Max-Planck-Institut für Mathematik
Bonn

Large absolute values of cyclotomic polynomials at roots of unity

by

Lilit Martirosyan
Pieter Moree

Max-Planck-Institut für Mathematik
Preprint Series 2020 (25)

Large absolute values of cyclotomic polynomials at roots of unity

Lilit Martirosyan
Pieter Moree

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Department of Mathematics and Statistics
University of North Carolina, Wilmington
601 South College Road
Wilmington, NC 28403-5970
USA

MPIM 20-25

LARGE ABSOLUTE VALUES OF CYCLOTOMIC POLYNOMIALS AT ROOTS OF UNITY

LILIT MARTIROSYAN AND PIETER MOREE

Abstract. The n^{th} cyclotomic polynomial $\Phi_n(X)$ is the minimal polynomial of $\zeta_n := e^{2\pi i/n}$. Given an integer $m \geq 1$ and a prescribed set S of arithmetic progressions modulo m, we define n_x as the product of the primes $p \leq x$ lying in those progressions. Let $d(n)$ denote the number of divisors of n. It turns out that under certain conditions on S and m there exists j_x such that $\log |\Phi_{n_x}(\zeta_m^{j_x})|/d(n_x)$ tends to a positive limit. Our aim is to determine those conditions. We use the arithmetic of cyclotomic number fields, non-standard properties of character tables of finite abelian groups and a recent theorem of Bzdęga, Herrera-Poyatos and Moree. After developing some generalities, we restrict to the case where m is a prime.

Our motivation comes from a paper of Vaughan (1975). He studied the case where $S = \{\pm 2 \pmod 5\}$ and used it to show that the maximum coefficient in absolute value of Φ_n can be very large.

1. Introduction

Let $\Phi_n(X) = \sum_{j=0}^{\varphi(n)} a_n(j)X^j$ be the n^{th} cyclotomic polynomial, where φ denotes Euler's totient function. The height $A(n)$ of Φ_n is defined as $A(n) = \max_{0\leq j\leq\varphi(n)} |a_n(j)|$. If z is on the unit circle, then

$$A(n) \geq \frac{\sum_{0\leq j\leq\varphi(n)} |a_n(j)|}{\varphi(n)+1} \geq \frac{|\Phi_n(z)|}{\varphi(n)+1}. \tag{1}$$

This inequality shows that if we can identify n and z for which $|\Phi_n(z)|$ is large, then $A(n)$ must be large. Vaughan [15] identified appropriate n in the case where z is a fifth root of unity and showed that for a certain sequence of integers n_j with $d(n_j)$ tending to infinity, one has

$$A(n_j) \geq \frac{\tau^{d(n_j)/2}}{\varphi(n_j)+1}, \tag{2}$$

with $\tau = (1+\sqrt{5})/2$, the golden ratio[1]. This lower bound can be compared to the upper bound

$$A(n) < e^{\frac{1}{2}d(n)\log n}, \tag{3}$$

due to Bateman [1]. Vaughan used his lower bound (2) to establish the following result.

Theorem 1 (Vaughan [15])**.** *There exist infinitely many integers n for which*

$$\log\log A(n) > (\log 2)\frac{\log n}{\log\log n}.$$

From (3) it can be inferred that this result cannot be improved in the sense that it becomes false if $\log 2$ is replaced by any larger number. However, it is possible to improve on (2).

Mathematics Subject Classification (2000). 11N37, 11Y60

[1] Vaughan, however, does not mention the golden ratio, cf. Remark 32.

Theorem 2 (Bateman et al. [2]). *Let $\alpha > 1$ be arbitrary. There is a sequence n_j with $d(n_j)$ tending to infinity, for which*

$$A(n_j) \geq \frac{\alpha^{d(n_j)}}{\varphi(n_j)+1}. \tag{4}$$

Corollary 3. *The sequence $\{\log(A(n))/d(n)\}_{n=1}^{\infty}$ is unbounded.*

In the latter result and (2) the numbers n_j are of a very particular form. We study more systematically when $|\Phi_{n_j}(\zeta)|$ can get very large for a more general class of numbers n_j (with ζ a root of unity). As a byproduct, we obtain a new proof of Theorem 2. We now introduce this more general class of numbers.

Let $m \geq 2$ be an integer and $S \subseteq (\mathbb{Z}/m\mathbb{Z})^*$ be a non-empty subset. Let

$$P_S := \{q : \exists\, s \in S \text{ such that } q \equiv s \,(\text{mod } m)\},$$

where here and in the sequel the letter q is exclusively used to denote prime numbers. Given a real number x, consider the prime product

$$n_x = \prod_{q \leq x,\ q \in P_S} q. \tag{5}$$

We define

$$\Psi_n(m) = \max_{1 \leq j \leq m,\, (j,m)=1} |\Phi_n(\zeta_m^j)|.$$

Note that $\Psi_n(m) \neq 0$ if and only if $n \neq m$. Now suppose that $n \neq m$. As $\Phi_n(\zeta_m)$ is an algebraic integer the norm $N_{\mathbb{Q}(\zeta_m):\mathbb{Q}}(\Phi_n(\zeta_m))$ is at least one in absolute value, $1 \leq |N_{\mathbb{Q}(\zeta_m):\mathbb{Q}}(\Phi_n(\zeta_m))| \leq \Psi_n(m)^{\varphi(m)}$, and thus $\Psi_n(m) \geq 1$.

It follows from Vaughan [15] that, with the choice $S = \{2, 3\}$ and $m = 5$,

$$\log|\Psi_{n_x}(5)| \geq (\log \tau) d(n_x)/2.$$

Let $r \geq 2$ be an integer. Bateman et al. [2] took $S = \{2r-1, 2r+1\}$ and $m = 4r$ and showed

$$\log|\Psi_{n_x}(4r)| > (\log r) d(n_x)/2.$$

This result, via (1), then implies Theorem 2.

Our main result on $\Psi_n(m)$ is Theorem 5 and is proved in Section 4. Before formulating it, we set forth an important definition.

Definition 4. Given an integer m and a non-empty subset $S \subseteq (\mathbb{Z}/m\mathbb{Z})^*$, the set $\mathfrak{S}$ of even characters modulo m such that $\chi(s) = -1$ for every s in S is said to be the *S-clan*. If $\mathfrak{S}$ is non-empty, then $(S; m)$ is said to be a *Vaughan pair.* If for an integer m a Vaughan pair exists, m is said to be a *Vaughan number.*

The mention of even characters might look odd, but is a consequence of the fact that only even characters appear in (13), which is the basic identity we use. Likewise, the importance of character values being -1 is related to the factor $\prod_{q|n}(1-\overline{\chi}(q))$ in (13) being maximal in that case.

As usual, we let $\omega(n)$ denote the number of distinct prime factors of n.

