THREE-CYCLOTOMIC-COSETS IRREDUCIBLE CYCLIC CODES

YVES AUBRY AND PHILIPPE LANGEVIN

ABSTRACT. The paper is devoted to the study of the semiprimitivity of three-cyclotomic-cosets irreducible cyclic codes. We prove in a particular case, without assuming the Generalized Riemann Hypothesis, but with at most one exception, a conjecture of Schmidt and White on two-weight irreducible cyclic codes. Namely, we prove that if v is an integer such that there is three p-cyclotomic cosets modulo v then any irreducible cyclic code $c(p, m, v)$ with two non-zero Hamming weights which is not one of the six known sporadic examples is semiprimitive with at most one exception. The result is proved without any exception for three-cyclotomic-cosets index-two irreducible cyclic $c(p, m, v)$ codes with v prime not congru to 3 modulo 8.

1. INTRODUCTION

Irreducible cyclic codes are extensively studied in the litterature. They can be defined as a convenient way by three parameters p, m and v and denoted $c(p, m, v)$. Such codes with only few different weights are highly appreciated, especially those with exactly two (non-zero) Hamming weights (when we deal with the number of weights of a code, we always deal with the number of non-zero weights) which we will call two-weight codes (contrary to some authors who allow two-weight codes to have only one non-zero weight). The classification of two-weight irreducible cyclic codes is not yet available but it underwent recent progress. An infinite family, namely the semiprimitives codes (i.e. when -1 is a power of p modulo v), and eleven sporadic examples are known. Schmidt and White in [8] provided evidence to conjecture that, in a certain sense, this is the whole story:

Conjecture 1. *An irreducible cyclic code $c(p, m, v)$ is a two-weight code if and only if it is a semiprimitive code or it is one of the eleven sporadic known codes.*

They proved their conjecture, conditionally on the Generalized Riemann Hypothesis (G.R.H.), for index-two codes (i.e. when p has index 2 modulo v).

After to have considered in [1] the conjecture in the binary case and proved it in a particular case without assuming G.R.H., our main goal here is to prove this conjecture still without assuming G.R.H. for a larger class, namely the three-cyclotomic-cosets irreducible cyclic codes i.e. irreducible cyclic code $c(p, m, v)$ with three p-cyclotomic cosets modulo v.

More precisely, we introduce in section 2 the irreducible cyclic codes, denoted $c(p, m, v)$, by the way of the Trace function. This vision is very useful to estimate "à la McEliece" the weight of the codewords by means of linear combinations of Gauss sums.

We remark in section 3 that a $c(p, m, v)$ irreducible cyclic code has at most three non-zero weights if the ring $\mathbf{Z}/v\mathbf{Z}$ contains exactely three p-cyclotomic cosets. Thus, the class of irreducible cyclic codes $c(p, m, v)$ with three p-cyclotomic cosets modulo v is of particular interest for the study of two-weight irreducible cyclic codes.

Section 4 is attached to the cardinality of the class of index-two codes with v prime i.e. $c(p, m, v)$ irreducible cyclic codes with v prime and with the index of p modulo v equal to 2. We show that, conditionally on G.R.H., this last class of codes (which provide codes with at most two weights) is infinite using near-primitive root densities.

Section 5 is devoted to prove (inconditionally) the conjecture of Schmidt and White for index-two irreducible cyclic $c(p, m, v)$ codes with v prime not congru to 3 modulo 8. Indeed, consider a $c(p, m, v)$ irreducible cyclic code with three p-cyclotomic cosets modulo v. We show that either v is a square of a prime and p is a primitive root modulo v, either v is a prime and p has index 2 modulo v. Since the first case gives rise immediately to a semiprimitive code (-1 is trivially a power of p modulo v), we focus on the second case which itself is divided in two cases: where $v \equiv 1 \pmod 4$ or $v \equiv 3 \pmod 4$. Since -1 is a square modulo v in the first case, our study is reduced to $c(p, m, v)$ codes with the three following conditions:

(i) v is a prime greater than 3,
(ii) p has index 2 modulo v,
(iii) $v \equiv 3 \pmod 4$.

