HYBRID BOUNDS FOR PRIME DIVISORS

Gustav Kjærbye Bagger
School of Science, UNSW Canberra, Australia
g.bagger@unsw.edu.au

Received: 8/10/25, Revised: 1/7/26, Accepted: 7/7/26, Published: 7/29/26

Abstract

Let x and n be positive integers. We prove a non-trivial lower bound for x, dependant only on ω_n, the number of distinct prime factors of x^n-1. By considering the divisibility of $p \mid x^n-1$ for $p \mid n$, we obtain a further refinement. This bound has applications for existence problems relating to primitive elements in finite fields.

1. Introduction

Consider the following problem. Given only the number ω_n of distinct prime factors of x^n-1, what lower bound can one give for x? One might bound x via

$$x^n-1 \geq \prod_{i=1}^{\omega_n} s_i \quad \text{implying} \quad x \geq \left(1+\prod_{i=1}^{\omega_n} s_i\right)^{1/n}. \tag{1}$$

where s_i denotes the i^{th} prime. Here and throughout, let $\mathbb{P}$ denote the set of all rational primes and refer to the bound appearing in Equation (1) as the *trivial bound* on x. In 2022, Booker, Cohen, Leong and Trudgian [1] considered the problem of finding elements with prescribed traces in certain $\mathbb{F}_q$ extensions. For $n=3$ or 5 and q a prime power, they proved a hybrid bound for q in terms of certain residue classes. This paper generalizes their approach and extends the hybrid bound to any positive integers n and x. We prove the following bound.

Theorem 1. (Hybrid bound) *Let $n=\prod_{i=1}^{m} p_i^{a_i}$, $x \in \mathbb{Z}_{>1}$ and $k_i \in \mathbb{Z}^+$. Then*

$$x \geq min\left\{ max\left\{ \left(1+\prod_{j=0}^{t} \prod_{\substack{i=1 \\ r_{i,j} \in \Pi_n^j}}^{k_j} r_{i,j} \right)^{T(t)} : t \in [0,m] \right\} : \sum_{s=0}^{m} k_s = \omega_n \right\},$$

where $\Pi_n^j = \{\rho \in \mathbb{P} : \rho \equiv 1 \mod p_j$ and $\rho \not\equiv 1 \mod p_m, ..., p_{j+1}\}$ for $j \in \{0,...,m\}$, $p_0 := 1$, $T(t) = \prod_{k=1}^{t} p_k^{-a_k}$, and $r_{i,j}$ denotes the i^{th} element of Π_n^j.

DOI: 10.5281/zenodo.21678328

To emphasize the improvement Theorem 1 provides over the trivial bound (1), consider the case where $n = 3$ and $\omega_3 = 10$. Here, the trivial bound gives

$$x^3 - 1 \geq \prod_{i=1}^{10} s_i,$$

implying $x \geq 1864$. In contrast, Theorem 1 takes into account the factorization $x^3 - 1 = (x-1)(x^2+x+1)$ in $\mathbb{Z}[x]$ and the fact that any prime divisor $\rho \mid x^2+x+1$ satisfies $\rho \equiv 0, 1 \mod 3$. Thus, either ρ is in a restricted congruence class or $\rho \mid x - 1$ and we call Theorem 1 a *hybrid bound* since it is balances bounding $x - 1$ and $x^n - 1$ simultaneously. Playing these criteria on ρ off against each other results in the bound $x \geq 3032$, a 63% improvement over Equation (1).

Based on calculations, for fixed $n \neq 2^a$, the hybrid bound is expected to outperform the trivial bound at an ever increasing rate as $\omega_n \to \infty$. For fixed ω_n and varying n, calculations also support the assertion that the largest relative improvement is obtained when n is prime. In 2010, Cohen [2] considered the problem of finding primitive elements on certain lines in $\mathbb{F}_{q^n}$ for small n. In the special case where $n = 4$ and q is a prime power, Cohen noted that q being odd implies $2^4 \mid q^4 - 1$. It follows that one obtains an improvement over Equation (1):

$$q \equiv 1 \mod 2 \quad \text{implies} \quad q \geq \left(1 + 8 \prod_{i=1}^{\omega_n} s_i\right)^{1/4}.$$

This result is suggestive of additional structure arising from special factors $p \mid x^n - 1$, governed by the factors $p \mid n$. This paper generalizes Cohen's approach to any positive integers n and x, obtaining a refinement over the hybrid bound.

