Glasgow Math. J. **60** (2018) 97–110. © Glasgow Mathematical Journal Trust 2017.
doi:10.1017/S0017089516000586.

AN EFFECTIVE BOUND FOR THE CYCLOTOMIC LOXTON–KEDLAYA RANK

CONSTANTIN N. BELI and FLORIN STAN

Simion Stoilow Institute of Mathematics of the Romanian Academy, Research unit 5, P. O. Box 1-764, RO-014700 Bucharest, Romania
e-mails: raspopitu1@yahoo.com, Beli.Constantin@imar.ro, sfloringabriel@yahoo.com

and ALEXANDRU ZAHARESCU

Simion Stoilow Institute of Mathematics of the Romanian Academy, Research unit 5, P. O. Box 1-764, RO-014700 Bucharest, Romania
Department of Mathematics, University of Illinois at Urbana-Champaign, Altgeld Hall, 1409 W. Green Street, Urbana, IL, 61801, USA
e-mail: zaharesc@math.uiuc.edu

(Received 7 October 2015; revised 10 July 2016; accepted 20 October 2016; first published online 20 March 2017)

Abstract. In this paper, we provide an explicit upper bound for the Loxton–Kedlaya rank of the maximal abelian extension of $\mathbb{Q}$.

2000 *Mathematics Subject Classification.* 11R18, 11R06.

1. Introduction. Let $\mathbb{Q}$ and $\mathbb{C}$ be the fields of rational and complex numbers, respectively, let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ and let $\mathbb{Q}^{ab}$ be the maximal abelian extension of $\mathbb{Q}$. Fix a positive integer m. An m-Weil number is an algebraic integer α such that $|\sigma(\alpha)|^2 = m$, for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. A classical theorem of Kronecker [**3**] shows that the 1-Weil numbers are the roots of unity. Weil numbers appear in a variety of contexts. For example, Weil numbers arise in the study of abelian varieties, in Honda–Tate theory (see [**2**], [**6**] and [**10**]) and in the representation theory of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the absolute Galois group of $\mathbb{Q}$ (see [**1**]). Further examples of Weil numbers include the eigenvalues of $\rho(\mathrm{Frob}_l)$, where ρ is a geometric representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and l is a prime at which ρ is unramified (see [**1**]).

While, as seen above, Weil numbers appear in various contexts, there is also much interest in the study of cyclotomic Weil numbers in particular. For instance, Gauss and Jacobi sums are cyclotomic, as are examples coming from character tables of finite groups. In [**5**], Loxton proved that modulo multiplication by roots of unity, there are only finitely many cyclotomic m-Weil numbers. Moreover, Lemma 7 of [**5**] gives an effective method for finding them all. Another approach, describing the same phenomenon, was provided more recently in an unpublished manuscript by Kedlaya. In [**9**], this result is extended to all finite extensions of $\mathbb{Q}^{ab}$.

For any positive integer m, we let H_m denote the set of elements x of the form $x = x_1^{e_1} x_2^{e_2} \dots x_n^{e_n}$, where $n \in \mathbb{N}$, $x_1, \dots, x_n$ are m-Weil numbers in $\mathbb{Q}^{ab}$, and the exponents $e_1, \dots, e_n$ are integers and satisfy $e_1 + \dots + e_n = 0$. Then, H_m is a multiplicative subgroup of $(\mathbb{Q}^{ab})^\times$, and μ_∞, the group of all roots of unity in $\mathbb{Q}^{ab}$, is a subgroup of H_m. From Loxton's work it follows that the quotient group H_m/μ_∞ is free of finite rank. This finite rank is called the Loxton–Kedlaya rank in [**9**], and we

denote it by r_m. This rank is also defined in general, for any finite extension of $\mathbb{Q}^{ab}$ and the techniques of [**9**] are used to prove the following theorem.

THEOREM 1. *For any positive integer m, the cyclotomic Loxton–Kedlaya rank r_m satisfies the following inequality (here, $\pi(x)$ denotes the number of primes less than or equal to x).*

$$r_m < \sum_{d=1}^{13^{6^m}} \prod_{k=1}^{d} \left[2^{1+k\pi(4m^2+2m-2)} ((2m)!)^k \binom{d}{k} + 1 \right].$$

Our approach is inspired by the work of Kedlaya, to which we add two new key ingredients. One of them is a certain norm defined on the set of algebraic numbers. Its square, which we denote by $A(\cdot)$, was used in recent investigations on the classical trace problem of Siegel ([**8**]). The other key tool in our approach is an effective, quantitative p-adic lemma which enables us to obtain bounds for the p-adic valuation of the degrees of m-Weil numbers. The link with [**9**] is in the methods, not in the main result, as the present paper concerns only the case of $\mathbb{Q}^{ab}$.

2. Preliminary results. For any positive integer q, we let ζ_q denote a primitive qth root of unity. For any algebraic number field F, we denote by O_F its ring of integers.

We consider the map $A : \overline{\mathbb{Q}} \longrightarrow [0, \infty)$ given by

$$A(\alpha) = \frac{1}{[F : \mathbb{Q}]} \sum_{\sigma} |\sigma(\alpha)|^2,$$

where F is a number field containing α and σ runs over all the embeddings of F into $\mathbb{C}$. Here, $A(\alpha)$ depends only on α and not on the field F containing α.

Clearly, for any non-zero algebraic integer α, if we denote by n its degree over $\mathbb{Q}$, and by $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ its conjugates over $\mathbb{Q}$, we have

$$A(\alpha) = \frac{|\alpha_1|^2 + \cdots + |\alpha_n|^2}{n} \geq \left(\frac{|\alpha_1| + \cdots + |\alpha_n|}{n} \right)^2 \geq \left(|\alpha_1| \ldots |\alpha_n| \right)^{\frac{2}{n}} \geq 1.$$

Since any cyclotomic integer $\alpha \in O_{\mathbb{Q}^{ab}}$ is a sum of roots of unity, we can define the length $l(\alpha)$ of α to be the smallest number $l \geq 0$ such that α can be written as a sum of l roots of unity.

Next, we collect several lemmas which will be used in the subsequent sections. We begin by recalling the following standard result.

LEMMA 1. *Let $N \in \mathbb{N} \setminus \{0\}$ and p a prime number. For any $\alpha \in \mathbb{Q}(\zeta_{pN})$, let $\alpha_0, \ldots, \alpha_{p-1} \in \mathbb{Q}(\zeta_N)$ such that $\alpha = \sum_0^{p-1} \alpha_i \zeta_p^i$.*

(1) *If $p \nmid N$, then $(p-1)A(\alpha) = \sum_{0 \leq i < j \leq p-1} A(\alpha_i - \alpha_j)$.*

(2) *If $p \mid N$, then $A(\alpha) = \sum_{j=0}^{p-1} A(\alpha_j)$.*

LEMMA 2. *Let $p_1, p_2, \ldots, p_n$ be distinct primes. Then, $A(\alpha) \geq \frac{l(\alpha)}{2^n}$, for any $\alpha \in O_{\mathbb{Q}(\zeta_{p_1 p_2 \ldots p_n})}$.*

Proof. This inequality is proved in [**4**, **Lemma** 9]. □

https://doi.org/10.1017/S0017089516000586 Published online by Cambridge University Press