In particular, while involving the class number of the number field $\mathbf{Q}(\sqrt{-v})$, we prove that, if a $c(p, m, v)$-code with the previous three conditions has two non-zero weights, then the parameter $s = m/\operatorname{ord}_v(p)$ appearing in [8] and in [4] is equal to 1, i.e. $m = \operatorname{ord}_v(p)$.

Then, we show that there does not exit two-weight binary such codes which implies that any two-weight binary irreducible cyclic code with three cyclotomic cosets is semiprimitive.

Finally, using a result of Tatuzawa on the class number of imaginary quadratic number fields, we determine all the two-weight irreducible cyclic code satisfying the previous three conditions with at most one exception, which enable us to prove Conjecture 1 in the case where v is an integer such that there is three p-cyclotomic cosets modulo v. This case contains in particular the "index-two" case with v prime ;

the "index-two" case is the one proved by Schmidt and White under G.R.H..

2. Irreducible cyclic codes and McEliece weight-formula

Let us introduce irreducible cyclic codes over a prime finite field. Indeed, it is enough for the purpose here, namely the classification of two-weight irreducible cyclic codes, to consider irreducible cyclic codes defined over a prime field, as remarked in [8].

Let p be a prime number and consider the finite field K with p elements. Let L be the extension of degree m of K and consider a divisor n of $p^m - 1$ and write $v = \frac{p^m-1}{n}$ (thus v and p are coprime). Let ζ be a primitive n-th root of unity in L (i.e. ζ is a generator of the cyclic subgroup of order n of the multiplicative group L^*). Consider the following map Φ_m:

$$\begin{array}{cccc} \Phi_m : & L & \longrightarrow & K^n \\ & t & \longmapsto & \big(\mathrm{Tr}_{L/K}(t\zeta^{-i})\big)_{i=0}^{n-1} \end{array}$$

where $\mathrm{Tr}_{L/K}$ is the trace of the field L over K.

Definition 2. *We define the $c(p,m,v)$ code to be the image of the map Φ_m.*

It is a code of length n and dimension equals to $\mathrm{ord}_n(p)$, the multiplicative order of p modulo n. It is trivially a cyclic code (i.e. invariant under the cyclic shift) and it is irreducible in the sense that it has no proper subspace which is cyclic. Every irreducible cyclic code over K in the classical definition, i.e. cyclic code generated by a polynomial $(X^n-1)/P(X)$ with $P(X)$ an irreducible divisor of $X^n - 1$ over K, can be viewed as a $c(p,m,v)$ code (see [8]). So, we can take $c(p,m,v)$ as the definition of irreducible cyclic codes over K of length n. The $c(p,m,v)$ codes are known to be projective or saturated according to whether $(n, p-1) = 1$ or $(n, p-1) = p-1$.

Now we are interested in the weight $w(t)$ of a codeword $\Phi_m(t)$ of such a code, for $t \in L^*$. Let χ be a character of the multiplicative group L^* and let $\tau_L(\chi)$ be the Gauss sum associated to χ:

$$\tau_L(\chi) = -\sum_{x\in L^*} \chi(x) e^{\frac{2i\pi}{p}\mathrm{Tr}_{L/K}(x)}. \tag{1}$$

Let V be the subgroup of L^* of index v and let Γ be the subgroup of characters of L^* which are trivial both on V and K^*. Note that the order of Γ is equal to $v(n,p-1)/(p-1)$. We have the well-known following McEliece formula:

Proposition 3. *For any $t \in L^*$, the weight $w(t)$ of the codeword $\Phi_m(t)$ is given by:*

$$w(t) = \frac{p-1}{pv}\big(p^m + \sum_{\chi \in \Gamma \setminus \{1\}} \tau_L(\chi)\bar{\chi}(t)\big). \tag{2}$$

And, conversely by Fourier inversion

$$\tau_L(\chi) = \frac{p}{p-1} \sum_{t \in L^*/V} w(t)\chi(t). \tag{3}$$

One says that p is semiprimitive modulo v when -1 is in the group generated by p in $(\mathbf{Z}/v\mathbf{Z})^*$. Note that, in this case, all the Gauss sums are rationals and the $c(p, m, v)$ code is a two-weight code. We investigate in the rest of the paper the reciprocal: besides some examples, any two-weight irreducible cyclic code is semiprimitive ?