Theorem 2. (Ramified bound) *Let $n = \prod_{i=1}^{m} p_i^{a_i}$, $x \in \mathbb{Z}_{>1}$ and $k_i \in \mathbb{Z}^+$. For any distinguished prime factor p_α of n, we have*

$$x \geq min\left\{ max\left\{ \left(1 + \prod_{j=0}^{t} \delta_\alpha(j) \prod_{\substack{i=1 \\ r_{i,j} \in \Pi_n^j}}^{k_j} r_{i,j} \right)^{T(t)} : t \in [0, m] \right\} : \sum_{s=0}^{m} k_s = \omega_n \right\},$$

where $T(t) = \prod_{k=1}^{t} p_k^{-a_k}$ and $\delta_\alpha(j)$ is defined as

$$\delta_\alpha(j) = \begin{cases} p_\alpha / r_{k_\tau, \tau} & j = \tau \text{ and } k_\tau < b \\ p_\alpha^{a_\alpha} & j = \alpha \\ 1 & \textit{elsewhere} \end{cases} \qquad \textit{for } p_\alpha \mid x^n - 1$$

$$\delta_\alpha(j) = \begin{cases} r_{k_\tau + 1, \tau} / p_\alpha & j = \tau \text{ and } k_\tau \geq b \\ 1 & \textit{elsewhere} \end{cases} \qquad \textit{for } p_\alpha \nmid x^n - 1.$$

Here, we take τ such that $p_\alpha \in \Pi_n^\tau$ and b such that $p_\alpha = r_{b,\tau}$.

Returning to the example where $n = 3$ and $\omega_3 = 10$, Theorem 2 gives:

$$x \geq B = \begin{cases} 4387 & \text{for} \quad 3 \mid x^3 - 1 \\ 5423 & \text{for} \quad 3 \nmid x^3 - 1 \end{cases}.$$

In both divisibility cases, we obtain a significant improvement over both the hybrid and trivial bounds. In the special case where $n = 2^a$ for some $a \in \mathbb{Z}^+$, the hybrid bound collapses down to the trivial bound. In this setting, we instead prove a modified version of the ramified bound.

Theorem 3. *Let $x, a \in \mathbb{Z}^+$ and $n = 2^a$. Then, we have*

$$x \geq min\left\{ \left(1 + 2n \cdot \prod_{i=1}^{\omega_n} s_i\right)^{1/n}, \left(1 + \prod_{i=2}^{\omega_n+1} s_i\right)^{1/n} \right\}.$$

If we consider $n = 8$ and $\omega_8 = 20$, then Equation (1) gives the bound $x \geq 2205$. In contrast, Theorem 3 results in the bound $x \geq 3118$, a 41% improvement. For fixed $n = 2^a$ and ω_n sufficiently large, Theorem 3 outperforms the trivial bound by a factor of $(2n)^{1/n}$. We call Theorem 2 a *ramified bound* due to the following observation: when viewing a prime $p \in \mathbb{P}$ as a prime ideal $\mathfrak{p} = \langle p \rangle \trianglelefteq \mathbb{Z}$, we have

$$\mathfrak{p} \text{ ramifies across } \mathbb{Q}(e^{2\pi i/n})/\mathbb{Q} \text{ if and only if } p \mid n.$$

See Washington [11, p. 10] for a proof of this fact. Similarly, the hybrid bound can be thought of as stratifying the potential prime factors of $x^n - 1$ by splitting type, when viewed as prime ideals, in various intermediate extensions

$$\mathbb{Q}(e^{2\pi i/n}) \supseteq K \supseteq \mathbb{Q}.$$

Indeed, Π_n^j contains precisely those primes p which split completely in the cyclotomic extension $\mathbb{Q}(e^{2\pi i/p_j})/\mathbb{Q}$, but not in any of $\mathbb{Q}(e^{2\pi i/p_k})/\mathbb{Q}$ for $j+1 \leq k \leq m$. This follows from cyclotomic reciprocity [11, p. 14]:

$$p \text{ splits completely over } \mathbb{Q}(e^{2\pi i/n})/\mathbb{Q} \text{ if and only if } p \equiv 1 \mod n.$$