Theorem 5. *Let $m \geq 1$ be an integer. Let $\widehat{G}(m)$ be the multiplicative group of the Dirichlet characters on the multiplicative group $G(m)$ modulo m. For any $\chi \in \widehat{G}(m)$ we define*

$$C_\chi(\xi_m) = \sum_{g \in G(m)} \overline{\chi}(g) \log(1 - \xi_m^g), \tag{6}$$

where ξ_m is any m^{th} primitive root of unity, log *stands for the principal determination of the logarithm in $\mathbb{C} \setminus \mathbb{R}^-$ and the notation $g \in G(m)$ is a compact way of writing $1 \leq g \leq m$ and $(g, m) = 1$.*

Suppose that $S \subseteq (\mathbb{Z}/m\mathbb{Z})^*$ is non-empty. Let j be coprime to m. We have, as x tends to infinity,

$$\log |\Phi_{n_x}(\zeta_m^j)| = (-1)^{\omega(n_x)} d(n_x) q_j(S; m) + o(d(n_x)), \tag{7}$$

with

$$q_j(S; m) = \frac{1}{\varphi(m)} \sum_{\chi \in \mathfrak{S}} C_\chi(\zeta_m^j), \tag{8}$$

where χ ranges over the characters in the S-clan $\mathfrak{S}$. Furthermore, we have

$$\log \Psi_{n_x}(m) = d(n_x) q(S; m) + o(d(n_x)), \tag{9}$$

with

$$q(S; m) = \max\{q_j(S; m) : 1 \leq j \leq m,\ (j, m) = 1\},$$

Corollary 6. *If S and T have the same clan, then $q(S; m) = q(T; m)$.*

Remark 7. The factor $(-1)^{\omega(n_x)}$ in (7) is a nuisance. The way Vaughan dealt with this is to keep n_x as it is if $\omega(n_x)$ is odd and leave out 2 otherwise (in our setting this would be the smallest prime factor of n_x). Our way to deal with this technical complication is not to keep j fixed, but maximize over all j that are allowed (that is we consider $\Psi_{n_x}(m)$).

It follows from (9) that

$$\lim_{x \to \infty} \frac{\log \Psi_{n_x}(m)}{d(n_x)} = q(S; m).$$

We call $q(S; m)$ the *quality* of the pair $(S; m)$. Note that $q(S; m) \geq 0$ (some of the numbers $q_j(S; m)$ might be negative though). A necessary condition for the pair $(S; m)$ to have positive quality is that it is a Vaughan pair. Any Vaughan pair $(S; m)$ with $q(S; m) > 0$ (which we call a *positive quality Vaughan pair*) leads via (1) to a good lower bound for $A(n_x)$.

Proposition 8. *Let $(S; m)$ be a positive quality Vaughan pair, $\epsilon > 0$ and n_x as in (5). Then*

$$A(n_x) \geq \frac{e^{(q(S;m) - \epsilon) d(n_x)}}{\varphi(n_x) + 1} \tag{10}$$

for every x sufficiently large.

Proof. By (1) we have $A(n_x) \geq \Psi_{n_x}(m)/(\varphi(n_x) + 1)$. Now invoke Theorem 5. □

The following result generalizes Theorem 1 and is proved in Section 5.

Theorem 9. *If $(S; m)$ is a positive quality Vaughan pair and n_x is as in (5), then*

$$\log \log A(n_x) \geq \log 2 \frac{\log n_x}{\log \log n_x} \Big(1 + \frac{1 + \log |S| - \log \varphi(m)}{\log \log n_x} + O\Big(\frac{1}{(\log \log n_x)^2}\Big)\Big),$$

for every x sufficiently large, with the implied error term depending at most on m.

Corollary 10. *If $|S| > \varphi(m)/e$, then we have*

$$\log \log A(n_x) > \log 2 \frac{\log n_x}{\log \log n_x}$$

for every x sufficiently large.

Proposition 8 and Theorem 9 suggest the relevance of the following problem.

Problem 11. *Determine all Vaughan pairs $(S;m)$ and their quality.*

A crucial concept to make this problem more manageable is that of *optimal Vaughan pair.*

Definition 12. We say that a Vaughan pair $(S;m)$ is *optimal* if there does not exist a Vaughan pair $(T;m)$ with $S \subset T$ such that the T-clan equals the S-clan.

Corollary 6 implies that if s is in S, then S and $S \cup \{-s\}$ have the same quality. We thus infer that if S is optimal, then $S = -S$. A Vaughan pair $(S;m)$ with $S = -S$ can be regarded as a pair $(S;m)$ with $S \subseteq (\mathbb{Z}/m\mathbb{Z})^*/\{\pm 1\}$. In the rest of the paper, we only consider pairs of the form $(S;m)$ with $S \subseteq (\mathbb{Z}/m\mathbb{Z})^*/\{\pm 1\}$, where we write elements in S as $\pm b$. Although not entirely consistent with this, it turns out more practical to have $\pm b$ contribute two, rather than one, to the cardinality of S.

As our aim is finding high quality Vaughan pairs, we will focus on the following problem.

Problem 13. *Determine all optimal Vaughan pairs $(S;m)$ with $S \subseteq (\mathbb{Z}/m\mathbb{Z})^*/\{\pm 1\}$ having positive quality.*

This turns out to be quite challenging and we restrict here to the case where $m = p$ is a prime. As a warm up we consider two easy examples.

Example 14 ($p = 11$): Here there is no even character assuming the value -1. Hence, 11 is not a Vaughan number.

Table 1. The even characters modulo 11 (with $\omega = \zeta_{10}$)

χ	± 1	± 2	± 3	± 4	± 5
χ_1	1	1	1	1	1
χ_2	1	ω^2	$-\omega$	ω^4	$-\omega^3$
χ_3	1	ω^4	ω^2	$-\omega^3$	$-\omega$
χ_4	1	$-\omega$	$-\omega^3$	ω^2	ω^4
χ_5	1	$-\omega^3$	ω^4	$-\omega$	ω^2

Example 15 ($p = 13$): There are two possible S-clans, namely χ_5 and $\{\chi_4, \chi_5, \chi_6\}$. Note that χ_5 is the Legendre symbol. The Vaughan pairs $(\pm 2; 13)$ and $(\{\pm 2, \pm 6\}; 13)$ are not optimal. On the other hand $(\pm 5; 13)$ and $(\{\pm 2, \pm 5, \pm 6\}; 13)$ are (for their qualities, see Table 3). Furthermore, these two optimal pairs are the only two, cf. Theorem 19.

Table 2. The even characters modulo 13

χ	± 1	± 2	± 3	± 4	± 5	± 6
χ_1	1	1	1	1	1	1
χ_2	1	ζ_3	ζ_3	$-\zeta_6$	1	$-\zeta_6$
χ_3	1	$-\zeta_6$	$-\zeta_6$	ζ_3	1	ζ_3
χ_4	1	ζ_6	$-\zeta_6$	ζ_3	-1	$-\zeta_3$
χ_5	1	-1	1	1	-1	-1
χ_6	1	$-\zeta_3$	ζ_3	$-\zeta_6$	-1	ζ_6

That 13 is a Vaughan number and 11 is not, is predicted by the following result.

Proposition 16. *The integer m is a Vaughan number if and only if $4 \mid \varphi(m)$.*

Proof. This is a corollary of Theorem 28 below, stating that there is an even character modulo m assuming the value -1 if and only if 4 divides $\varphi(m)$. □

If we restrict to the case where $m = p$ is a prime, the result already follows from Lemma 27, as $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.

We thus may assume that $p \equiv 1 \pmod 4$. In Theorem 17, proved in Section 6, we exhibit two optimal Vaughan pairs having positive quality. As $\big(\frac{-1}{p}\big) = (-1)^{(p-1)/2} = 1$, the Legendre symbol is an even character. It follows that we can write the set of quadratic non-residues modulo p as $N = \{\pm n_1, \ldots, \pm n_{(p-1)/4}\}$. The equation $x^2 \equiv -1 \pmod p$ has two solutions a_1, a_2 with $0 < a_1 < p/2 < a_2 < p$ and $a_2 = p - a_1$. Note that $\sin(\pi a_1/p) = \sin(\pi a_2/p)$. Thus the optimal Vaughan pair in part b exists and has a well-defined quality.