LEMMA 3. *Let $q \geq 2$ be an integer, let p be a prime such that $p^r || q$, where $r \geq 2$, and let $\zeta = \zeta_{p^r}$. Then, the set $\{1, \zeta, \ldots, \zeta^{p^d-1}\}$ is an integral basis of $\mathbb{Q}(\zeta_q)$ over $\mathbb{Q}(\zeta_{\frac{q}{p^d}})$, for any $1 \leq d \leq r-1$. Moreover, for any $\alpha \in \mathbb{Q}(\zeta_q)$,*

$$\alpha = \sum_{j=0}^{p^d-1} \alpha_j \zeta^j,$$

with $\alpha_j \in \mathbb{Q}(\zeta_{\frac{q}{p^d}})$, one has

$$A(\alpha) = \sum_{j=0}^{p^d-1} A(\alpha_j).$$

Proof. This follows by successively applying Lemma 1 and using the fact that ζ^{p^d} is a primitive root of unity of order p^{r-d}, for any $1 \leq d \leq r-1$. □

LEMMA 4. *Let $k \geq 4$ be an integer, p a prime larger than $6^{\frac{k}{2}}$, and $a_1, a_2, \ldots, a_k$ distinct elements of $\mathbb{Z}/p\mathbb{Z}$. Then, at least one of the differences $a_i - a_j$ $(1 \leq i \neq j \leq k)$ occurs only once.*

Proof. This is Lemma 16 in [**9**]. □

3. Representations as sums of roots of unity. For any algebraic number α, we denote by $\deg(\alpha)$ the degree of α over $\mathbb{Q}$. We will need the following result on the number of cyclotomic integers of bounded degree and length.

LEMMA 5. *Let $D, M \geq 2$ be integers, and let*

$$n(D, M) = \#\{\alpha \in O_{\mathbb{Q}^{ab}} : \deg(\alpha) \leq D, l(\alpha) \leq M\}.$$

Then,

$$n(D, M) < D \sum_{d=1}^{D} \prod_{k=1}^{d} \left[2\binom{d}{k} M^k + 1\right].$$

Proof. Note that $l(\sigma(\alpha)) = l(\alpha)$, for any $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ and any cyclotomic integer $\alpha \in O_{\mathbb{Q}^{ab}}$.

Next, let α be a cyclotomic integer with $\deg(\alpha) \leq D$ and $l(\alpha) \leq M$. Then $|\alpha| \leq M$, and $l(\alpha') \leq M$, for any conjugate α' of α over $\mathbb{Q}$. Let $d = \deg(\alpha)$, let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$ be the conjugates of α over $\mathbb{Q}$, and let $f = X^d + a_1 X^{d-1} + \cdots + a_{d-1} X + a_d$, where $a_1, a_2, \ldots, a_d \in \mathbb{Z}$, be the minimal polynomial of α over $\mathbb{Q}$. Employing Viète's relations, we obtain

$$|a_k| = |(-1)^k \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq d} \alpha_{i_1} \alpha_{i_2} \ldots \alpha_{i_k}| \leq \binom{d}{k} M^k,$$

for any $1 \leq k \leq d$. Hence, there are at most $2\binom{d}{k} M^k + 1$ possibilities for the integer a_k.

https://doi.org/10.1017/S0017089516000586 Published online by Cambridge University Press

It follows that there are at most $\prod_{k=1}^{d}[2\binom{d}{k}M^k+1]$ such polynomials of degree d, which have at most $d\prod_{k=1}^{d}[2\binom{d}{k}M^k+1]$ roots.

Hence,

$$n(D,M) < \sum_{d=1}^{D} d\prod_{k=1}^{d}\left[2\binom{d}{k}M^k+1\right] < D\sum_{d=1}^{D}\prod_{k=1}^{d}\left[2\binom{d}{k}M^k+1\right].$$

□

LEMMA 6. *For any positive integer $n \geq 1$, there is an integer k_n such that any $\alpha \in O_{\mathbb{Q}^{ab}}$ with $A(\alpha) \leq \frac{n}{2}$ has $l(\alpha) \leq k_n$. One can take $k_n = n!2^{\pi(n^2+n-2)}$.*

Proof. We prove the above statement by induction on $n \geq 1$. For $n = 1$, or $n = 2$, we can take $k_1 = k_2 = 1$. Indeed, we have seen in Section 2 that $A(\alpha) \geq 1$, for any non-zero algebraic integer α. Thus, $A(\alpha) \leq \frac{1}{2}$ implies $\alpha = 0$, so we can take $k_1 = 1$. Similarly, $A(\alpha) \leq 1$ implies that α is 0 or a root of unity, which shows that we can take $k_2 = 1$ as well.

Assume that for any $1 \leq t \leq n$, there exists a $k_t \geq 1$ such that any $\alpha \in O_{\mathbb{Q}^{ab}}$ with $A(\alpha) \leq \frac{t}{2}$ has $l(\alpha) \leq k_t$.

Let $\alpha \in O_{\mathbb{Q}^{ab}}$ such that $A(\alpha) \leq \frac{n+1}{2}$. Let $\beta \in \{\alpha\eta : \eta \text{ root of unity}\}$ of minimal conductor q, in the sense that $\beta \in \mathbb{Q}(\zeta_q)$ and q is minimal with this property, where ζ_q is a primitive qth root of unity.

Note that $A(\alpha) = A(\beta)$ and $l(\alpha) = l(\beta)$. We distinguish two cases.

Case 1. There exists a prime p such that $p^2|q$. Then, let ζ be a primitive root of unity of order $p^r||q$, where $r \geq 2$. Using Lemma 1, we write $\beta = \sum_{j=0}^{p-1}\beta_j\zeta^j$. We eliminate from this sum all terms which have coefficient $\beta_j = 0$. We obtain

$$\beta = \beta_1\zeta^{i_1} + \beta_2\zeta^{i_2} + \cdots + \beta_k\zeta^{i_k}, \tag{1}$$

where k denotes the number of those j for which β_j is non-zero, $0 \leq i_1 < i_2 < \ldots < i_k \leq p-1$, and $\beta_j \in O_{\mathbb{Q}(\zeta_{\frac{q}{p}})} \setminus \{0\}$. Moreover, it follows from the minimality of q that $k \geq 2$, since for $k = 1$, $\beta = \beta_1\zeta^{i_1}$, hence $\beta\zeta^{-i_1}$ would belong to the smaller field $\mathbb{Q}(\zeta_{\frac{q}{p}})$.

Since $A(x) \geq 1$, for any non-zero algebraic integer x, using Lemma 1, we derive

$$\frac{n+1}{2} \geq A(\alpha) = A(\beta) = A(\beta_1) + A(\beta_2) + \cdots + A(\beta_k) \geq A(\beta_j) + k - 1 \geq A(\beta_j) + 1,$$

for any $1 \leq j \leq k$. Hence ,$A(\beta_j) \leq \frac{n+1}{2} - 1 = \frac{n-1}{2}$. By the inductive hypothesis $l(\beta_j) \leq k_{n-1}$, for any $1 \leq j \leq k$. We derive that

$$l(\alpha) = l(\beta) \leq \sum_{j=1}^{k} l(\beta_j) \leq kk_{n-1} \leq \frac{n+1}{2}k_{n-1}.$$

Case 2. q is square-free.

Subcase 2.1 There exists a prime $p|q$ such that $p \geq n^2 + n - 1$.