Bounds dependant on ω_n have applications to numerous existence results concerning primitive elements in $\mathbb{F}_q$ extensions. By applying our hybrid bounds, we can often obtain immediate improvements over previous known results. We discuss two such applications in detail: Cohen's line problem [2] and Liao, Li and Pu's primitive elements sum problem [7]. In general, sieves reliant on ω_n are natural settings for these hybrid bounds. See for example Lemos, Neumann and Ribas [6], Rani et al. [8], Sharma [10] and [9], or Kapetanakis et al. [4].

The outline of this paper is as follows. In Section 2, we develop some elementary lemmas. In Section 3, we utilize the lemmas to prove the hybrid and ramified bounds in the setting where n is prime. In Section 4, we extend the lemmas to composite n and via a cyclotomic factorization of $x^n - 1$ in $\mathbb{Z}[x]$. The proof of Theorem 1 will follow from these observations. In Section 5 we prove Theorem 2 and Theorem 3. In Section 6, we conclude with applications to finite field theory.

2. Preliminaries

Throughout this section, we assume that $n = p$ for some $p \in \mathbb{P}$. This will provide the base case for the general construction. Denote the k^{th} cyclotomic polynomial by $\Phi_k(x)$ and recall that $\Phi_p(x) = \sum_{i=0}^{p-1} x^i$ in $\mathbb{Z}[x]$. We have the $\mathbb{Z}[x]$-factorization

$$x^p - 1 = \prod_{d|p} \Phi_d(x) = \Phi_1(x)\Phi_p(x) = (x-1)\Phi_p(x).$$

Our aim will be to classify the prime divisors of $x^p - 1$ in terms of the divisors of $x - 1$ and $\Phi_p(x)$. To that end, we have the following result.

Lemma 1. *Let $\rho, p \in \mathbb{P}$ and $x \in \mathbb{Z}^+$. If $\rho \mid x - 1$ and $\rho \mid \Phi_p(x)$, then $\rho = p$.*

Proof. If $\rho \mid x - 1$ then $x \equiv 1 \mod \rho$. Thus $0 \equiv \Phi_p(x) \equiv \Phi_p(1) \equiv p \mod \rho$. Then $\rho \mid p$, implying $\rho = p$, as required. □

Thus, apart from potential twice-divisibility by ρ, no other prime factor divides both $x - 1$ and $\Phi_p(x)$. In fact, if p divides $x^p - 1$, then p^2 divides $x^p - 1$. This follows from the result below.

Lemma 2. *Let $p \in \mathbb{P}$ and $x \in \mathbb{Z}^+$. Then $p \mid x^p - 1$ if and only if $p \mid x - 1$ and $p \mid \Phi_p(x)$.*

Proof. We have $p \mid x^p - 1$ if and only if $x^p - 1 \equiv 0 \mod p$. By Fermat's little theorem, we have $0 \equiv x^p - x \equiv 1 - x \mod p$, implying $p \mid x - 1$. Therefore, we have $\Phi_p(x) \equiv \Phi_p(1) \equiv p \equiv 0 \mod p$, as required. The reverse implication follows trivially from the factorization of $x^p - 1$ in $\mathbb{Z}[x]$. □

A priori, it is not clear why it should be advantageous to factor $x^p - 1$ in $\mathbb{Z}[x]$ in this way. In order to leverage this form, we require a necessary condition for divisibility of $\Phi_p(x)$.