Theorem 17. *Let $p \equiv 1 \pmod 4$ be prime.*
a) *Let N be the set of quadratic non-residues. Then $(N; p)$ is an optimal Vaughan pair having quality*

$$q(N; p) = \frac{\sqrt{p}}{p-1} L\big(1, \big(\tfrac{\cdot}{p}\big)\big).$$

b) *Let a be a solution of $a^2 \equiv -1 \pmod p$ with $0 < a < p$. Then $(\{\pm a\}; p)$ is an optimal Vaughan pair having quality*

$$q(\{\pm a\}; p) = \frac{1}{2} \log\Big(\frac{\sin(\pi a/p)}{\sin(\pi/p)}\Big).$$

The qualities appearing above are positive. In case (a) it is a very classical fact that $L\big(1, \big(\frac{\cdot}{p}\big)\big) \neq 0$ (a crucial ingredient in Legendre's proof that there are infinitely many primes in any primitive residue class modulo p), in case (b) it is obvious. Furthermore, note that all the pairs under (a) satisfy the condition of Corollary 10, but for the pairs under (b) only if $p = 5$.

A small sample of numerical data related to Theorem 17 is given in Table 3.

Table 3. Some optimal Vaughan pairs

p	$q(N;p)$	a	$q(\{\pm a\};p)$
5	$0.2406059125\ldots$	2	$0.2406059125\ldots$
13	$0.1991272028\ldots$	5	$0.6813902247\ldots$
17	$0.2618390684\ldots$	5	$0.7342783356\ldots$
29	$0.1176593675\ldots$	12	$1.0936958650\ldots$
37	$0.1384322140\ldots$	6	$0.8746623453\ldots$
41	$0.2079563567\ldots$	9	$1.0588226638\ldots$
...	...	...	...
97	$0.1942579811\ldots$	22	$1.5025608718\ldots$

For $p = 5$ the two qualities coincide as the two optimal Vaughan pairs are the same in that case (and only in that case).

In Proposition 18 (proved in Section 7) we give estimates for the quantities in Table 3, where for compactness of exposition we let a_p be the unique solution of

$$a_p^2 \equiv -1 \pmod p,\ 0 < a_p < p/2. \tag{11}$$

Proposition 18.
a) *Let $\epsilon > 0$ be arbitrary. For all primes $p \equiv 1 \,(\mathrm{mod}\ 4)$ sufficiently large we have*

$$\frac{1}{4}\log p - \epsilon < q(\{\pm a_p\}; p) < \frac{1}{2}\log\Big(\frac{p}{\pi}\Big) + \epsilon, \tag{12}$$

with a_p as in (11)*. For a positive fraction of all primes $p \equiv 1 \,(\mathrm{mod}\ 4)$ we have*

$$q(\{\pm a_p\}; p) > \frac{1}{2}\log\Big(\frac{p}{\pi}\Big) - \epsilon.$$

b) *We have*

$$\max\{q(N; p) \,:\, p \equiv 1 \,(\mathrm{mod}\ 4)\} = q(N; 17) = \frac{1}{8}\log(4 + \sqrt{17}) = 0.2618390684\ldots$$

The primes $p = 5, 17, 41, 97$, and no other primes $p \equiv 1 \,(\mathrm{mod}\ 4)$, satisfy $q(N; p) \geq 0.16$.
c) *We have $q(\{\pm a_p\}; p) \geq q(N; p)$, with equality only if $p = 5$.*

Given a Vaughan number m, we define its *top quality* as

$$q(m) = \max\{q(S; m) : (S; m) \text{ is an optimal Vaughan pair}\}.$$

Note that $q(m) = \max\{q(S; m) : (S; m) \text{ is a Vaughan pair}\}$. Proposition 18a shows that the top quality is unbounded in case m ranges over the primes, which, when combined with Proposition 8, yields a proof of Theorem 2 different from the one given by Bateman et al. [2].

If $p = 4p_1 + 1$ with p_1 an odd prime, we will prove (in Section 8) that there are no optimal Vaughan pairs other than the ones that appear in Theorem 17.

Theorem 19. *Let $p \equiv 5 \,(\mathrm{mod}\ 8)$ be a prime such that $(p-1)/4$ is also a prime. Then there are precisely two optimal Vaughan pairs, namely the ones given in Theorem 17. For the top quality $q(p)$ we have*

$$q(p) = q(\{\pm a_p\}; p) = \frac{1}{2}\log\Big(\frac{\sin(\pi a_p/p)}{\sin(\pi/p)}\Big),$$

with a_p as in (11)*.*

In case $p \equiv 5 \,(\mathrm{mod}\ 8)$ and $(p-1)/4$ is a composite number, further optimal Vaughan pairs may occur. We determined all of those for $p < 100$, see Table 4. This analysis is discussed in detail in Section 9 with the help of various tables.

The reader might be more ambitious than the authors and ask for the determination for $\Phi_n(\zeta_m^j)$ for all n, rather than just for the integers n_x. This only seems feasible for small values of m and is discussed in Bzdęga et al. [3] for $m \in \{3, 4, 5, 6, 8, 10, 12\}$.

2. Preliminaries

2.1. **The basic tool.** Our basic tool to evaluate $|\Phi_n(z)|$ in roots of unity z is the following result [3, Theorem 1].

Theorem 20. (Bzdęga et al. [3]). *Let $n, m > 1$ be coprime integers. In the notation of Theorem 5 we have*

$$\log|\Phi_n(\xi_m)| = \frac{1}{\varphi(m)} \sum_{\substack{\chi \in \widehat{G}(m) \\ \chi(-1)=1}} C_\chi(\xi_m)\chi(n)\prod_{q|n}(1 - \overline{\chi}(q)), \tag{13}$$

where the product is over the prime divisors q of n.

If $(j, m) = 1$, then

$$C_\chi(\zeta_m^j) = \chi(j) C_\chi(\zeta_m). \tag{14}$$

To see this, note that

$$C_\chi(\zeta_m^j) = \sum_{g \in G(m)} \overline{\chi}(g) \log(1 - \zeta_m^{jg}) = \chi(j) \sum_{g \in G(m)} \overline{\chi}(jg) \log(1 - \zeta_m^{jg}) = \chi(j) C_\chi(\zeta_m).$$

Thus in some sense it suffices to study $C_\chi(\xi_m)$ in case $\xi_m = \zeta_m$.

When χ is even, which is the only relevant case by (13), there is a more practical formula for $C_\chi(\zeta_m)$.