Let ζ be a primitive root of unity of order p. Using Lemma 1, we can write $\beta = a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{p-1}\zeta^{p-1}$, with $a_j \in \mathbb{Z}[\zeta_{\frac{q}{p}}]$.

https://doi.org/10.1017/S0017089516000586 Published online by Cambridge University Press

Let r be the largest number of equal coefficients among $a_0, a_1, \ldots, a_{p-1}$. Then,

$$A(\beta) \geq \frac{1}{2(p-1)} \sum_{0 \leq i \leq p-1} \#\{0 \leq j \leq p-1 : a_j \neq a_i\}$$
$$\geq \frac{1}{2(p-1)} \sum_{0 \leq i \leq p-1} (p-r) = \frac{p(p-r)}{2(p-1)}.$$

Thus $\frac{n+1}{2} \geq \frac{p(p-r)}{2(p-1)}$, which implies $r \geq p-(n+1)+\frac{n+1}{p} > p-(n+1)$, hence $r \geq p-n$. Subtracting $s(1+\zeta+\cdots+\zeta^{p-1})=0$ from β, where s is the common value of the r equal coefficients, we may assume in what follows that

$$\beta = \beta_1 \zeta^{j_1} + \beta_2 \zeta^{j_2} + \cdots + \beta_k \zeta^{j_k}, \tag{2}$$

with $k \leq n$, $0 \leq j_1 < j_2 < \cdots < j_k \leq p-1$ and all the coefficients $\beta_1, \beta_2, \ldots, \beta_k$ are non-zero elements of $\mathbb{Z}[\zeta_{\frac{q}{p}}]$.

On the other hand, using Lemma 1, we see that

$$\frac{n+1}{2} \geq A(\alpha) = A(\beta) = \frac{1}{p-1}\big(A(\beta_1-\beta_2)+A(\beta_1-\beta_3)+\cdots+A(\beta_{k-1}-\beta_k)\big)$$
$$+\frac{p-k}{p-1}\big(A(\beta_1)+A(\beta_2)+\cdots+A(\beta_k)\big).$$

This implies

$$\frac{n+1}{2} \geq \frac{p-k}{p-1}\sum_{j=1}^{k} A(\beta_j) \geq \frac{p-n}{p-1}\sum_{j=1}^{k} A(\beta_j),$$

hence

$$\sum_{j=1}^{k} A(\beta_j) \leq \frac{(p-1)(n+1)}{2(p-n)}.$$

Fix $j \in \{1, 2, \ldots, k\}$. Since each β_i is a non-zero algebraic integer, we have $A(\beta_i) \geq 1$, and we obtain

$$k-1+A(\beta_j) \leq \sum_{i \neq j} A(\beta_i) + A(\beta_j) \leq \frac{(p-1)(n+1)}{2(p-n)},$$

therefore

$$A(\beta_j) \leq \frac{(p-1)(n+1)}{2(p-n)} - k + 1.$$

Since $k \geq 2$, this further implies

$$A(\beta_j) \leq \frac{p(n-1)+n-1}{2(p-n)}. \tag{3}$$

https://doi.org/10.1017/S0017089516000586 Published online by Cambridge University Press

Since $p \geq n^2 + n - 1$, from (3) we have $A(\beta_j) \leq \frac{n}{2}$, for any $1 \leq j \leq k$. Then, the inductive hypothesis implies $l(\beta_j) \leq k_n$, and from (2) we obtain

$$l(\alpha) = l(\beta) \leq \sum_{j=1}^{k} l(\beta_j) \leq kk_n \leq nk_n.$$

Subcase 2.2 All the primes p in the decomposition of q are less than or equal to $n^2 + n - 2$.

Let $p_1 < p_2 < \cdots < p_{\pi(n^2+n-2)}$ be the primes not exceeding $n^2 + n - 2$, and let $N_0(n)$ be their product. Then, $\beta \in \mathbb{Q}(\zeta_{N_0(n)})$ and Lemma 2 implies

$$l(\beta) \leq 2^{\pi(n^2+n-2)} A(\beta) \leq 2^{\pi(n^2+n-2)} \frac{n+1}{2}.$$

We may now take

$$k_{n+1} \geq \max\Big\{\frac{n+1}{2} k_{n-1}, nk_n, 2^{\pi(n^2+n-2)} \frac{n+1}{2}\Big\}, \tag{4}$$

and then in all cases we have $l(\alpha) = l(\beta) \leq k_{n+1}$. Note that if we let for each j, $k_{j+1} = (j+1)!2^{\pi((j+1)^2+(j+1)-2)}$, then (4) is satisfied for all n.

This completes the proof of Lemma 6. □

REMARK 1. Looking at (4), a natural choice would be for each n to define for k_{n+1} to equal the third bound appearing on the right side of (4). With this choice for all n, however, one runs into difficulty when trying to prove (4), because it is not known that there are prime numbers in each interval of the form $(n^2 + n - 2, (n+1)^2 + (n+1) - 2)$. For this reason, and for simplicity, we introduced the factorial $j!$ in our choice of k_j above (notice that $j!$ is anyway of much smaller order than the other factor, $2^{\pi(j^2+j-2)}$).

4. p-adic bounds on the degree. Let $\mathbb{Q}_p$ be the field of p-adic numbers, and let $|\cdot|_p$ be the usual p-adic absolute value on $\mathbb{Q}_p$.

LEMMA 7. *For any $n \geq 2$, for any prime p, and for any $a_1, a_2, \ldots, a_n \in \mathbb{Q}_p$, we have*

$$\max_{i,j} \min_{(k,l)\neq(i,j)} |(a_i - a_j) - (a_k - a_l)|_p \geq \frac{1}{6^{\frac{n-1}{2}}} \min_{i\neq j} |a_i - a_j|_p.$$

Proof. Let $N = n^2$ and let $\{1, \ldots, n\} \times \{1, \ldots, n\} = \{(i_1, j_1), \ldots, (i_N, j_N)\}$. For every t, let $(k_t, l_t) \neq (i_t, j_t)$ such that $|(a_{i_t} - a_{j_t}) - (a_{k_t} - a_{l_t})|_p = \min_{(k,l)\neq(i_t,j_t)} |(a_{i_t} - a_{j_t}) - (a_k - a_l)|_p$. We must prove that $\max_t |(a_{i_t} - a_{j_t}) - (a_{k_t} - a_{l_t})|_p \geq \frac{1}{6^{\frac{n-1}{2}}} \min_{i\neq j} |a_i - a_j|_p$, i.e. that $6^{\frac{n-1}{2}} \max_t |(a_{i_t} - a_{j_t}) - (a_{k_t} - a_{l_t})|_p \geq |a_i - a_j|_p$ for some $i \neq j$.

We denote by $(\mathbb{R}^n)^*$ the dual of $\mathbb{R}^n$ and for any subspaces $V \subseteq \mathbb{R}^n$, $U \subseteq (\mathbb{R}^n)^*$, we denote by $V^o \subseteq (\mathbb{R}^n)^*$ and $U^o \subseteq \mathbb{R}^n$ their annihilators, $V^o = \{f \in (\mathbb{R}^n)^* \mid f(x) = 0\, \forall x \in V\}$ and $U^o = \{x \in \mathbb{R}^n \mid f(x) = 0\, \forall f \in U\}$. We have $V^{oo} = V$ and $U^{oo} = U$.