Proposition 1. *Let $\rho, p \in \mathbb{P}$ with $\rho \neq p$ and $x \in \mathbb{Z}^+$. Then, $\rho \mid \Phi_p(x)$ implies that $\rho \equiv 1 \mod p$.*

Proof. Assume $\rho \mid \Phi_p(x)$. By Lemma 1, p cannot divide $x - 1$ since this would imply $\rho = p$, a contradiction. Indeed $x^p - 1 = (x-1)\Phi_p(x) \equiv 0 \mod \rho$ implies $x^p \equiv 1 \mod \rho$. Then, the multiplicative order of x in $(\mathbb{Z}/\rho\mathbb{Z})^\times$ divides p, implying $\operatorname{ord}(x) \in \{1, p\}$. If $\operatorname{ord}(x) = 1$, then $\rho \mid x - 1$, a contradiction. Thus $\operatorname{ord}(x) = p$ and, by Lagrange's Theorem on finite groups, $p \mid \rho - 1$, proving the claim. □

Note that, by the contrapositive statement, if $\rho \mid x^p - 1$, for some prime different from p, then we obtain a sufficient condition for $x - 1$ divisibility. That is, if $\rho \not\equiv 1 \mod p$, then we must have $\rho \mid x - 1$.

3. The Prime Case

We are now in a position to extend the hybrid bound to any prime $n = p$. The effectiveness of the bound fundamentally relies on the following observation.

Remark 1. For any prime divisor $\rho \mid x^p - 1$ outside of p itself, ρ divides either $x-1$ or $\Phi_p(x)$. If ρ divides $\Phi_p(x)$ then ρ is in a sparse subset of the primes, namely in the arithmetic progression $\rho \equiv 1 \mod p$. If most of the prime divisors are of this form, the bound on x is improved since each factor in the product bounding $x^p - 1$ is larger. If instead many prime divisors of $x^p - 1$ also divide $x - 1$, then we can bound $x-1$ by a product of small primes instead of $x^p - 1$. This, in turn, improves the bound on x.

Consider the case where $n = 3$ and $\omega_3 = 6$. The bound (1) gives $x \geq 32$. Let $k \in \{0, \ldots, 6\}$ denote the number of primes $\rho \mid x^3 - 1$ where $\rho \equiv 2 \mod 3$. If we assume $k = 2$, then we can bound x in two ways:

$$\begin{aligned} x^3 - 1 &\geq (2 \cdot 5) \cdot (3 \cdot 7 \cdot 13 \cdot 19) \\ x - 1 &\geq (2 \cdot 5). \end{aligned}$$

This gives the bound $x \geq (51871)^{1/3} > 37$. If instead we take $k = 3$, we obtain

$$\begin{aligned} x^3 - 1 &\geq (2 \cdot 5 \cdot 11) \cdot (3 \cdot 7 \cdot 13) \\ x - 1 &\geq (2 \cdot 5 \cdot 11). \end{aligned}$$

This gives the bound $x \geq 111$. If we continue in the same manner over all values of k, we find that the bound is minimal when $k = 2$. Since k is unknown for general x, we choose the worst possible case, minimize over k, and conclude that $x \geq 38$.

In order to formalise Remark 1, we partition the primes via the exponent p. Define $\Pi_p^0 := \{\rho \in \mathbb{P} : \rho \not\equiv 1 \mod p\}$ and $\Pi_p^1 := \{\rho \in \mathbb{P} : \rho \equiv 1 \mod p\}$. By construction, we must have $\mathbb{P} = \Pi_p^0 \sqcup \Pi_p^1$. Moreover, define the sets $\Omega_p(x) := \{\rho \in \mathbb{P} : \rho \mid x^p - 1\}$ and $\Omega_p^i(x) := \Omega_p(x) \cap \Pi_p^i$ for $i = 0$ or 1. Under the canonical ordering of the primes, denote the i^{th} element of Π_p^0 and Π_p^1 by $r_{i,0}$ and $r_{i,1}$, respectively. Using this notation, we have $\omega_p = |\Omega_p(x)|$. Then, we can split the bound for $x^p - 1$ into disjoint factors according to $\Omega_p^i(x)$ membership:

$$x^p - 1 \geq \prod_{\rho \in \Omega_p(x)} \rho = \prod_{\rho_0 \in \Omega_p^0(x)} \rho_0 \prod_{\rho_1 \in \Omega_p^1(x)} \rho_1.$$

By Proposition 1, we have $\rho_0 \mid x - 1$ for any $\rho_0 \in \Omega_p^0(x)$. Thus, x must also satisfy $x - 1 \geq \prod_{\rho_0 \in \Omega_p^0(x)} \rho_0$. Combining these bounds, we obtain

$$x \geq \max\left\{1 + \prod_{\rho_0 \in \Omega_p^0(x)} \rho_0, \left(1 + \prod_{\rho_0 \in \Omega_p^0(x)} \rho_0 \prod_{\rho_1 \in \Omega_p^1(x)} \rho_1\right)^{1/p}\right\}. \tag{2}$$

By considering pointwise bounds on these products, we obtain a general bound.