Proposition 21. *If χ is an even non-principal character, then*

$$C_\chi(\zeta_m) = \sum_{g \in G(m)} \overline{\chi}(g) \log \sin\big(\frac{\pi g}{m}\big).$$

Proof. We have

$$2C_\chi(\zeta_m) = \sum_{g \in G(m)} \overline{\chi}(g) \log(1 - \zeta_m^g) + \sum_{g \in G(m)} \overline{\chi}(-g) \log(1 - \zeta_m^{-g}) = \sum_{g \in G(m)} \overline{\chi}(g) \log|1 - \zeta_m^g|^2,$$

and hence

$$C_\chi(\zeta_m) = \sum_{g \in G(m)} \overline{\chi}(g) \log|1 - \zeta_m^g|. \tag{15}$$

For real α, we have

$$1 - e^{-i\alpha} = e^{-i\alpha/2} 2i \sin(\alpha/2) = 2\sin(\alpha/2) e^{i(\pi-\alpha)/2}.$$

Thus, when $0 < \alpha < 2\pi$, we have

$$\log(1 - e^{-i\alpha}) = \log(2\sin(\alpha/2)) + i(\pi - \alpha)/2$$

for the principal determination of the logarithm. We infer that

$$\log|1 - e^{-i\alpha}| = \log 2 + \log(\sin(\alpha/2)).$$

Inserting this into (15), we obtain

$$C_\chi(\zeta_m) = \sum_{g \in G(m)} \overline{\chi}(g) \log \sin\left(\frac{\pi g}{m}\right) + \log 2 \sum_{g \in G(m)} \overline{\chi}(g).$$

Since the latter sum is zero, the proof is complete. □

Remark 22. The character sums C_χ are related to special values of Dirichlet L-series. Indeed, if χ is a primitive character modulo m and $(j, m) = 1$, then Dirichlet (cf. [16, p. 37]) proved that

$$L(1, \chi) = -\frac{\overline{\chi}(-j)\tau(\chi)}{m} C_\chi(\zeta_m^j),$$

where $\tau(\chi) = \sum_{k=1}^m \chi(k)\zeta_m^k$ is the Gauss sum.

2.2. **Abelian number fields and their character groups.** Let $K/\mathbb{Q}$ be abelian. By the Kronecker-Weber theorem there exists an integer m such that K is a subfield of $\mathbb{Q}(\zeta_m)$. Let H be the subgroup of $G(m)$ which corresponds to K by Galois theory. We let $X(K)$ be the group of all characters which are equal to unity on H. We extend each of these characters first to a Dirichlet character modulo m, and then to a primitive character. As an example, consider the even characters modulo m in $X(\mathbb{Q}(\zeta_m))$. These form a subgroup equal to $X(\mathbb{Q}^+(\zeta_m))$, see, e.g., Narkiewicz [13, Proposition 8.3]. We are interested in the case where $m = p$ is a prime satisfying $p \equiv 1 \,(\mathrm{mod}\ 4)$. The characters that are unity on the subgroup $\{\pm 1, \pm a_p\}$ form a subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$ equal to $X(L_p)$, with $L_p := \mathbb{Q}(\zeta_p + \zeta_p^{a_p} + \zeta_p^{-a_p} + \zeta_p^{-1})$. As an application we obtain the following result.

Lemma 23. *Let $p \equiv 1 \,(\mathrm{mod}\ 4)$ and let a_p be as in* (11). *Let $\mathfrak{S}$ be the S-clan of $\{\pm a_p\}$. Then*

$$\mu_{\mathfrak{S}}(b) := \frac{1}{|\mathfrak{S}|} \sum_{\chi \in \mathfrak{S}} \chi(b) = \begin{cases} 1 & \text{if } b = \pm 1; \\ -1 & \text{if } b = \pm a_p; \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We consider the even characters χ that are not in the S-clan. These satisfy $\chi(a_p) = 1$ and form a group. Let us denote them $\chi_1, \ldots, \chi_{(p-1)/4}$. Their fixed field is L_p, which is of degree $(p-1)/4$. By orthogonality we then have $\sum_{j=1}^{(p-1)/4} \chi_j(b) = (p-1)/4$ if $b \in \{\pm 1, \pm a_p\}$ and zero otherwise. By orthogonality again it follows from this that $\mu_{\mathfrak{S}}(b) = 0$ if $b \notin \{\pm 1, \pm a_p\}$. As clearly $\mu_{\mathfrak{S}}(\pm 1) = 1$ and $\mu_{\mathfrak{S}}(\pm a_p) = -1$, we are done. □

Example 24 ($p = 13$): It is instructive to verify the above argument in this case using Table 2 and the identity $1 + \zeta_3 - \zeta_6 = 0$. The reader might also want to apply Galois theory and write down all subfields. One of them is L_{13}, which is of degree 3 and has minimal polynomial $x^3 + x^2 - 4x + 1$. For details, see, e.g., Narkiewicz [13, pp. 429–430]. For a Hasse diagram of the subfields of $\mathbb{Q}(\zeta_{13})$ see, e.g., Dummit and Foote [7, p. 512].

2.3. **Two simple results involving trigonometric functions.** In our proof of Theorem 17b we will need Lemma 26, the proof of which makes use of the following lemma.

Lemma 25. *Let $b > 1$ be a real number. The function $\sin(bx)/\sin(x)$ is non-increasing for $x \in (0, \frac{\pi}{b})$.*

Proof. The derivative of the function is $F_b(x)/\sin^2 x$, with $F_b(x) = \cos(bx) b \sin x - (\cos x)\sin(bx)$. It suffices to show that $F_b(x) \le 0$ in the interval $(0, \pi/b)$. As $F_b(0) = 0$, it is enough to show $F_b'(x) \le 0$ in the said interval. However, as $F_b'(x) = (1 - b^2)\sin(bx)\sin x$ this is obvious. □

We will use that $\sin x$ is increasing for $x \in (0, \pi/2)$.

Lemma 26. *Let $1 \le a < m/2$ be an integer coprime to m. Then*

$$\max\Big\{ \frac{\sin(\pi \overline{ja}/m)}{\sin(\pi j/m)} : 1 \le j < m,\ (j, m) = 1 \Big\} = \frac{\sin(\pi a/m)}{\sin(\pi/m)},$$

where $\overline{ja}$ denotes the unique number $1 \le j_1 < m$ such that $j_1 \equiv ja \,(\mathrm{mod}\ m)$.

Proof. As the result is trivial for $a = 1$, we may assume that $a \ge 2$. For brevity we will put $m_a = \sin(\pi a/m)/\sin(\pi/m)$. Since clearly the maximum is $\ge m_a \ge 1$, it suffices to consider only those quotients of the form $\sin y/\sin z$ with $y > z$ and so we may assume that $j_1 > j$. Note that $j_1 \le ja$. It now follows by Lemma 25 with $b = j_1/j$ that $\sin(\pi j_1/m)/\sin(\pi j/m) \le \sin(\pi j_1/jm)/\sin(\pi/m)$, which on its turn is bounded above by m_a as $j_1/j \le a < m/2$. □

3. Relevant properties of character tables

The next lemma deals with a special case of Theorem 28.

Lemma 27. *Let $m \geq 3$. Suppose that $(\mathbb{Z}/m\mathbb{Z})^*$ is cyclic. There is an even character modulo m assuming the value -1 if and only if 4 divides $\varphi(m)$.*

Proof. Let g be a generator. The order of the group is $\varphi(m) = n$ is even. Recall that the characters of a cyclic group of order n are given by

$$\chi_k(g^r) = e^{\frac{2\pi i k r}{n}},\ 0 \leq k < n,\ 0 \leq r < n.$$

Put $b = n/2$. On noting that $g^b = -1$, we see that χ_k is even if and only k is even. In case k is even $\chi_k(-1) = \chi_k(g^b) = \chi_k(g)^b = 1$ and so $\chi_k(g)$ is a b-th root of unity. If b is odd, it now follows that $\chi_k(g^r) = \chi_k(g)^r \neq -1$ for every $r \geq 0$. If b is even, trivially $\chi_2(g^{b/2}) = e^{\frac{2\pi i b}{2b}} = -1$. □

For ease of notation we work in the proof of the next theorem with additive notation (and thus if χ is a character of a cyclic group we write $\chi(b)$ for $\chi(g^b)$, with g some fixed generator of the group).