For $1 \leq t \leq N$ and $i \neq j$, we consider the linear functions $f_t, g_{i,j} \in (\mathbb{R}^n)^*$ given by $f_t(x_1, \ldots, x_n) = (x_{i_t} - x_{j_t}) - (x_{k_t} - x_{l_t})$ and $g_{i,j}(x_1, \ldots, x_n) = x_i - x_j$. Let $V = \sum_t \mathbb{R} f_t$. We claim that $V^o \subseteq \cup_{i\neq j} (\mathbb{R} g_{i,j})^o$. Assume the contrary. Then, let $x = (x_1, \ldots, x_n) \in$

https://doi.org/10.1017/S0017089516000586 Published online by Cambridge University Press

$V^o \setminus \cup_{i\neq j}(\mathbb{R}g_{i,j})^o$. We have $x_i - x_j = g_{i,j}(x) \neq 0$ if $i \neq j$ and $(x_{i_t} - x_{j_t}) - (x_{k_t} - x_{l_t}) = f_t(x) = 0\ \forall t$. Since x_i are mutually distinct, there are unique indices $i_{\max}$ and $i_{\min}$ such that $x_{i_{\max}} = \max_i x_i$ and $x_{i_{\min}} = \min_i x_i$. We have $x_i < x_{i_{\max}}$ if $i \neq i_{\max}$ and $x_i > x_{i_{\min}}$ if $i \neq i_{\min}$. Let t be the index for which $(i_t, j_t) = (i_{\max}, i_{\min})$. We have $x_{i_t} - x_{k_t} \geq 0$ and $x_{l_t} - x_{j_t} \geq 0$ with equalities iff $k_t = i_t$ and $l_t = j_t$, respectively. Then, from $(x_{i_t} - x_{k_t}) + (x_{l_t} - x_{j_t}) = (x_{i_t} - x_{j_t}) - (x_{k_t} - x_{l_t}) = 0$, we get $k_t = i_t$ and $l_t = j_t$, i.e. $(k_t, l_t) = (i_t, j_t)$. Contradiction.

From $V^o \subseteq \cup_{i\neq j}(\mathbb{R}g_{i,j})^o$, we obtain that $V^o \subseteq (\mathbb{R}g_{i,j})^o$ for some $i \neq j$. (Otherwise V^o could be written as a finite union of subspaces of smaller dimensions, $V^o = \cup_{i\neq j}(V^o \cap (\mathbb{R}g_{i,j})^o)$.) By taking annihilators, we get $V = V^{oo} \supseteq (\mathbb{R}g_{i,j})^{oo} = \mathbb{R}g_{i,j}$, i.e. $g_{i,j} \in V$.

Let $e_1, \ldots, e_n$ be the canonical basis of $\mathbb{R}^n$ and let $e_1^*, \ldots, e_n^*$ be the dual basis of $(\mathbb{R}^n)^*$. We have $e_k^*(e_l) = \delta_{k,l}$ so $e_k^*(x_1, \ldots, x_n) = x_k$. Then, $f_t = (e_{i_t}^* - e_{j_t}^*) - (e_{k_t}^* - e_{l_t}^*) = \sum_k a_{k,t}e_k^*$ and $g_{i,j} = e_i^* - e_j^* = \sum_k b_k e_k^*$, with $a_{k,t}, b_k \in \mathbb{Z}$. Note that the only non-zero entries in the sequence $a_{1,t}, \ldots, a_{n,t}$ are, in some order $1, -1, -1, 1$ or $1, -2, 1$ or $-1, 2, -1$ or $1, -1$. In all cases $\sum_k a_{k,t}^2 \leq 6$.

Now $f_1, \ldots, f_N$ belong to the subspace of $(\mathbb{R}^n)^*$ spanned by $e_2^* - e_1^*, \ldots, e_n^* - e_1^*$, of dimension $n-1$, so $d := \dim V \leq n-1$. Let $1 \leq \beta_1 < \cdots < \beta_d \leq N$ such that $f_{\beta_1}, \ldots, f_{\beta_d}$ is a basis for V. In particular, they are linearly independent so the vectors $(a_{1,\beta_s}, \ldots, a_{n,\beta_s})^T$ with $s = 1, \ldots, d$ are linearly independent. It follows that the $n \times d$ matrix $(a_{k,\beta_s})_{k,s}$ has rank d and hence it has a non-zero $d \times d$ minor, i.e. there are $1 \leq \alpha_1 < \cdots < \alpha_d \leq n$ such that $\det(a_{\alpha_r,\beta_s})_{r,s} \neq 0$.

Since $g_{i,j} \in V$ there are unique $c_1, \ldots, c_d \in \mathbb{R}$ with $g_{i,j} = \sum_s c_s f_{\beta_s}$. When we write this relation in the basis $e_1^*, \ldots, e_n^*$, we get $b_k = \sum_s a_{k,\beta_s}c_s$ for $1 \leq k \leq n$. In particular, $b_{\alpha_r} = \sum_s a_{\alpha_r,\beta_s}c_s$. Hence, $X = (c_1, \ldots, c_d)^T$ is a solution of the equation $AX = b$, where $A = (a_{\alpha_r,\beta_s})_{r,s}$ and $b = (b_{\alpha_1}, \ldots, b_{\alpha_d})^T$. Since A is non-degenerate, we get $c_s = \Delta_s/\Delta$, where $\Delta = \det A$ and Δ_s is the determinant of the matrix obtained by replacing the sth column of A by b. Since A, b have integer entries we have $\Delta, \Delta_s \in \mathbb{Z}$. But for any s, we have $\sum_{r=1}^d a_{\alpha_r,\beta_s}^2 \leq \sum_{k=1}^n a_{k,\beta_s}^2 \leq 6$ so the length of each column vector of A is $\leq \sqrt{6}$. By Hadamard's inequality, we have $|\Delta| \leq \sqrt{6}^d = 6^{\frac{d}{2}} \leq 6^{\frac{n-1}{2}}$.

We now define the linear functions $\tilde{f}_t$ and $\tilde{g}_{i,j} \in (\mathbb{Q}_p^n)^*$ given by $\tilde{f}_t(x_1, \ldots, x_n) = (x_{i_t} - x_{j_t}) - (x_{k_t} - x_{l_t})$ and $\tilde{g}_{i,j}(x_1, \ldots, x_n) = x_i - x_j$. Since $\tilde{f}_t, \tilde{g}_{i,j}$ have the same integer coefficients as $f_t, g_{i,j}$ and $c_s \in \mathbb{Q}$ from $g_{i,j} = \sum_s c_s f_{\beta_s}$, we get the similar relation $\tilde{g}_{i,j} = \sum_s c_s \tilde{f}_{\beta_s}$.