Proposition 2. (p-hybrid bound) *Let $p \in \mathbb{P}$ and $x \in \mathbb{Z}_{>1}$. Then*

$$x \geq min_{0\leq k<\omega_p}\left\{max\left\{1+\prod_{\substack{i=1\\ r_{i,0}\in\Pi_p^0}}^{k} r_{i,0},\left(1+\prod_{\substack{i=1\\ r_{i,0}\in\Pi_p^0}}^{k}\prod_{\substack{j=1\\ r_{j,1}\in\Pi_p^1}}^{\omega_p-k} r_{i,0}r_{j,1}\right)^{1/p}\right\}\right\}.$$

Proof. If we take $k=\left|\Omega_p^0\right|$, then we must have $\left|\Omega_p^1\right|=\omega_p-k$. By choosing the smallest possible candidates for $\rho_0\in\Omega_p^0(x)$ and $\rho_1\in\Omega_p^1(x)$, we obtain the inequalities $\prod_{\rho_0\in\Omega_p^0(x)}\rho_0\geq\prod_{i=1}^{k} r_{i,0}$ and $\prod_{\rho_1\in\Omega_p^1(x)}\rho_1\geq\prod_{j=1}^{\omega_p-k} r_{j,1}$. We apply the pointwise bounds for $\prod_{\Omega_p^0(x)}$ and $\prod_{\Omega_p^1(x)}$ in Equation (2) at each k via the argument above. Thus, we are left with

$$x \geq \max\left\{1+\prod_{\substack{i=1\\ r_{i,0}\in\Pi_p^0}}^{k} r_{i,0},\left(1+\prod_{\substack{i=1\\ r_{i,0}\in\Pi_p^0}}^{k}\prod_{\substack{j=1\\ r_{j,1}\in\Pi_p^1}}^{\omega_p-k} r_{i,0}r_{j,1}\right)^{1/p}\right\}.$$

Note that $\left|\Omega_p^1\right|>0$ for any x, so $k\neq\omega_p$. This follows from the fact that Ω_p^1 contains all factors of $\Phi_p(x)$. By assumption, $x>1$, so $\Phi_p(x)>p$ has at least one prime factor. Since $k\in[0,\omega_p)$ is unknown, we minimize over k and arrive at the statement. □

We are able to improve this result further by considering the divisibility of x^p-1 by p. This follows from Lemmas 1 and 2. If $p\mid x^p-1$, then $p^2\mid x^p-1$. Moreover, if $p\nmid x^p-1$, we exclude p from our lower bound, replacing it with a larger prime factor. For ease of notation, define $R_k^0:=\prod_{i=1}^{k} r_{i,0}$ and $R_k^1:=\prod_{j=1}^{\omega_p-k} r_{j,1}$, with the convention that $r_{i,s}\in\Pi_p^s$ denotes the i^{th} element under the natural ordering.

Proposition 3. (p-ramified bound) *Let $p\in\mathbb{P}$ with $x\in\mathbb{Z}_{>1}$ and assume, without loss of generality, that $p=r_{k'}\in\Pi_p^0$. Let $I_{k'}^-=[0,k')$ and $I_{k'}^+=[k',\omega_p)$. Then we have*

$$\begin{aligned}
x \geq\ & min\left\{max\left\{1+R_k^0,\left(1+R_k^0R_k^1\right)^{1/p}\right\}\ :\ k\in I_{k'}^-\right\}\\
&\bigcup\left\{max\left\{1+p^{-1}R_{k+1}^0,\left(1+p^{-1}R_{k+1}^0R_k^1\right)^{1/p}\right\}\ :\ k\in I_{k'}^+\right\} \qquad \text{for } p\notin\Omega_p(x)\\
x \geq\ & min\left\{max\left\{1+pR_{k-1}^0,\left(1+p^2R_{k-1}^0R_k^1\right)^{1/p}\right\}\ :\ k\in I_{k'}^-\right\}\\
&\bigcup\left\{max\left\{1+R_k^0,\left(1+pR_k^0R_k^1\right)^{1/p}\right\}\ :\ k\in I_{k'}^+\right\} \qquad \text{for } p\in\Omega_p(x).
\end{aligned}$$

Proof. Consider the general bound obtained in (2). We subdivide the proof into cases dependant on p-membership of $\Omega_p(x)$.