Let us say a few words in the case of v is small. It is wellknown that a $c(p, m, 2)$ is a two-weight code, the weights can be expressed in term of quadratic Gauss sum, see [6]. In the same way, the weights of a $c(p, m, 3)$ can be expressed by means of cubic Gauss sums. However, it is an hard question to give the exact values of the cubic Gauss sums [5], thus the weights a such code . Nevertheless , we have the following characterization

Proposition 4. *The $c(p, m, 3)$-code has two weights if and only if p is semiprimitive modulo 3 that is $p \equiv 2 \mod 3$.*

Proof. Let χ be a multiplicative character of L of order 3. The number of weights is equal to the number of distincts values taken by the mapping: $L^* \ni t \mapsto f(t) = \tau(\chi)\chi(t) + \tau(\bar{\chi})\bar{\chi}(t)$.

Let $1 \neq j$ be a cubic root of unity. Let t be such that $\chi(t) = j$. The collision $f(1) = f(t)$ implies $\tau(\bar{\chi}) = j\tau(\chi)$, the equality $f(t) = f(t^2)$ implies $\tau(\bar{\chi}) = \tau(\chi)$ and $f(1) = f(t^2)$ implies $\tau(\bar{\chi}) = j^2\tau(\chi)$. To resume, the code is a two-weights code if and only if there exists a cubic root of the unity w such that

$$\tau(\bar{\chi}) = w\tau(\chi) \tag{4}$$

In particular, since $\tau(\chi)^3$ is an algebraic number of degree two whose the norm is equal to p^{3m}, we deduce that $\tau(\chi)^6 = \tau(\bar{\chi})^6 = p^{6m}$. Using the terminology of the litterature, these Gauss sums are pure. It follows from [6] that p is semiprimitive modulo 3. $\square$

3. Cyclotomic cosets

Let p be a prime. For any integer v prime to p, consider on the ring $\mathbf{Z}/v\mathbf{Z}$ the equivalence relation given by: for $a, b \in \mathbf{Z}/v\mathbf{Z}$, we set $a \sim b$ if and only if there exists $t \in \mathbf{Z}$ such that $a = bp^t$. The equivalence classes for this equivalence relation are the so-called p-cyclotomic cosets modulo v.

Recall that the order $\mathrm{ord}_v(g)$ of an element g of the multiplicative group $(\mathbf{Z}/v\mathbf{Z})^*$ divides the order $\varphi(v)$ of this group, where φ is the Euler function. We denote by $\mathrm{ind}_v(g)$ the index of g modulo v i.e.

$$\mathrm{ind}_v(g) = \frac{\varphi(g)}{\mathrm{ord}_v(g)}.$$

We have of course $\mathrm{ind}_v(g) = [(\mathbf{Z}/v\mathbf{Z})^* :< g >]$ where $< g >$ denote the subgroup of $(\mathbf{Z}/v\mathbf{Z})^*$ generated by g. It is well-known that the number $\gamma(p, v)$ of p-cyclotomic cosets modulo v is exactly the number of irreducibles polynomials in the decomposition of the polynomial $X^v - 1$ over $\mathbf{F}_p$, thus it is equal to

$$\gamma(p, v) = \sum_{d|v} \frac{\varphi(d)}{\mathrm{ord}_d(p)} = \sum_{d|v} \mathrm{ind}_d(p) \tag{5}$$

(with the convention that $\mathrm{ind}_1(p) = 1$). For example, the condition $\gamma(p, v) = 2$ is equivalent to $\mathrm{ind}_v(p) = 1$ i.e. p is a primitive root modulo v. What about the case of three cyclotomic cosets ?

Proposition 5. *Let v be an integer. The ring $\mathbf{Z}/v\mathbf{Z}$ contains exactly three p-cyclotomic cosets if and only if:*

(i) *v is a prime and p has index 2 mod v*
or
(ii) *v is the square of a prime and p has index 1 mod v.*

Proof. By the relation (5) we have $\gamma(p, v) = 3$ if and only if $\mathrm{ind}_v(p) = 2$ and v has no proper divisor, or $\mathrm{ind}_v(p) = 1$ and v has a unique proper divisor. The proposition is then proved. □

Proposition 6. *Let v be an integer. If the ring $\mathbf{Z}/v\mathbf{Z}$ contains exactly three p-cyclotomic cosets then any $c(p, m, v)$ code has at most three non-zero weights.*