Theorem 28. *There is an even character modulo m assuming the value -1 if and only if 4 divides $\varphi(m)$.*

Proof. For $m \leq 2$ the result is obvious and so we may assume $m \geq 3$. If $(\mathbb{Z}/m\mathbb{Z})^*$ is cyclic we are done by Lemma 27, and so we may assume it is not cyclic. Then

$$(\mathbb{Z}/m\mathbb{Z})^* \cong C(2a_1) \times \cdots \times C(2a_r),\ r \geq 2,$$

is a direct product of at least two cyclic groups of even order and so $4 \mid \varphi(m)$. This follows from the group structure of $(\mathbb{Z}/m\mathbb{Z})^*$ that is determined in many introductory books on algebra or number theory, e.g. in the book by Ireland and Rosen [10, Chapter 4].

To finish the proof we have to show there is an even character assuming the value -1.

The residue class -1 modulo m corresponds with $(a_1, \ldots, a_r)$ and so χ is an even character if and only if $\chi((a_1, \ldots, a_r)) = 1$.

Suppose that one of the a_i's is even, say a_1. Then we can take $\chi = \chi_1 \times \cdots \times \chi_r$ such that $\chi_1(a_1/2) = -1$ and $\chi_i(a_i) = 1$ for all $i \neq 1$. Then $\chi((a_1, \ldots, a_r)) = 1$ and $\chi((a_1/2, \ldots, a_r)) = -1$.

If all a_i's are odd, then take $\chi = \chi_1 \times \cdots \times \chi_r$, such that $\chi_1(a_1) = -1$ and $\chi_2(a_2) = -1$ and $\chi_i(a_i) = 1$ for $i > 2$. Then $\chi((a_1, \ldots, a_r)) = 1$ and $\chi((a_1, 0, a_2, \ldots, a_r)) = -1$. □

Note that Proposition 16 is a corollary of this result.

The next lemma concerns the character table of $(\mathbb{Z}/p\mathbb{Z})^*/\{\pm 1\}$ for certain primes p such as $p = 13$ (cf. Table 2). We return to the usage of multiplicative notation.

Lemma 29. *Let $p \equiv 5 \pmod 8$ be a prime such that $(p-1)/4$ is a prime also, and let a_p be as in (11). Let χ be any even character modulo p and b an integer coprime to p. If $\chi(b) = -1$, then $b \equiv a_p \pmod p$, $b \equiv -a_p \pmod p$ or χ is the Legendre symbol.*

Proof. By assumption $p - 1 = 4q$ with q an odd prime. For every integer $0 \leq k < p-1$ there is a character χ_k satisfying

$$\chi_k(g^j) = e^{\frac{2\pi i}{p-1} jk} = e^{\frac{2\pi i}{4q} jk}.$$

There are no further characters. Since $-1 \equiv g^{2q} \pmod p$, we have $\chi_k(-1) = 1$ iff k is even. It thus suffices to determine when

$$\chi_{2r}(g^j) = e^{\frac{\pi i j r}{q}} = -1, \text{ with } 0 \leq r < 2q,\ 0 \leq j < 4q.$$

Since by assumption q is prime, there are only two cases:
Case 1. $j = q$ or $j = 3q$. Here we note that, modulo p, we have $\{g^q, g^{3q}\} = \{a_p, -a_p\}$.
Case 2. $r = q$. We observe that $\chi_{2q}(g^j) = -1$ iff j is odd, and hence χ_{2q} is the Legendre symbol. □

Remark 30. It is not difficult to show that one can take $g = 2$, that is that 2 is a primitive root for the primes under consideration, see, e.g., the survey [12, p. 1306]. This implies that either $a_p \equiv 2^{(p-1)/4} \pmod{p}$ or $a_p \equiv -2^{(p-1)/4} \pmod{p}$.

4. The proof of Theorem 5

Proof of Theorem 5. First we will establish (7), which we will do by determining the various contributions of the different characters χ to the sum in the right hand side of formula (13). Write $\xi_m = \zeta_m^j$.

If $\chi \in \mathfrak{S}$, then $\prod_{q|n_x}(1 - \overline{\chi}(q)) = 2^{\omega(n_x)} = d(n_x)$, where in the last step we use that n_x is square free. The contribution is $(-1)^{\omega(n_x)} d(n_x) C_\chi(\zeta_m^j)/\varphi(m)$. On adding the various contributions we obtain $(-1)^{\omega(n_x)} d(n_x) q_j(S; m)$.

If $\chi \notin \mathfrak{S}$ and χ is odd, then there is no contribution.

If $\chi \notin \mathfrak{S}$ and χ is even, then $\chi(s) \neq -1$ for some element s of S and putting $r = |1-\overline{\chi}(s)|/2$, we obtain

$$2^{\omega(n_x)} \big|\chi(n_x) \prod_{\substack{q|n_x \\ q\equiv s \ (\mathrm{mod}\ p)}} \frac{(1-\overline{\chi}(s))}{2}\big| \le 2^{\omega(n_x)} r^{\pi(x;p,s)}, \tag{16}$$

where $\pi(x; p, s)$ denotes the number of primes $q \le x$ such that $q \equiv s \pmod{p}$. Since we have $|1 - \overline{\chi}(s)| < 2$, it follows by Dirichlet's theorem on primes in arithmetic progression that $r^{\pi(x;p,s)}$ tends to zero as x tends to infinity, and hence the contribution of χ is $o(2^{\omega(n_x)})$.

Next we establish the estimate (9). It immediately follows from the estimates (7) in case $\omega(n_x)$ is even. In case $\omega(n_x)$ is odd, it follows if we show that

$$q(S; m) = \max\{-q_j(S; m) : 1 \le j \le m,\ (j, m) = 1\}.$$

We claim that

$$\{-q_j(S; m) : 1 \le j \le m,\ (j, m) = 1\} = \{q_j(S; m) : 1 \le j \le m,\ (j, m) = 1\}. \tag{17}$$

Let j be as in (17). By (14) we see that $\varphi(m)q_j(S; m) = \sum_{\chi\in\mathfrak{S}} C_\chi(\zeta_m^j) = \sum_{\chi\in\mathfrak{S}} \chi(j)C_\chi(\zeta_m)$. If k is any element in S, then

$$\varphi(m)q_{jk}(S; m) = \sum_{\chi\in\mathfrak{S}} C_\chi(\zeta_m^{jk}) = \sum_{\chi\in\mathfrak{S}} \chi(jk)C_\chi(\zeta_m) = -\sum_{\chi\in\mathfrak{S}} C_\chi(\zeta_m^j) = -q_j(S; m)\varphi(m),$$

since $\chi(k) = -1$ for every χ in $\mathfrak{S}$. It follows that $q_{k_1}(S; m) = -q_j(S; m)$ with $1 \le k_1 < m$ such that $k_1 \equiv jk \pmod{m}$. □

5. The proof of Theorem 9

Proof of Theorem 9. Put $\delta = |S|/\varphi(m)$. By two equivalent versions of the prime number theorem for arithmetic progressions we have

$$\log n_x = \sum_{p\le x,\ p\in P_S} = \delta x\,(1 + O(\log^{-2} x)), \tag{18}$$

respectively

$$\omega(n_x) = \sum_{p\le x,\ p\in P_S} = \delta\frac{x}{\log x} + \delta\frac{x}{\log^2 x} + O\big(\frac{x}{\log^3 x}\big). \tag{19}$$

It follows from (18) that $\log x = O(\log\log n_x)$ and more precisely that $\log x = \log\log n_x - \log\delta + O((\log\log n_x)^{-2})$. Combining the various estimates we infer that

$$\omega(n_x) = \frac{\log n_x}{\log\log n_x}\Big(1 + \frac{1+\log\delta}{\log\log n_x} + O\Big(\frac{1}{(\log\log n_x)^2}\Big)\Big), \tag{20}$$

as x (and hence n_x) tends to infinity. The implied error terms depend at most on $(S; m)$. Moreover, since for fixed m there are only finitely many choices for S, the implied error term depends at most on m.