`Case 1a:` $p \notin \Omega_p(x)$ and $k < k'$. Since p is not a factor of R_k^0, we use the hybrid bound

$$x \geq \max\left\{1 + R_k^0, \left(1 + R_k^0 R_k^1\right)^{1/p}\right\}.$$

`Case 1b:` $p \notin \Omega_p(x)$ and $k' \leq k < \omega_p$. Now p appears as a factor of R_k^0. Therefore, we can exclude p from the product and instead consider $p^{-1}R_{k+1}^0$, resulting in the bound

$$x \geq \max\left\{1 + p^{-1}R_{k+1}^0, \left(1 + p^{-1}R_{k+1}^0 R_k^1\right)^{1/p}\right\}.$$

We minimize over possible values of k, obtaining the desired bound.

`Case 2a:` $p \in \Omega_p(x)$ and $k < k'$. All factors of R_k^0 will be smaller than p, thus we can replace the largest such factor $r_{k,0}$ by p. Moreover, by Lemma 2, if $p \in \Omega_p(x)$, then $p^2 \mid x^p - 1$. Thus, we can replace R_k^1 by pR_k^1. Then

$$x \geq \max\left\{1 + pR_{k-1}^0, \left(1 + p^2 R_{k-1}^0 R_k^1\right)^{1/p}\right\}.$$

`Case 2b:` $p \in \Omega_p(x)$ and $k' \leq k < \omega_p$. Now p already appears as a factor in R_k^0 but we still gain an extra p factor in $R_k^0 R_k^1$ by the argument in case `2a`. Thus

$$x \geq \max\left\{1 + R_k^0, \left(1 + pR_k^0 R_k^1\right)^{1/p}\right\}.$$

We minimize over possible values of k, obtaining the desired bound. □

Returning to the example given in Remark 1, let $k = 2$ and $3 \nmid x^3 - 1$. Then

$$\begin{aligned} x^3 - 1 &\geq (2 \cdot 5) \cdot (7 \cdot 13 \cdot 19 \cdot 31) \\ x - 1 &\geq (2 \cdot 5). \end{aligned}$$

This gives the bound $x \geq (535991)^{1/3} > 81$. If instead $3 \mid x^3 - 1$, we obtain

$$\begin{aligned} x^3 - 1 &\geq 3 \cdot (2 \cdot 5) \cdot (3 \cdot 7 \cdot 13 \cdot 19) \\ x - 1 &\geq 3 \cdot (2 \cdot 5), \end{aligned}$$

resulting in the bound $x \geq (155611)^{1/3} > 53$. Both divisibility cases provide a significant improvement over the bound in Remark 1.

4. The Generalized Hybrid Bound

We generalize results from the previous sections to the setting where we consider $x^n - 1$ with n composite. The first step is to factor $x^n - 1$ in $\mathbb{Z}[x]$ such that we

obtain a natural partition of the prime divisors of x^n-1. If $n=\prod_{i=1}^m p_i^{a_i}$ for unique primes $p_i\in\mathbb{P}$, define the following notation: for any $k\in[1,m]$, set

$$M_k:=\prod_{r=1}^{k-1}p_r^{a_r}\quad\text{and}\quad x_k:=x^{M_k}.$$

Proposition 4. *Let $n=\prod_{i=1}^m p_i^{a_i}$ and take x_k as above. Then we have the $\mathbb{Z}[x]$-factorization*

$$x^n-1=(x-1)\prod_{i=1}^{m}\prod_{j=1}^{a_i}\Phi_{p_i}\left(x_i^{p_i^{j-1}}\right).$$