Let $a = (a_1, \ldots, a_n)$. Then, $\tilde{g}_{i,j}(a) = \sum_s c_s \tilde{f}_{\beta_s}(a)$, which implies $|\tilde{g}_{i,j}(a)|_p \leq \max_s |c_s|_p |\tilde{f}_{\beta_s}(a)|_p$. But $|c_s|_p = |\Delta_s/\Delta|_p \leq |\Delta| \leq 6^{\frac{n-1}{2}}$. It follows that $|\tilde{g}_{i,j}(a)|_p \leq 6^{\frac{n-1}{2}} \max_s |\tilde{f}_{\beta_s}(a)|_p \leq 6^{\frac{n-1}{2}} \max_t |\tilde{f}_t(a)|_p$, i.e. $|a_i - a_j|_p \leq 6^{\frac{n-1}{2}} \max_t |(a_{i_t} - a_{j_t}) - (a_{k_t} - a_{l_t})|_p$. □

NOTE. This proof is very similar with the proof of Lemma 4, i.e. Kedlaya's Lemma 16 from [**9**]. In fact Lemma 4 can be seen as a particular case of Lemma 7. Indeed, if $a_1, \ldots, a_n \in \mathbb{Z}$ such that a_i are mutually distinct in $\mathbb{Z}/p\mathbb{Z}$ then $|a_i - a_j|_p = 1$ whenever $i \neq j$. Then, by Lemma 7 we have

$$\max_{i,j} \min_{(k,l)\neq(i,j)} |(a_i - a_j) - (a_k - a_l)|_p \geq \frac{1}{6^{\frac{n-1}{2}}} \min_{i\neq j} |a_i - a_j|_p = \frac{1}{6^{\frac{n-1}{2}}}.$$

Hence, there is a pair (i, j) such that for any $(k, l) \neq (i, j)$, we have $|(a_i - a_j) - (a_k - a_l)|_p \geq \frac{1}{6^{\frac{n-1}{2}}}$. If $p > 6^{\frac{n-1}{2}}$ then for any integer a the only possible values of $|a|_p$ are

https://doi.org/10.1017/S0017089516000586 Published online by Cambridge University Press

$1 > \frac{1}{p} > \frac{1}{p^2} > \ldots$ and 0. So if $|a|_p \geq \frac{1}{6^{\frac{n-1}{2}}} > \frac{1}{p}$ then $|a|_p = 1$, i.e. $a \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. Hence, for any $(k, l) \neq (i, j)$, we have $(a_i - a_j) - (a_k - a_l) \neq 0$ so $a_i - a_j \neq a_k - a_l$ in $\mathbb{Z}/p\mathbb{Z}$.

5. Proof of Theorem 1. We first prove the following proposition.

PROPOSITION 1. *For any positive integer m, there is a finite set T_m (consisting of cyclotomic m-Weil numbers), with*

$$|T_m| < \sum_{d=1}^{13^{6^m}} \prod_{k=1}^{d} \left[2^{1+k\pi(4m^2+2m-2)} \big((2m)!\big)^k \binom{d}{k} + 1 \right]$$

such that the set W_m of all cyclotomic m-Weil numbers satisfies $W_m = T_m \mu_\infty$. Here, $\pi(x)$ is the number of primes less than or equal to x.

Proof. Let $\alpha \in O_{\mathbb{Q}^{ab}}$ be an m-Weil number. Then, $\alpha\zeta$ is an m-Weil number, for any root of unity ζ. Let $\beta \in \{\alpha\zeta : \zeta \text{ root of unity}\}$ with minimal conductor, say $\beta \in \mathbb{Q}(\zeta_q)$, where ζ_q is a primitive qth root of unity, and q is minimal. Note that $A(\beta) = A(\alpha) = m$. Before embarking on the actual proof of Proposition 1, we first outline our general strategy. We first employ a variation of Kedlaya's method (which successfully bounds q in the case q is a prime), to provide in our case of a general q a uniform upper bound for the size of each prime factor dividing q. This part of the proof also makes use of some ideas from our proof of Lemma 6. After completing this first step, we proceed with the second stage of the proof. This consists in providing, for each fixed prime factor p of q, an upper bound for the exponent of p in q. Intuitively, this step is a type of descent, via a tower of subfields of $\mathbb{Q}(\zeta_q)$, where the key tool is provided by the quantitative p-adic Lemma 7. With the completion of this step, which entirely bounds q, we will be in a position where we can view β inside a large, but fixed, cyclotomic field. This will then immediately conclude the proof of Proposition 1, since by Lemma 6 we will have an explicit, uniform upper bound for the length of all m-Weil numbers β, and then applying Lemma 5, we obtain the desired bound on the number of m-Weil numbers in the above fixed cyclotomic field.

STEP I. We bound the prime factors of q.

Let now p be a prime with $p|q$. We distinguish two cases.

Case 1. $p||q$. Let ζ be a primitive pth root of unity. Then, $\beta \in \mathbb{Q}(\zeta_q)$ can be written as $\beta = a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{p-1}\zeta^{p-1}$, with $a_j \in \mathbb{Z}[\zeta_{\frac{q}{p}}]$ and $\zeta = \zeta_q$.

Let r be the largest number of equal coefficients among $a_0, a_1, \ldots, a_{p-1}$. Then, employing Lemma 1 and using the fact that $A(a_j - a_i) \geq 1$ for all pairs (i, j) for which $a_j \neq a_i$, we deduce that

$$\begin{aligned} A(\beta) &\geq \frac{1}{2(p-1)} \sum_{0 \leq i \leq p-1} \#\{0 \leq j \leq p-1 : a_j \neq a_i\} \\ &\geq \frac{1}{2(p-1)} \sum_{0 \leq i \leq p-1} (p-r) = \frac{p(p-r)}{2(p-1)}. \end{aligned}$$

Thus, $m \geq \frac{p(p-r)}{2(p-1)}$, which means $r \geq p - 2m + \frac{2m}{p}$, hence $r \geq p - 2m$. Subtracting $s(1 + \zeta + \cdots + \zeta^{p-1}) = 0$ from β, where s is the common value of the r equal coefficients, we may assume in what follows that $\beta = \alpha_1\zeta^{j_1} + \alpha_2\zeta^{j_2} + \cdots + \alpha_k\zeta^{j_k}$, with

https://doi.org/10.1017/S0017089516000586 Published online by Cambridge University Press

$k \leq 2m$, $0 \leq j_1 < j_2 < \cdots < j_k \leq p-1$ and all the coefficients $\alpha_1, \alpha_2, \ldots, \alpha_k$ are non-zero elements of $\mathbb{Q}(\zeta_{\frac{q}{p}})$.

Here, $k \geq 1$ since β is non-zero. Moreover, we have that $k \geq 2$. Indeed, if $k = 1$, say $\alpha_1 \neq 0$, then $\beta = \alpha_1 \zeta^{j_1}$, hence $\beta \zeta^{-j_1} = \alpha_1 \in \mathbb{Q}(\zeta_{\frac{q}{p}})$, which contradicts the minimality of q.

Assume now that $p > 6^m$. Then $p > 6^{\frac{k}{2}}$, and applying Lemma 4 to $j_1, j_2, \ldots, j_k$, there exists a pair, say (j_1, j_2) such that $j_2 - j_1 \not\equiv j_l - j_s \pmod{p}$, for any $(l, s) \neq (2, 1)$.

Let $i_0 \in \{0, 1, \ldots, p-1\}$ such that $i_0 \not\equiv j_m - j_n \pmod{p}$, for any $1 \leq m, n \leq k$. Such an i_0 exists as $k^2 < p$. Indeed, one can easily prove by induction that $6^{k/2} > k^2$, for any positive integer k, hence we obtain $p > 6^{k/2} > k^2$. Then, since $[\mathbb{Q}(\zeta_q) : \mathbb{Q}(\zeta_{\frac{q}{p}})] = p - 1$, it follows that $1, \zeta, \ldots, \zeta^{i_0-1}, \zeta^{i_0+1}, \ldots, \zeta^{p-1}$ is a basis of $\mathbb{Q}(\zeta_q)$ over $\mathbb{Q}(\zeta_{\frac{q}{p}})$.