Proof. The result is in fact much general: the number of weights is less or equal than the number of cyclotomic cosets. It follows from the fact that the weight of a codeword of a $c(p, m, v)$ code is invariant under $t \mapsto t\zeta$ and under $t \mapsto t^p$ (see also theorem 2.5 of [2] for a detailed proof). □

The case (*ii*) of proposition 5 falls into the semiprimitive case since p generates the whole group $(\mathbf{Z}/v\mathbf{Z})^*$ and thus contains -1. The case (*i*) is then the remainder case to be studied: it is the topic of the next section.

4. Index-two irreducible cyclic codes

For the study of $c(p,m,v)$ codes with v prime and p of index two modulo v, we are interested in primitive and near-primitive root densities.

In 1927, Emil Artin made the following conjecture (called now the Artin's primitive root conjecture): for any integer α, not equal to ± 1 or a square, the natural density

$$\lim_{x\to+\infty} \frac{\sharp\{v \text{ prime} \mid v \le x \text{ and } <\alpha>= \mathbf{F}_v^*\}}{\sharp\{v \text{ prime} \mid v \le x\}}$$

of the set of primes v for which α is a primitive root modulo v inside the set of all prime numbers exists and is positive. In 1967, Hooley proved this conjecture if G.R.H. holds true. In particular, he proved that if α is neither ± 1 nor a perfect square, then there are infinitely many primes v for which α is a primitive root modulo v.

If we ask α to generate only the squares of $\mathbf{F}_v^*$ and not the whole group $\mathbf{F}_v^*$, i.e. to have index 2 and not index 1 modulo v, we touch the notion of near-primitive roots. Precisely, we fix α not equal to ± 1 or a perfect power and let v be a prime and t be an integer such that $v \equiv 1 \pmod{t}$. Consider

$$N_{\alpha,t}(x) = \sharp\{v \text{ prime} \mid v \le x \text{ and } v \not| \alpha \text{ and } \operatorname{ind}_v(\alpha) = t\}.$$

Notice that for $t = 1$, α is wanted to be a primitive root modulo v and thus this quantity is just the previous one studied by Artin and Hooley. In 2000, Moree introduced in [7] a weighting function depending on α and t and gave an estimation of $N_{\alpha,t}(x)$ assuming G.R.H.. In particular, for $\alpha = p$ a prime number and $t = 2$, he proved that

$$N_{p,2}(x) = \sum_{\substack{v \text{ oddprime} \\ v \le x}} \frac{\varphi(\frac{v-1}{2})}{v-1} + O(\frac{x \log\log x}{\log^2 x}).$$

This implies that there exists infinitely many primes v such that p has index 2 modulo v.

In particular, we have:

Proposition 7. *Conditionally on G.R.H., there are infinitely many index-two irreducible cyclic codes $c(p,m,v)$ with v prime.*

5. Index-two $c(p,m,v)$ codes with v prime

The irreducible cyclic codes $c(p,m,v)$ with v a prime number and with p of index 2 modulo v range in two families: the first one with $v \equiv 1 \pmod 4$ and the second one with $v \equiv 3 \pmod 4$. But if $v \equiv 1 \pmod 4$ then -1 is a square modulo v and since p generates the squares modulo v, we come to the semiprimitive case. This lead us to consider the second case, where -1 is not a square modulo v.

Hence, let us consider a prime number p and an integer v satisfying the following ($\sharp$)-conditions:

(a) v is a prime greater than 3,
(b) $\mathrm{ord}_v(p) = \frac{v-1}{2}$ i.e. p has index 2 modulo v,
(c) $v \equiv 3 \pmod 4$.

