

Table 1 : Generators for perfect codes.

r	cyclic	negacyclic
6	18191	7741
	20611	10831
	22391	11171
	25031	15161
	27791	22741
	37511	23431
	38011	23531
	40031	39971
	50231	42131
	50971	46381
	53591	46471
	56591	49261
	56951	56081
	59011	64451
	76871	65581
	82031	75641
	86491	79691
	91291	81371
		81401
		93251
7	19237	56053
	30013	67453
	73453	98893

.../...

r	cyclic	negacyclic
11	1513021 5652421 6169021 9227221	4723981 7556701
12	5187359 8936159	1588423 3079627 4911941 5847029

Table 2 : Densities of S and S' (modulo Riemann hypotheses)

r	d(S)	d(S')
2	1.8698×10^{-1}	3.7396×10^{-1}
3	3.7396×10^{-2}	3.7396×10^{-2}
6	1.5116×10^{-3}	3.0231×10^{-3}
7	3.1608×10^{-4}	3.1608×10^{-4}
11	6.1369×10^{-6}	6.1369×10^{-6}
12	5.5774×10^{-6}	9.2956×10^{-6}
14	3.8757×10^{-7}	7.7513×10^{-7}
15	2.7936×10^{-7}	4.0724×10^{-7}

Acknowledgement. - Research for this paper was supported by the Netherlands Organization for the Advancement of Pure Research (Z. W. O.).

REFERENCES

[1] BOJARINOV (J. M.) and KABATJANSKIJ (G. A.). - Perfect arithmetic AN-codes for correcting single errors [in Russian], Probl. Peredači Inform., t. 12, fasc. 1, 1976, p. 16-23; [in English] Problems of Inform. Transm., t. 12, 1976, p. 10-16.

[2] COOKE (G.) and WEINBERGER (P. J.). - On the construction of division chains in algebraic number rings, with applications to SL_2, Comm. in Algebra, t. 3, 1975, p. 481-524.

[3] GOTO (M.). - A note on perfect decimal AN-codes, Inform. and Control, t. 29, 1975, p. 385-387.

[4] GOTO (M.) and FUKUMURA (T.). - Perfect nonbinary AN-codes with distance three, Inform. and Control, t. 27, 1975, p. 336-348.

[5] GRICENKO (V. M.). - Nonbinary arithmetic correcting codes [in Russian], Probl. Peredači Inform., t. 5, fasc. 4, 1969, p. 19-27 ; [in English] Problems of Inform. Transm., t. 5, 1969, fasc. 4, p. 15-22.

[6] HOOLEY (C.). - On Artin's conjecture, J. für die reine und angew. Math., t. 225, 1967, p. 209-220.

[7] IWANIEC (H.). - Primes of the type $\varphi(x, y) + A$ where φ is a quadratic form, Acta Arithm., Warszawa, t. 21, 1972, p. 203-234.

[8] LENSTRA (H. W., Jr). - On Artin's conjecture and Euclid's algorithm in global fields, Invent. Math., Berlin, t. 42, 1977, p. 201-224 ; [cf. Artin's conjecture on primes with prescribed primitive roots, Séminaire Delange-Pisot-Poitou : Théorie des nombres, 18e année, 1976/77, n° 14, 8 p.].

[9] MASSEY (J. H.) and GARCIA (O. N.). - Error-correcting codes in computer arithmetic, Advances Inform. Syst. Sc., t. 4, 1972, p. 273-326.

[10] NARKIEWICZ (W.). - Elementary and analytic theory of algebraic numbers. - Warszawa, PWN-Polish scientific Publishers, 1974 (Polska Akademia Nauk. Monografie Matematyczne, 57).

[11] PETERSON (W. W.) and WELDON (E. Y., Jr). - Error-correcting codes, 2nd edition. - Cambridge, MIT Press, 1972.

[12] RAO (T. R. N.). - Error coding for arithmetic processors. - London, Academic Press, 1974 (Electrical Science Series).

[13] WESTERN (A. E.) and MILLER (J. C. P.). - Tables of indices and primitive roots. - London, Cambridge University Press, 1968 (Royal Society mathematical Tables, 9).

(Texte reçu le 12 juin 1978)

H. W. LENSTRA, Jr
15 Roetersstraat
1018 WB AMSTERDAM (Pays-Bas)