Note that for $0 \leq i < j \leq p-1$, we have $1 \leq p - (j-i) \leq p-1$ and

$$\zeta^{i-j} = \zeta^{-(j-i)} = \zeta^{p-(j-i)}.$$

One has

$$\begin{aligned} m = \beta\bar{\beta} &= (\alpha_1\zeta^{j_1} + \alpha_2\zeta^{j_2} + \cdots + \alpha_k\zeta^{j_k})(\bar{\alpha_1}\zeta^{-j_1} + \bar{\alpha_2}\zeta^{-j_2} + \cdots + \bar{\alpha_k}\zeta^{-j_k}) \\ &= \sum_{1\leq j\leq k} |\alpha_j|^2 + \sum_{1\leq l<s\leq k} \alpha_s\bar{\alpha_l}\zeta^{j_s-j_l} + \sum_{1\leq u<v\leq k} \alpha_u\bar{\alpha_v}\zeta^{j_u-j_v} \\ &= \sum_{1\leq j\leq k} |\alpha_j|^2 + \sum_{1\leq l<s\leq k} \alpha_s\bar{\alpha_l}\zeta^{j_s-j_l} + \sum_{1\leq u<v\leq k} \alpha_u\bar{\alpha_v}\zeta^{p-(j_v-j_u)}. \end{aligned}$$

Since $j_2 - j_1 \not\equiv j_l - j_s \pmod{p}$, for any $(l, s) \neq (2, 1)$, the term $\alpha_2\bar{\alpha_1}\zeta^{j_2-j_1}$ on the right side of the above equality cannot be cancelled by any other terms. It follows that $\alpha_2 = 0$ or $\alpha_1 = 0$, a contradiction.

Hence, for any prime p such that $p||q$ one has $p < 6^m$.

Case 2. $p^2|q$. Let ζ be a primitive root of unity of order p^r, where $p^r||q$. Then, $\gamma := \zeta^p \in \mathbb{Q}(\zeta_{\frac{q}{p}})$ is a primitive root of unity of order p^{r-1}.

Using Lemma 1, $\beta \in \mathbb{Q}(\zeta_q)$ can be written as $\beta = \alpha_1\zeta^{i_1} + \alpha_2\zeta^{i_2} + \cdots + \alpha_k\zeta^{i_k}$, with $\alpha_j \in \mathbb{Z}[\zeta_{\frac{q}{p}}] - \{0\}$, for any $1 \leq j \leq k$, with $0 \leq i_1 < i_2 < \cdots < i_k \leq p-1$.

Note that by the same argument as in Case 1, $k \geq 2$.

On the other hand, using Lemma 1, we see that

$$m = A(\beta) = A(\alpha_1) + A(\alpha_2) + \cdots + A(\alpha_k) \geq k,$$

since each α_j is a non-zero algebraic integer.

If $p > 6^{\frac{m}{2}}$, then $p > 6^{\frac{k}{2}}$, and applying Lemma 4 to $i_1, i_2, \ldots, i_k$, there exists a pair, say (i_1, i_2) such that $i_2 - i_1 \not\equiv i_l - i_s \pmod{p}$, for any $(l, s) \neq (2, 1)$.

Note that for $0 \leq i < j \leq p-1$, we have $1 \leq p - (j-i) \leq p-1$ and

$$\zeta^{i-j} = \zeta^{i-j+p^r} = \zeta^{p-(j-i)+p(p^{r-1}-1)} = \zeta^{p-(j-i)} \cdot \zeta^{p(p^{r-1}-1)} = \gamma^{p^{r-1}-1} \cdot \zeta^{p-(j-i)},$$

where $\gamma := \zeta^p \in \mathbb{Q}(\zeta_{\frac{q}{p}})$.

https://doi.org/10.1017/S0017089516000586 Published online by Cambridge University Press

In a similar way as above, we write

$$\begin{aligned} m = \beta\bar{\beta} &= (\alpha_1\zeta^{i_1} + \alpha_2\zeta^{i_2} + \cdots + \alpha_k\zeta^{i_k})(\bar{\alpha_1}\zeta^{-i_1} + \bar{\alpha_2}\zeta^{-i_2} + \cdots + \bar{\alpha_k}\zeta^{-i_k}) \\ &= \sum_{1\le j\le k} |\alpha_j|^2 + \sum_{1\le l<s\le k} \alpha_s\bar{\alpha_l}\zeta^{i_s-i_l} + \sum_{1\le u<v\le k} \alpha_u\bar{\alpha_v}\zeta^{i_u-i_v} \\ &= \sum_{1\le j\le k} |\alpha_j|^2 + \sum_{1\le l<s\le k} \alpha_s\bar{\alpha_l}\zeta^{i_s-i_l} + \sum_{1\le u<v\le k} \alpha_u\bar{\alpha_v}\gamma^{p^{r-1}-1}\zeta^{p-(i_v-i_u)}. \end{aligned}$$

Here, $1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$ is a basis of $\mathbb{Q}(\zeta_q)$ over $\mathbb{Q}(\zeta_{\frac{q}{p}})$. Reasoning as before, we find that $\alpha_2\bar{\alpha_1} = 0$, which is a contradiction.

Hence, for any prime p such that $p^2|q$ one has $p < 6^{\frac{m}{2}}$.

Now that we have a uniform upper bound for the size of all prime factors of q, we proceed with the second stage of the proof of Proposition 1.

STEP II. We now fix a prime divisor p of q, and bound the exponent, call it r, of p in q.

Let ζ be a primitive root of unity of order p^r, where $p^r||q$. Consider the following tower of $r-1$ extensions, each of degree p:

$$\mathbb{Q}(\zeta_{\frac{q}{p^{r-1}}}) \subset \mathbb{Q}(\zeta_{\frac{q}{p^{r-2}}}) \ldots \subset \mathbb{Q}(\zeta_{\frac{q}{p}}) \subset \mathbb{Q}(\zeta_q).$$

Using Lemma 3, write $\beta \in \mathbb{Q}(\zeta_q)$ as

$$\beta = \alpha_1\zeta^{i_1} + \alpha_2\zeta^{i_2} + \cdots + \alpha_k\zeta^{i_k}, \tag{5}$$

with $\alpha_j \in \mathbb{Z}[\zeta_{\frac{q}{p^{r-1}}}] - \{0\}$, for any $1 \le j \le k$, with $0 \le i_1 < i_2 < \cdots < i_k < p^{r-1}$.

Note that for $0 \le i < j \le p^{r-1} - 1$, we have $1 \le p^{r-1} - (j-i) \le p^{r-1} - 1$ and

$$\zeta^{i-j} = \zeta^{i-j+p^r} = \zeta^{p^{r-1}-(j-i)+p^{r-1}(p-1)} = \zeta^{p^{r-1}-(j-i)} \cdot \zeta^{p^{r-1}(p-1)} = \delta^{p-1} \cdot \zeta^{p^{r-1}-(j-i)},$$

where $\delta := \zeta^{p^{r-1}} \in \mathbb{Q}(\zeta_{\frac{q}{p^{r-1}}})$.