Definition 8. *An irreducible cyclic $c(p, m, v)$ code with v satisfying the ($\sharp$)-conditions is called a $(\sharp) - c(p, m, v)$ code.*

Let f be the multiplicative order of p modulo v. Note that f divides m, we denote by s the quotient $s = m/f$. Under theses conditions, the Gauss sums of order v, the class number h of the imaginary quadratic number field $\mathbf{Q}(\sqrt{-v})$ and the sum of the p-digits of n are deeply connected (see [4]) :

$$h = t' - t, \qquad t = \frac{1}{p-1} s_p(n), \quad t' = \frac{1}{p-1} s_p(n(v-1)), \tag{6}$$

where $s_p(x)$ denotes the sum of the p-ary digit of the integer x. Let χ be a multiplicative character of L^* of order v. Up to complex conjugacy, the value of the Gauss sum corresponding to χ is then given by:

$$\tau_L(\chi) = p^{ts}(a + b\kappa)^s \tag{7}$$

where $\kappa^2 + \kappa + \frac{v+1}{4} = 0$, and where the point (a, b) is the only integer point on the ellipse defined by the equation

$$p^h = a^2 - ab + b^2 \frac{v+1}{4}, \tag{8}$$

satisfying the conditions

$$2a - b \equiv p^{t'} \pmod v, \quad (p, b) = 1, \quad b < 0. \tag{9}$$

The ($\sharp$) conditions on v give rise to the following powerfull identity:

Proposition 9. *If a $c(p, m, v)$ code with v satisfying the ($\sharp$) conditions has two weights then:*

$$\frac{v+1}{4} = p^{hs}. \tag{10}$$

Proof. We adapt the proof given in [4]. Let w_0, w_1 and w_2 be the weights of $\Phi(1)$, $\Phi(\beta)$, and $\Phi(\beta^{-1})$. By (3), we have:

$$\tau_L(\chi) = \frac{p}{p-1}(w_0 + w_1\kappa + w_2\bar{\kappa}) = \frac{p}{p-1}\big((w_0 - w_2) + (w_1 - w_2)\kappa\big). \tag{11}$$

Since the Gauss sum is not rationnal, we get $w_2 \neq w_3$. It follows that $\tau_L(\chi)$ is an integer multiple of κ or $\bar{\kappa}$. Let a_s and b_s be the rationnal integers such that $\tau_L(\chi) = p^{hs}(a_s + b_s\kappa)$. If it is a multiple of κ then $a_s = 0$. If it is a multiple of $\bar{\kappa}$ then $a_s = b_s$. In both case, we conclude by $b_s^2 \frac{v+1}{4} = p^{hs}$, the proposition follows since $(a_s + b_s\kappa) \notin (p)$. $\square$

Theorem 10. *If a $c(p,m,v)$ code with v satisfying the $(\sharp)$ conditions is a two-weight code then we have:*

$$m = \mathrm{ord}_v(p).$$

Proof. Since p has index 2 modulo v then p is a square modulo v, which implies that the ideal (p) splits in the extension $\mathbf{Q}(\sqrt{-v})/\mathbf{Q}$:

$$(p) = PP'.$$

We have that the norm $N_{\mathbf{Q}(\sqrt{-v})/\mathbf{Q}}(P) = p$ and that P^h is a principal ideal (since h is the ideal class number of $\mathbf{Q}(\sqrt{-v})$): $P^h = (\alpha)$ with $\alpha = \frac{a+b\sqrt{-v}}{2}$ $(a, b \in \mathbf{Z})$ an algebraic integer of $\mathbf{Q}(\sqrt{-v})$. Calculating the norms, we find $p^h = \frac{a2+vb2}{4}$ and since a and b can't be zero in this situation, we conclude that

$$\frac{v+1}{4} \leq p^h.$$

But by (10) a $(\sharp) - c(p,m,v)$ code has two weights if and only if

$$\frac{v+1}{4} = p^{hs}. \tag{12}$$

Thus, $p^{hs} \leq p^h$ and we conclude that necessarily $s = 1$. $\square$

Then, the parameter s defined previously and appearing in [8] and [4] is equal to 1 under the $(\sharp)$ conditions. In particular, we have the following corollary:

Corollary 11. *If a $c(p,m,v)$ code with v satisfying the $(\sharp)$ conditions is a two-weight code then*

$$\frac{v+1}{4} = p^h. \tag{13}$$

where h is the class number of the imaginary quadratic number field $\mathbf{Q}(\sqrt{-v})$. In particular, such a code is completely defined by the parameter v: the cardinal of the prime field on which the code is defined is $\log_h(\frac{v+1}{4})$ and the degree of the extension L is $\frac{v-1}{2}$.