The proof is now completed on noting that $d(n_x) = 2^{\omega(n_x)}$ and invoking Proposition 8. □

6. The proof of Theorem 17

The proof of part a will make use of a beautiful result from the 19th century.

Lemma 31. *Let $p \equiv 1 \pmod 4$ be a prime. Then*

$$\prod_{k=1}^{p-1}\Big(1-\zeta_p^k\Big)^{-(\frac{k}{p})} = e^{\sqrt{p}L(1,\chi_1)} = \epsilon_p^{2h_p},$$

where χ_1 denotes the Legendre symbol, ϵ_p is the fundamental unit of the quadratic number field $\mathbb{Q}(\sqrt{p})$ and h_p its class number.

Chowla and Mordell [4], reproduced in Narkiewicz [14, pp. 84-85], gave a beautiful elementary proof of the first identity in Lemma 31. They go on to infer that the product is $\neq 1$ and hence that $L(1,\chi_1)$ does not vanish, a crucial fact in the proof of Dirichlet's prime number theorem for the arithmetic progressions modulo p.

The second identity is a consequence of Dirichlet's class number formula

$$L\big(1,\chi_1\big) = \frac{2h_p\log\epsilon_p}{\sqrt{p}}, \tag{21}$$

cf. Lang [11, Theorem 5.2, p. 87] or Washington [16, Exercise 4.6].

Remark 32. Vaughan works with $\log\alpha = \sqrt{5}L(1,\chi_1)/4$ in (4). By (21) with $p = 5$ we see that $\alpha = \sqrt{\tau}$, see [8, p. 193] for a direct derivation.

Remark 33. (Refined version of Lemma 31.) Let $p \equiv 1 \pmod 4$ be a prime. Then we have

$$\prod_{k=1}^{(p-1)/2}\sin\Big(\frac{\pi k}{p}\Big)^{-(\frac{k}{p})} = \prod_{k=1}^{(p-1)/2}\Big(1-\zeta_p^k\Big)^{-(\frac{k}{p})} = e^{\sqrt{p}L(1,\chi_1)/2} = \epsilon_p^{h_p}. \tag{22}$$

This yields, e.g., $\sin(\pi 2/5)/\sin(\pi/5) = \tau$. Note that (22) implies Lemma 31. The product is easily seen to be a quadratic unit of norm -1. The identity then implies that ϵ_p has norm -1 and h_p is odd. See the book [9] for proofs.

The proof of part (b) will make use of a more explicit formula for $q_j(S; m)$, namely (23) below.

Lemma 34. *Let $(S;m)$ be a Vaughan pair having $\mathfrak{G}$ as S-clan. Let j be coprime with m. We have*

$$q_j(S,m)=\frac{|\mathfrak{G}|}{\varphi(m)}\prod_{g\in G(m)}\mu_{\mathfrak{G}}(g)\log(1-\zeta_m^{jg}),$$

where

$$\mu_{\mathfrak{G}}(g)=\frac{1}{|\mathfrak{G}|}\sum_{\chi\in\mathfrak{G}}\overline{\chi}(g).$$

Alternatively, we can write

$$q_j(S;m)=\frac{|\mathfrak{G}|}{\varphi(m)}\prod_{g\in G(m)}\mu_{\mathfrak{G}}(g/j)\log\sin\Big(\frac{\pi g}{m}\Big). \tag{23}$$

Proof. The first claim follows on inserting the expression (6) for C_χ in (8) and swapping the order of summation.

It follows from Proposition 21 and $C_\chi(\zeta_m^j)=\chi(j)C_\chi(\zeta_m)$ that

$$C_\chi(\zeta_m^j)=\sum_{g\in G(m)}\overline{\chi}(g/j)\log\sin\Big(\frac{\pi g}{m}\Big).$$

On inserting this in (8) and swapping the order of summation, the proof is concluded. □

The proof of Theorem 17. a) Recall that if χ is a non-trivial character, then $\sum_{b=1}^{p-1}\chi(b)=0$ by character orthogonality. It follows from this and $|\chi|\le 1$, that if $\chi(a)=-1$ for every quadratic non-residue a modulo p, then $\chi(a)=1$ for every quadratic residue a, and so χ must be the Legendre symbol χ_1. Since $\chi_1(-1)=\big(\frac{-1}{p}\big)=(-1)^{(p-1)/2}=1$, χ_1 is an even character. We conclude that the S-clan consists only of χ_1 if $S=N$. As N is the maximum set on which χ_1 assumes the value -1, it is clear that $(N;p)$ is an optimal Vaughan pair.

By Theorem 5 we have

$$(p-1)q_j(N;p)=\sum_{b=1}^{p-1}\overline{\chi}_1(b)\log(1-\zeta_p^{bj})=\chi_1(j)\sum_{b=1}^{p-1}\overline{\chi}_1(bj)\log(1-\zeta_p^{bj})=-\chi_1(j)\sqrt{p}\,L(1,\chi_1),$$

where the final identity is a consequence of Lemma 31. It now follows from (8) that

$$q(N;p)=\max\{-\sqrt{p}\,L(1,\chi_1)/(p-1),\sqrt{p}\,L(1,\chi_1)/(p-1)\}=\sqrt{p}\,L(1,\chi_1)/(p-1),$$

as $L(1,\chi_1)>0$.

b) Put $S=\{\pm a_p\}$. If χ is any even character, then $\chi(a_p)^2=\chi(a_p^2)=\chi(-1)=1$ and so $\chi(a_p)\in\{-1,1\}$. As $a_p\ne\pm1$, there is at least one even character χ such that $\chi(a_p)=-1$. By orthogonality, we then have precisely $(p-1)/4$ even characters satisfying $\chi(a_p)=-1$. Let us denote them $\chi_1,\ldots,\chi_{(p-1)/4}$. Now suppose that $(S;p)$ is not optimal. This implies that there is $b\ne\pm a_p$ such that $S\cup\{\pm b\}$ has a clan consisting of $\chi_1,\ldots,\chi_{(p-1)/4}$. We then must have $\chi_1(b)=\ldots=\chi_{(p-1)/4}(b)=-1$. We infer that $\chi(ba_p)=1$ for all even characters. This implies $ba_p\equiv\pm1\ (\mathrm{mod}\ p)$, contradicting our assumption that $b\ne\pm a_p$. We conclude that $(S;p)$ is an optimal Vaughan pair.

Combination of (23) with Lemma 23 yields

$$q_j(S;p)=\frac{1}{2}\log\Big(\frac{\sin(\pi j/p)}{\sin(\pi\overline{ja_p}/p)}\Big),$$

with $\overline{ja_p}$ denoting the unique number $1 \le j_1 < p$ such that $j_1 \equiv ja_p \,(\mathrm{mod}\ p)$. We have to show that

$$q(S;p) = \max\{q_1(S;p), \ldots, q_{p-1}(S;p)\} = \frac{1}{2}\log\Big(\frac{\sin(\pi a_p/p)}{\sin(\pi/p)}\Big).$$

By (17) and the monotonicity of the logarithm, we see that it suffices to show that

$$\max\Big\{\frac{\sin(\pi\overline{ja_p}/p)}{\sin(\pi j/p)} : 1 \le j < p\Big\} = \frac{\sin(\pi a_p/p)}{\sin(\pi/p)}.$$

That the latter identity holds is a consequence of Lemma 26. □

Remark 35. An alternative proof of part (a) can be given on using Proposition 21 and (22). The details are left to the interested reader.