One has

$$\begin{aligned} m = \beta\bar{\beta} &= (\alpha_1\zeta^{i_1} + \alpha_2\zeta^{i_2} + \cdots + \alpha_k\zeta^{i_k})(\bar{\alpha_1}\zeta^{-i_1} + \bar{\alpha_2}\zeta^{-i_2} + \cdots + \bar{\alpha_k}\zeta^{-i_k}) \\ &= \sum_{1\le j\le k} |\alpha_j|^2 + \sum_{1\le l<s\le k} \alpha_s\bar{\alpha_l}\zeta^{i_s-i_l} + \sum_{1\le u<v\le k} \alpha_u\bar{\alpha_v}\zeta^{i_u-i_v} \\ &= \sum_{1\le j\le k} |\alpha_j|^2 + \sum_{1\le l<s\le k} \alpha_s\bar{\alpha_l}\zeta^{i_s-i_l} + \sum_{1\le u<v\le k} \alpha_u\bar{\alpha_v}\delta^{p-1}\zeta^{p^{r-1}-(i_v-i_u)}. \end{aligned}$$

Note that $1, \zeta, \ldots, \zeta^{p^{r-1}-1}$ is an integral basis of $\mathbb{Q}(\zeta_q)$ over $\mathbb{Q}(\zeta_{\frac{q}{p^{r-1}}})$.

If there exists a pair (i_a, i_b) such that $i_a - i_b \not\equiv i_l - i_s \pmod{p^r}$, for all $(l, s) \ne (a, b)$ then $\alpha_a\bar{\alpha_b} = 0$, so $\alpha_a = 0$ or $\alpha_b = 0$, contradiction.

Hence, for any $a, b \in \{1, 2, \ldots, k\}$ there exist $l, s \in \{1, 2, \ldots, k\}$ such that $i_a - i_b \equiv i_l - i_s \pmod{p^r}$. This means $|(i_a - i_b) - (i_l - i_s)|_p \le \frac{1}{p^r}$. It follows that

$$\frac{1}{p^r} \ge \max_{a,b} \min_{l,s} |(i_a - i_b) - (i_l - i_s)|_p.$$

https://doi.org/10.1017/S0017089516000586 Published online by Cambridge University Press

Lemma 7 implies that $\frac{1}{p^r} \geq \frac{1}{6^{\frac{k-1}{2}}} \min_{a\neq b} |i_a - i_b|_p$. Then, there exist $a_0, b_0 \in \{1, 2, \ldots, k\}$ such that $|i_{a_0} - i_{b_0}|_p \leq 6^{\frac{k-1}{2}} \cdot \frac{1}{p^r}$.

Fix a positive integer $c_{k,p}$ such that $6^{\frac{k-1}{2}} < p^{c_{k,p}}$. Note that we can take $c_{k,p} = 2k-1$ (independent of p). Then

$$|i_{a_0} - i_{b_0}|_p < \frac{1}{p^{r-c_{k,p}}}. \tag{6}$$

If $r \leq c_{k,p} + 1 = 2k$, we are done. In this case, we have $r \leq 2k \leq 2m$, since Lemma 3 and relation (5) imply $m = A(\beta) = A(\alpha_1) + A(\alpha_2) + \cdots + A(\alpha_k) \geq k$.

If $r > c_{k,p} + 1$, then relation (6) is equivalent to $i_{a_0} \equiv i_{b_0} \pmod{p^{r-c_{k,p}}}$. Let t be an integer such that $i_{a_0} = i_{b_0} + p^{r-c_{k,p}} t$. We may assume, without loss of generality, $a_0 = 1$, $b_0 = 2$, and thus we obtain $i_1 = i_2 + p^{r-c_{k,p}} t$. We deduce

$$\alpha_1 \zeta^{i_1} + \alpha_2 \zeta^{i_2} = \zeta^{i_2}(\alpha_2 + \alpha_1 \zeta^{i_1 - i_2}) = \zeta^{i_2}(\alpha_2 + \alpha_1 \zeta^{p^{r-c_{k,p}} t}).$$

Note that

$$\zeta^{p^{r-c_{k,p}}} \in \mathbb{Q}(\zeta_{\frac{q}{p^{r-1}}})(\zeta_{p^{c_{k,p}}}) \subseteq \mathbb{Q}\Big(\zeta_{\frac{q}{p^{r-1-c_{k,p}}}}\Big), \text{ so}$$

$$\gamma_2 := \alpha_2 + \alpha_1 \zeta^{p^{r-c_{k,p}} t} \in \mathbb{Q}\Big(\zeta_{\frac{q}{p^{r-1-c_{k,p}}}}\Big).$$

Hence, $\beta = \gamma_2 \zeta^{i_2} + \gamma_3 \zeta^{i_3} + \cdots + \gamma_k \zeta^{i_k}$, where $\gamma_j := \alpha_j$, for any $3 \leq j \leq k$.

For each l, $2 \leq l \leq k$, we use the division algorithm to write $i_l = a_l p^{r-1-c_{k,p}} + b_l$, for some positive integers a_l, b_l with $0 \leq b_l < p^{r-1-c_{k,p}}$. It follows that

$$\gamma_l \zeta^{i_l} = \gamma_l \zeta^{a_l p^{r-1-c_{k,p}}} \zeta^{b_l} = \delta_l \zeta^{b_l}, \text{ where } \delta_l := \gamma_l \zeta^{a_l p^{r-1-c_{k,p}}} \in \mathbb{Q}\Big(\zeta_{\frac{q}{p^{r-1-c_{k,p}}}}\Big).$$

Hence,

$$\beta = \delta_2 \zeta^{b_2} + \delta_3 \zeta^{b_3} + \cdots + \delta_k \zeta^{b_k}. \tag{7}$$

Note that (7) is the representation of β in the basis $1, \zeta, \zeta^2, \ldots, \zeta^{p^{r-1-c_{k,p}}-1}$. In conclusion, β can be uniquely written as

$$\beta = \eta_1 \zeta^{j_1} + \eta_2 \zeta^{j_2} + \cdots + \eta_s \zeta^{j_s},$$

with $0 \leq j_1 < j_2 < \cdots < j_s < p^{r-1-c_{k,p}}$, $s < k$ and $\eta_i \in \mathbb{Q}\Big(\zeta_{\frac{q}{p^{r-1-c_{k,p}}}}\Big)$, for any $1 \leq i \leq s$.

This shows that the representation of β in the basis corresponding to $\mathbb{Q}\Big(\zeta_{\frac{q}{p^{r-1-c_{k,p}}}}\Big)$ is strictly shorter than the representation corresponding to $\mathbb{Q}\Big(\zeta_{\frac{q}{p^{r-1}}}\Big)$.

Let $L_\beta(j)$ be the length of the representation of β in the basis $1, \zeta, \ldots, \zeta^{p^j-1}$ of $\mathbb{Q}(\zeta_q)$ over $\mathbb{Q}(\zeta_{\frac{q}{p^j}})$. We proved that $k_2 := L_\beta(r-1-c_{k_1,p}) < L_\beta(r-1) = k =: k_1$.

Repeating this argument, we obtain $k_3 := L_\beta(r-1-c_{k_1,p}-c_{k_2,p}) < L_\beta(r-1-c_{k_1,p}) = k_2$, for a certain positive integer $c_{k_2,p}$.

Continuing in this way, there are two possibilities:

https://doi.org/10.1017/S0017089516000586 Published online by Cambridge University Press

Either 1. There is a $d \geq 1$ such that $L_\beta(r - 1 - c_{k_1,p} - c_{k_2,p} - \cdots - c_{k_d,p}) = 1$. This contradicts the minimality of q.

Or 2. There is an $e \geq 1$ such that $r - 1 - c_{k_1,p} - c_{k_2,p} - \cdots - c_{k_e,p} \leq c_{k_{e+1},p}$. This implies $r_p := r \leq 1 + \sum_{i=2}^{m} c_{i,p}$ (where $c_{i,p} = 0$, if $i \notin \{k_1, k_2, \ldots, k_{e+1}\}$). In this case, we have

$$r_p \leq 1 + \sum_{i=2}^{m} (2i - 1) = m^2.$$

STEP III. Constructing the set T_m.