Furthermore, we have the following necessary condition on p for two-weight $c(p,m,v)$ code with v satisfying the $(\sharp)$ conditions:

Corollary 12. *If a $c(p,m,v)$ code with v satisfying the $(\sharp)$ conditions has two weights then p is the least prime which totally splits in the extension $\mathbf{Q}(\sqrt{-v})/\mathbf{Q}$ i.e. p is the least prime which is a square modulo v.*

Proof. Indeed, if π is a prime which totaly splits in $\mathbf{Q}(\sqrt{-v})/\mathbf{Q}$, then the previous proof implies that $\pi^h \geq \frac{v+1}{4} = p^h$ which gives $\pi \geq p$. $\square$

5.1. **The binary case.** We showed in [1] the following proposition (we include here the short proof for the convenience of the reader):

Proposition 13. *There does not exist two-weight binary $c(p,m,v)$ code with v satisfying the ($\sharp$) conditions.*

Proof. The relation (13) implies that:

$$4p^h \equiv 1 \pmod{v}.$$

If $p=2$, we have that p^{h+2} is 1 modulo v, which implies that the order of p modulo v divides $h+2$. But, by hypothesis, we have $\mathrm{ord}_v(p) = (v-1)/2$. Then, taking the logarithm in (13), we have the inequalities:

$$\frac{v-1}{2} \leq h+2 = \log_p\left(\frac{v+1}{4}\right)+2. \tag{14}$$

We obtain that the only possible value for v is $v=7$ which gives a code with one non-zero weight, which implies already the desired result. □

Hence, this case produces only three-weight codes.

Remark 14. *The number of weights here is maximal with respect to the number of cyclotomic cosets.*

Finally, we have proved the following result:

Theorem 15. *If a binary irreducible cyclic code with three-cyclotomic cosets has two weights then it is semiprimitive.*

Proof. By proposition (5), an irreducible cyclic code with three-cyclotomic cosets leads to two cases. The first one leads $c(p,m,v)$ codes with v a square of a prime and p of index 1 modulo v which gives a semiprimitive code.

The other case leads to $c(p,m,v)$ codes with v a prime and p of index 2 modulo v (the so-called index-two codes). When $v \equiv 1 \pmod 4$, we saw that we obtain a semiprimitive code. When $v \equiv 3 \pmod 4$, we obtain $c(p,m,v)$ codes with v satisfying the ($\sharp$) conditions. In the case where $p=2$, i.e. the binary case, we just found that there is no two-weight codes. □

Our last alternative to find two-weight codes is among the non-binary $c(p,m,v)$ codes with v satisfying the ($\sharp$) conditions and we know that we will found examples of such codes in this last case. The study of this remainder case is the purpose of the next subsection.

5.2. **The non-binary case.** The case where 2 is a square i.e. when $v \equiv 7 \pmod 8$ is easy:

Theorem 16. *There does not exist two-weight $c(p,m,v)$ code with v satisfying the ($\sharp$) conditions and with $v \equiv 7 \pmod 8$.*

Proof. The condition $v \equiv 7 \pmod 8$ tell us that 2 is a square modulo v, which implies that the ideal (2) splits in the extension $\mathbf{Q}(\sqrt{-v})/\mathbf{Q}$. By corollary (12), we conclude that $p = 2$ and the result of the previous subsection gives the result. □

The remainder case is then when $v \equiv 3 \pmod 8$. Actually, we will consider now a more general approach using the identity of Corollary (11) but with perhaps an exception.

5.3. **The result with at most one exception.** We have shown in Corollary (11) that if a $c(p, m, v)$ code with v satisfying the ($\sharp$) conditions has two weights then we have the following relation

$$\frac{v+1}{4} = p^h$$

where h is the class number of the imaginary quadratic number field $\mathbf{Q}(\sqrt{-v})$.

In 1935, Siegel proved a non-effective lower bound on the residue at $s = 1$ of the L-function $L(s, \chi_v)$ associated to the primitive odd Dirichlet character χ_v of $\mathbf{Q}(\sqrt{-v})$. Tatuzawa, in 1951, proved an effective lower bound of $L(1, \chi_v)$ but with at most one exception (see [9]): if $0 < \varepsilon < 1/2$ and $v \geq \max(e^{1/\varepsilon}, e^{11.2})$, then

$$L(1, \chi_v) \geq 0.655\varepsilon v^{-\varepsilon}.$$

Since the class number h of $\mathbf{Q}(\sqrt{-v})$ with $-v \equiv 1 \pmod 4$ is linked to $L(1, \chi_v)$ by the following Dirichlet class number formula:

$$L(1, \chi_v) = \frac{\pi h}{\sqrt{v}},$$

we can use Tatuzawa theorem to get an upper bound on v.