7. Proof of Proposition 18

Proof. a) We only consider primes $p \equiv 1 \,(\mathrm{mod}\ 4)$, and let a_p be as in (11). We use the formula for $q(\{\pm a_p\};p)$ given in Theorem 17b. The upper bound in (12) follows on noting that $\sin x \sim x$ as x tends to zero and the trivial estimate $\sin x \le 1$.

Since $a_p \ge \sqrt{p-1}$, we find that $\sin(\pi a_p/p) \ge \pi e^{-2\epsilon}/\sqrt{p}$ for all p large enough. On noting that $1/\sin(\pi/p) \ge p/\pi$, it then follows that $q(\{\pm a_p\};p) > \frac{1}{4}\log p - \epsilon$ for every p large enough.

Duke et al. [6] proved that if f is a quadratic polynomial with complex roots, then for $0 \le \alpha < \beta \le 1$ we have

$$|\{(p,\nu) : p \le x,\ f(\nu) \equiv 0 \,(\mathrm{mod}\ p),\ \alpha \le \frac{\nu}{p} < \beta\}| \sim (\beta - \alpha)\pi(x), \tag{24}$$

where $\pi(x)$ denotes the number of primes $p \le x$. Choose $0 < \delta < 1$ such that $\sin(\frac{\pi}{2}\delta) \ge e^{-2\epsilon}$. By (24) with $f(X) = X^2 + 1$ we have for a positive fraction of primes p that $\delta p/2 < a_p < p/2$. For each of those primes p we have $\sin(\frac{\pi a_p}{p}) > \sin(\frac{\pi}{2}\delta) \ge e^{-2\epsilon}$ and therefore $q(\{\pm a_p\};p) > \frac{1}{2}\log(p/\pi) - \epsilon$.

b) By Theorem 17 we have $q(N;p) = \frac{\sqrt{p}}{p-1}L\big(1,\chi_1\big)$. Since $\epsilon_{17} = 4 + \sqrt{17}$ and $h_{17} = 1$ we obtain by (21) the claimed formula for $q(N;17)$. Using the easy estimate $L(1,\chi) \le 2 + \log p$, cf. Narkiewicz [13, Lemma 8.5], we conclude that $q(N;p) < 1.0003p^{-1/2}(2 + \log p)$ for $p \ge 4177$. As the right hand side is non-increasing for $p \ge e^2$, we infer that $q(N;p) \le q(N;4177) < 0.16$ for $p \ge 4177$. The proof of part b is finished by direct computation of $q(N;p)$ for the remaining primes $p \equiv 1 \,(\mathrm{mod}\ 4)$.

c) Using the sine inequality $\frac{2}{\pi}x \le \sin(x) \le x$ valid for $0 < x < \pi/2$, and observing that $a_p \ge \sqrt{p-1}$, we obtain $q(\{\pm a_p\};p) > \frac{1}{2}\log\big(\frac{2}{\pi}\sqrt{p-1}\big)$. The latter quantity is > 0.39 for $p \ge 13$. Combining this information with part b and Table 3, part c follows. □

8. Proof of Theorem 19

Lemma 29 says that if there is an -1 assumed by an even character, then that character is the Legendre symbol or the -1 is in the $\pm a_p$ column, cf. Table 2.

Let $(S;p)$ be an optimal Vaughan pair. Since $(\{\pm a_p\},p)$ is an optimal Vaughan pair by Theorem 17b, we may assume that S contains an element $b \ne \pm a_p$. We claim that $S = N$, the set of non-residues modulo p. Note that we must have $\big(\frac{b}{p}\big) = -1$. As there is no further even character χ satisfying $\chi(\pm b) = -1$, the S-clan only contains the Legendre symbol. The same will hold true if S contains all elements s for which $\big(\frac{s}{p}\big) = -1$, that is if $S = N$. By Theorem 17a the Vaughan pair $(N;p)$ is optimal.

It is a consequence of Proposition 18c and Theorem 17b that

$$q(p) = \max\{q(\{\pm a_p\};p), q(N;p)\} = q(\{\pm a_p\};p) = \frac{1}{2}\log\Big(\frac{\sin(\pi a_p/p)}{\sin(\pi/p)}\Big).$$

9. Further optimal Vaughan pairs with $p < 100$

In this section we determine all Vaughan pairs $(S;p)$ with $p < 100$ that are not covered by Theorem 17, which we call *non-standard*. They are recorded in Table 4.

The smallest example occurs for $p = 17$. From Table 5 one sees that there is one non-standard optimal Vaughan pair. It has $S = \{\pm 2, \pm 8\}$ and S-clan $\{\chi_3, \chi_7\}$.

Table 4. Further optimal Vaughan pairs with $p \le 100$

p	$\lvert\mathfrak{S}\rvert$	S
17	2	$2, 8$
37	3	$6, 8, 14$
41	5	$3, 14$
41	2	$2, 5, 8, 9, 20$
61	5	$11, 21, 29$
61	3	$8, 11, 23, 24, 28$
73	9	$10, 22$
73	6	$3, 24, 27$
73	3	$7, 10, 17, 21, 22, 30$
73	2	$3, 6, 12, 19, 23, 24, 25, 27, 35$
89	11	$12, 37$
89	2	$5, 9, 10, 17, 18, 20, 21, 34, 36, 40, 42$
97	12	$33, 47$
97	8	$6, 16, 22$
97	6	$8, 12, 18, 27$
97	4	$4, 9, 24, 33, 43, 47$
97	3	$19, 20, 28, 30, 34, 42, 45, 46$
97	2	$2, 3, 8, 11, 12, 18, 25, 27, 31, 32, 44, 48$

For readability and compactness we write a, rather than $\pm a$ in Table 4.

Table 5. Even characters modulo 17 (with $\omega = e^{\pi i/4}$)

χ	± 1	± 2	± 3	± 4	± 5	± 6	± 7	± 8
χ_1	1	1	1	1	1	1	1	1
χ_2	1	$-i$	ω	-1	$-\omega$	$-\omega^3$	ω^3	i
χ_3	1	-1	i	1	i	$-i$	$-i$	-1
χ_4	1	i	ω^3	-1	$-\omega^3$	$-\omega$	ω	$-i$
χ_5	1	1	-1	1	-1	-1	-1	1
χ_6	1	$-i$	$-\omega$	-1	ω	ω^3	$-\omega^3$	i
χ_7	1	-1	$-i$	1	$-i$	i	i	-1
χ_8	1	i	$-\omega^3$	-1	ω^3	ω	$-\omega$	$-i$

Table 6. Part of even character table modulo 37 (with $\omega = e^{\pi i/9}$)