Recall that we proved that if $p||q$ then $p < 6^m$, and that if $p^2|q$ one has $p < 6^{\frac{m}{2}}$.

We have

$$q = \prod_{p|q} p^{r_p} = \Big(\prod_{p||q} p\Big)\Big(\prod_{p^2|q} p^{r_p}\Big).$$

Let

$$T = \Big(\prod_{p<6^m} p\Big)\Big(\prod_{p<6^{\frac{m}{2}}} p\Big)^{m^2}.$$

Then $q \mid T$ and $\log T = A + B$, where

$$A := \log\Big(\prod_{p<6^m} p\Big) = \sum_{p<6^m} \log p < \sum_{p<6^m} m \log 6 = m \log 6 \sum_{p<6^m} 1 < m(\log 6)\pi(6^m) \qquad \text{and}$$

$$B := m^2 \log\Big(\prod_{p<6^{\frac{m}{2}}} p\Big) = m^2 \sum_{p<6^{\frac{m}{2}}} \log p < m^2\Big(\frac{m}{2} \log 6\Big) \sum_{p<6^{\frac{m}{2}}} 1 < \frac{m^3}{2}(\log 6)\pi(6^{\frac{m}{2}}).$$

Using the inequality $\pi(x) < C_0 \frac{x}{\log x}$, where $C_0 = 1.25506$ valid for $x > 1$ (see [7]), we derive

$$\log T = A + B < C_0 6^m + C_0 m^2 6^{\frac{m}{2}} = C_0 6^{\frac{m}{2}}(6^{\frac{m}{2}} + m^2) < C_0 6^{\frac{m}{2}}(6^{\frac{m}{2}} + 6^{\frac{m}{2}}) = 2C_0 6^m,$$

hence $T < e^{2C_0 6^m} < 13^{6^m}$.

Now, since $A(\beta) = A(\alpha) = m$, using Lemma 6, we obtain

$$l(\beta) \leq k_{2m} = (2m)! \cdot 2^{\pi(4m^2+2m-2)} =: M.$$

On the other hand, $\beta \in \mathbb{Q}(\zeta_q) \subset \mathbb{Q}(\zeta_T)$ implies $\deg \beta \leq \phi(T) < T < 13^{6^m}$. Applying Lemma 5, we conclude that there are at most $n(T, M)$ such numbers β, where $n(T, M) < T \sum_{d=1}^{T} \prod_{k=1}^{d} [2\binom{d}{k} M^k + 1]$.

Let $\{u_1, u_2, \ldots, u_L\} \subset W_m \cap \mathbb{Q}(\zeta_T)$ be such that $W_m = \{u_1, u_2, \ldots, u_L\}\mu_\infty$ and $\frac{u_i}{u_j} \notin \mu_\infty$ for any $i \neq j$. Since $\frac{u_i}{u_j} \notin \mu_T$ for any $i \neq j$, the sets $u_i\mu_T$, $1 \leq i \leq L$, are disjoint. Since $\bigsqcup_{i=1}^{n} u_i\mu_T \subset \mathbb{Q}(\zeta_T) \cap W_m$, we derive

$$LT \leq |W_m \cap \mathbb{Q}(\zeta_T)| \leq n(T, M) < T \sum_{d=1}^{T} \prod_{k=1}^{d} \Big[2\binom{d}{k} M^k + 1\Big].$$

https://doi.org/10.1017/S0017089516000586 Published online by Cambridge University Press

Therefore

$$L < \sum_{d=1}^{T} \prod_{k=1}^{d} \left[2\binom{d}{k} M^k + 1 \right] < \sum_{d=1}^{13^{6^m}} \prod_{k=1}^{d} \left[2\binom{d}{k} \left((2m)! \cdot 2^{\pi(4m^2+2m-2)} \right)^k + 1 \right],$$

hence

$$L < \sum_{d=1}^{13^{6^m}} \prod_{k=1}^{d} \left[2^{1+k\pi(4m^2+2m-2)} \left((2m)! \right)^k \binom{d}{k} + 1 \right],$$

so we can take $T_m = \{u_1, u_2, \ldots, u_L\}$, which completes the proof of Proposition 1. □

We now prove Theorem 1.
Let $m \geq 1$ be an integer and let

$$H_m = \{x_1^{e_1} x_2^{e_2} \ldots x_n^{e_n} : n \in \mathbb{N}, x_i \in W_m, e_i \in \mathbb{Z}, \forall 1 \leq i \leq n \text{ and } e_1 + e_2 + \cdots + e_n = 0\}.$$

For any finitely generated abelian group G, let $d(G)$ denote the minimum number of generators of G.

Let $\{u_1, u_2, \ldots, u_L\} \subset W_m$ be such that $W_m = \{u_1, u_2, \ldots, u_L\}\mu_\infty$ and $\frac{u_i}{u_j} \notin \mu_\infty$ for any $i \neq j$. Then, $\{\frac{u_1}{u_2}, \frac{u_1}{u_3}, \ldots, \frac{u_1}{u_L}\}$ provides a set of generators for the quotient group H_m/μ_∞.

We know from [**9**] that $G = H_m/\mu_\infty$ is a finitely generated, torsion-free abelian group, hence $r_m = \operatorname{rank}(H_m/\mu_\infty) = d(H_m/\mu_\infty) \leq L - 1$. Thus,

$$r_m < L < \sum_{d=1}^{13^{6^m}} \prod_{k=1}^{d} \left[2^{1+k\pi(4m^2+2m-2)} \left((2m)! \right)^k \binom{d}{k} + 1 \right].$$

ACKNOWLEDGEMENTS. The authors are grateful to the referee for many useful comments and suggestions. C. Beli was supported by the Romanian IDEI project PCE_2012-4-364 of the Ministry of National Education CNCS-UEFISCIDI.

REFERENCES

1. A. J. de Jong, Smoothness, semi-stability and alterations, *Inst. Hautes Études Sci. Publ. Math.* **83** (1996), 51–93.

2. T. Honda, Isogeny classes of abelian varieties over finite fields, *J. Math. Soc. Japan* **20** (1968), 83–95.

3. L. Kronecker, Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten, *J. Reine Angew. Math.* **53** (1857), 173–175.

4. J. H. Loxton, On the maximum modulus of cyclotomic integers, *Acta Arith.* **22** (1972), 69–85.

5. J. H. Loxton, On two problems of R. M. Robinson about sums of roots of unity, *Acta Arith.* **26** (1974/75), 159–174.

6. D. Mumford, *Abelian varieties* (Tata Institute of Fundamental Research, Bombay and Oxford University Press, London, 1970).

7. J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6**(1) (1962), 64–94.

8. F. Stan and A. Zaharescu, Siegel's trace problem and character values of finite groups, *J. Reine Angew. Math.* **637** (2009), 217–234.

9. F. Stan and A. Zaharescu, Weil numbers in finite extensions of $\mathbb{Q}^{ab}$: The Loxton-Kedlaya phenomenon, *Trans. Amer. Math. Soc.* **367**(6) (2015), 4359–4376.

10. J. Tate, Classes d'isogénie de variétés abéliennes sur un corps fini (d'après T. Honda), Exp. No. 352, in *Séminaire Bourbaki 1968/69*, Lecture Notes in Mathematics 175 (Springer-Verlag, Berlin, 1971), 95–110.