Theorem 17. *There does not exist, with at most one exception, two-weight $c(p, m, v)$ code with v satisfying the ($\sharp$) conditions for $v \geq 10^8$.*

Proof. Let $\varepsilon = 1/\log(10^8)$. We have $0 < \varepsilon < 1/2$ and for $v \geq \max(e^{1/\varepsilon}, e^{11.2}) = 10^8$, we have, with at most one exception:

$$L(1, \chi_v) \geq 0.655\varepsilon v^{-\varepsilon} = 0.035 v^{-0.054}.$$

Now, we can write: $\frac{v+1}{4} = p^h \geq 2^h$ which implies that $\log \frac{v+1}{4} \geq h \log 2$. By the Dirichlet class number formula, we get:

$$\log \frac{v+1}{4} \geq \frac{\sqrt{v} L(1, \chi_v)}{\pi} \log 2.$$

But, for $v \geq 10^8$, we have on one hand $\log \frac{v+1}{4} \geq 17.03$ and on the other hand $\frac{\sqrt{v} L(1,\chi_v)}{\pi} \log 2 > 28.55$ by Tatuzawa theorem. Thus, there does not exist $v \geq 10^8$ such that $\frac{v+1}{4} = p^h$, with at most one exception. □

TABLE 1. Sporadic $c(p, m, v)$ codes with v satisfying the ($\sharp$) conditions and $v \leq 10^8$.

v	11	19	67	107	163	499
p	3	5	17	3	41	5
h	1	1	1	3	1	3

We have just, now, to make an exhaustive research of primes $v \leq 10^8$ such that $\frac{v+1}{4}$ is a power of a prime p. Then, for such primes v, we have just to check that the identity $\frac{v+1}{4} = p^{h_v}$ holds or not. Actually, we recover the following sporadic known examples of table 1.

Thus, we have proved the following theorem:

Theorem 18. *If v is an integer such that there is three p-cyclotomic cosets modulo v then any two-weight irreducible cyclic code $c(p, m, v)$ which is not one of the six sporadic examples is semiprimitive with at most one exception.*

In particular, we have shown that:

Corollary 19. *Conjecture 1 is true, with at most one exception, for all index-two $c(p, m, v)$ codes with v prime.*

References

[1] Y. Aubry and P. Langevin, On the weights of binary irreducible cyclic codes, *WCC'2005, Bergen, Norway,* P. Charpin and O. Ytrehus, Editors, to appear in Springer Lecture Notes on Computer Science series.

[2] R. W. Fitzgerald and J. L. Yucas, Sums of Gauss sums and weights of irreducible codes, *Finite field and their applications*, 11 (2005) 89-110.

[3] R. Calderbank, W. M. Kantor The geometry of two-weight codes. Technical report, Bell Laboratory, 1978.

[4] Ph. Langevin, A new class of two weight codes, *Finite field and their applications, Glasgow 1995, London Math. Soc.* Lecture Note Ser. 233, 181-187 (1996).

[5] C. R. Matthews Gauss sums and elliptic functions I. The Kummer sums, *Invent. Math.*, 52 (1979), 163-185.

[6] B. C. Berndt, R. J. Evans and K. S. Williams Gauss and Jacobi Sums, Wiley-Interscience, N. Y., 1998.

[7] P. Moree, Asymptotically exact heuristics for (near) primitive roots, *J. Number Theory* **83** (2000),no. 1, 155-181.

[8] B. Schmidt and C. White, All two-weight irreducible cyclic codes ?, *Finite Fields and Their Applications* **8** (2002), 1-17.

[9] T. Tatuzawa, On a theorem of Siegel, *Jap. J. Math.* **21** (1951), 163-178 (1952).

G.R.I.M., UNIVERSITÉ DU SUD TOULON-VAR, FRANCE.
E-mail address: {yaubry, langevin}@univ-tln.fr