χ	± 2	± 5	± 6	± 8	± 13	± 14	± 15	± 17	± 18
χ_1	ω	ω^5	-1	ω^3	$-\omega^2$	$-\omega^6$	$-\omega^4$	ω^7	$-\omega^8$
χ_2	ω^3	$-\omega^6$	-1	-1	$-\omega^6$	-1	ω^3	ω^3	$-\omega^6$
χ_3	ω^5	ω^7	-1	$-\omega^6$	ω	ω^3	$-\omega^2$	$-\omega^8$	$-\omega^4$
χ_4	ω^7	$-\omega^8$	-1	ω^3	ω^5	$-\omega^6$	ω	$-\omega^4$	$-\omega^2$
χ_5	-1	-1	-1	-1	-1	-1	-1	-1	-1
χ_6	$-\omega^2$	ω	-1	$-\omega^6$	$-\omega^4$	ω^3	$-\omega^8$	ω^5	ω^7
χ_7	$-\omega^4$	$-\omega^2$	-1	ω^3	$-\omega^8$	$-\omega^6$	ω^7	ω	ω^5
χ_8	$-\omega^6$	ω^3	-1	-1	ω^3	-1	$-\omega^6$	$-\omega^6$	ω^3
χ_9	$-\omega^8$	$-\omega^4$	-1	$-\omega^6$	ω^7	ω^3	ω^5	$-\omega^2$	ω

For the next case, $p = 37$, we deleted the rows and columns not having a -1 in the table of even characters, leading to Table 6. Note that there is one non-standard optimal Vaughan pair, namely $(\{\pm 6, \pm 8, \pm 14\}; 37)$. In fact, that table contains more information than we need in order to determine the non-standard optimal Vaughan pairs for $p = 37$. All that matters are the entries that are -1. Also the columns having only one -1 can be deleted. These only contribute to the standard Vaughan pair with S the set of non-residues. Taking these remarks into account we can then consider the next two cases: $p = 41$ and $p = 61$ (see Tables 7, respectively 8). These tables together with consideration of what happens for the next three primes $73, 89$ and 97 (not tabulated here), suggest that the following is true.

Conjecture 36. *Let $p \equiv 1 \pmod 4$ be a prime. Then for every divisor d of $(p-1)/4$, there is a unique optimal Vaughan pair $(S; p)$ with S having cardinality $2d$ and S-clan having $\frac{p-1}{4d}$ characters. These are the only optimal Vaughan pairs.*

As for $p \equiv 3 \pmod 4$ there are no Vaughan pairs, this conjecture would give a *complete classification* of all optimal Vaughan pairs for prime modulus.

The number $(p-1)/4$ has always the divisors 1 and $(p-1)/4$, corresponding to the optimal Vaughan pairs $(\{\pm a_p\}; p)$, respectively $(N; p)$. In case $(p-1)/4$ is a prime, there are no further divisors and the conjecture claims that these are all the optimal Vaughan pairs. By Theorem 19 this is true.

In a sequel to this paper, we hope to make progress on establishing this conjecture and to address the issue of computing the qualities of the non-standard pairs in a systematic way. Preliminary work suggests the following conjecture.

Conjecture 37. *Let p be a prime number. If $(S; p)$ is a Vaughan pair, then its quality $q(S; p)$ is positive.*

Table 7. Relevant part of even character table modulo 41

χ	±2	±3	±5	±8	±9	±14	±20
χ_1					-1		
χ_2		-1				-1	
χ_3					-1		
χ_4	-1		-1	-1	-1		-1
χ_5		-1				-1	
χ_6					-1		
χ_7					-1		
χ_8		-1				-1	
χ_9					-1		
χ_{10}					-1		
χ_{11}		-1				-1	
χ_{12}	-1		-1	-1	-1		-1
χ_{13}					-1		
χ_{14}		-1				-1	
χ_{15}					-1		

Table 8. Relevant part of even character table modulo 61

χ	±8	±11	±21	±23	±24	±28	±29
χ_1		-1					
χ_2		-1	-1				-1
χ_3	-1	-1		-1	-1	-1	
χ_4		-1					
χ_5		-1	-1				-1
χ_6		-1					
χ_7		-1					
χ_8	-1	-1	-1	-1	-1	-1	-1
χ_9		-1					
χ_{10}		-1					
χ_{11}		-1	-1				-1
χ_{12}		-1					
χ_{13}	-1	-1		-1	-1	-1	
χ_{14}		-1	-1				-1
χ_{15}		-1					

`Acknowledgement.` Part of the work on this paper was done during two research stays, namely of the first author at the Max Planck Institute for Mathematics in June 2018 and of the second author at the University of North Carolina in Wilmington in September 2019. We thank both institutions for their support and hospitality. The first author, in addition, acknowledges support by the Cahill Grant. The paper was finalized during lockdown in early 2020. We thank Bartłomiej Bzdęga, Alexandru Ciolan, Andrés Herrera-Poyatos and Florian Luca for helpful correspondence and Alessandro Languasco for numerically computing $L(1,\chi)$ for us. The character tables in this paper were produced using the online Dirichlet character table generator [5].

References

[1] P.T. Bateman, Note on the coefficients of the cyclotomic polynomial, *Bull. Am. Math. Soc.* **55** (1949), 1180–1181.

[2] P.T. Bateman, C. Pomerance and R.C. Vaughan, On the size of the coefficients of the cyclotomic polynomial, in: *Topics in classical number theory*, Vol. I, II (Budapest, 1981), 171–202, Colloq. Math. Soc. János Bolyai, 34, North-Holland, Amsterdam, 1984.

[3] B. Bzdęga, A. Herrera-Poyatos and P. Moree, Cyclotomic polynomials at roots of unity, *Acta Arith.* **184** (2018), 215–230.

[4] S. Chowla and L.J. Mordell, Note on the nonvanishing of $L(1)$, *Proc. Amer. Math. Soc.* **12** (1961), 283–284.

[5] Dirichlet character table generator, `https://www.di-mgt.com.au/cgi-bin/dirichlet.cgi`

[6] W. Duke, J.B. Friedlander and H. Iwaniec, Equidistribution of roots of a quadratic congruence to prime moduli, *Ann. of Math.* (2) **141** (1995), 423–441.

[7] D.S. Dummit and R.M. Foote, *Abstract algebra*, Prentice Hall, Inc., Englewood Cliffs, NJ, 1991.

[8] H.M. Edwards, *Fermat's last theorem. A genetic introduction to algebraic number theory*, Graduate Texts in Mathematics **50**, Springer-Verlag, New York-Berlin, 1977.

[9] A. Fröhlich and M.J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics **27**, Cambridge University Press, Cambridge, 1993.

[10] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Second edition, Graduate Texts in Mathematics **84**, Springer-Verlag, New York, 1990.

[11] S. Lang, *Cyclotomic fields I and II*, Combined second edition, With an appendix by Karl Rubin, Graduate Texts in Mathematics **121**, Springer-Verlag in Mathematics, New York, 1990.

[12] P. Moree, Artin's primitive root conjecture – a survey, *Integers* **12A** (2012), No. 6, 1305–1416.

[13] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Second edition, Springer-Verlag, Berlin; PWN—Polish Scientific Publishers, Warsaw, 1990.

[14] W. Narkiewicz, *The development of prime number theory. From Euclid to Hardy and Littlewood*, Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000.

[15] R.C. Vaughan, Bounds for the coefficients of cyclotomic polynomials, *Michigan Math. J.* 21 (1975), 289–295.

[16] L.C. Washington, *Introduction to cyclotomic fields*, Second edition, Graduate Texts in Mathematics **83**, Springer-Verlag, New York, 1997.

Lilit Martirosyan

University of North Carolina, Wilmington, Department of Mathematics and Statistics, 601 South College Road, Wilmington, NC 28403-5970.

e-mail: `martirosyanl@uncw.edu`

Pieter Moree

Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany.

e-mail: `moree@mpim-bonn.mpg.de`