Proof. Consider the factorization $n=M_m\cdot p_m^{a_m}$. Then, we have

$$\begin{aligned}
x^n-1&=(x^{n/p_m})^{p_m}-1\\
&=(x^{n/p_m}-1)\Phi_{p_m}\left(x^{M_m\cdot p_m^{a_m-1}}\right)\\
&\ \ \vdots\\
&=(x^{M_m}-1)\Phi_{p_m}(x^{M_m})\cdot\ldots\cdot\Phi_{p_m}\left(x^{M_m\cdot p_m^{a_m-1}}\right)\\
&=(x_m-1)\prod_{j=1}^{a_m}\Phi_{p_m}\left(x_m^{p_m^{j-1}}\right).
\end{aligned}$$

Iterating the factorization on x_k-1 for $k\in\{m,\ldots,1\}$, we obtain

$$\begin{aligned}
x^n-1&=(x_m-1)\prod_{j=1}^{a_m}\Phi_{p_m}\left(x^{r\cdot p_m^{j-1}}\right)\\
&=(x_{m-1}-1)\left[\prod_{j=1}^{a_{m-1}}\Phi_{p_{m-1}}\left(x_{m-1}^{p_{m-1}^{j-1}}\right)\right]\left[\prod_{j=1}^{a_m}\Phi_{p_m}\left(x_m^{p_m^{j-1}}\right)\right]\\
&=(x-1)\left[\prod_{j=1}^{a_1}\Phi_{p_1}\left(x_1^{p_1^{j-1}}\right)\right]\cdot\ldots\cdot\left[\prod_{j=1}^{a_m}\Phi_{p_m}\left(x_m^{p_m^{j-1}}\right)\right]\\
&=(x-1)\prod_{i=1}^{m}\left[\prod_{j=1}^{a_i}\Phi_{p_i}\left(x_i^{p_i^{j-1}}\right)\right].
\end{aligned}$$

□

Note that, if we define $x_{m+1}:=x^n$, for any $s\in[1,m]$ we have the relation

$$x_{s+1}-1=(x_s-1)\prod_{j=1}^{a_s}\Phi_{p_s}\left(x_s^{{p_s}^{j-1}}\right),$$

in the polynomial ring $\mathbb{Z}[x]$. We proceed by generalizing Lemmas 1 and 2.

Lemma 3. *Let $\rho, p \in \mathbb{P}$ and $y \in \mathbb{Z}^+$. Then $\rho \mid y-1$ and $\rho \mid \Phi_p\left(y^{p^{a-1}}\right)$ for some $a \in \mathbb{Z}^+$ implies we must have $\rho = p$.*

Proof. Assume $\rho \mid y-1, \Phi_p\left(y^{p^{a-1}}\right)$. Then, $y \equiv 1 \mod \rho$, which implies that

$$\Phi_p\left(y^{p^{a-1}}\right) \equiv \Phi_p\left(1^{p^{a-1}}\right) \equiv \Phi_p(1) \equiv p \mod \rho.$$

Therefore $\rho \mid \Phi_p\left(y^{p^{a-1}}\right)$ implies that $\rho \mid p$. Since both ρ and p are primes, we conclude that indeed $\rho = p$. □

Remark 2. Consider the situation where $n = rp_1^{a_1}p_2^{a_2}$ for two distinct $p_1, p_2 \in \mathbb{P}$ and $p_1, p_2 \nmid r$. We have the $\mathbb{Z}[x]$-factorization

$$x^n - 1 = (x^r - 1)\prod_{i=1}^{a_1} \Phi_{p_1}\left((x^r)^{p_1^{i-1}}\right) \prod_{j=1}^{a_2} \Phi_{p_2}\left((x^{rp_1^{a_1}})^{p_2^{j-1}}\right).$$

Assume there exists some k_1, k_2 and some prime ρ such that

$$\rho \mid \Phi_{p_1}\left((x^r)^{p_1^{k_1-1}}\right) \text{ and } \rho \mid \Phi_{p_2}\left((x^{rp_1^{a_1}})^{p_2^{k_2-1}}\right).$$

If we set $y = x^{rp_1^{a_1}}$, then we have $\Phi_{p_1}\left((x^r)^{p_1^{k_1-1}}\right) \mid y-1$. Thus we obtain $\rho \mid y-1$ and $\rho \mid \Phi_{p_2}\left(y^{p_2^{k_2-1}}\right)$ which, by Lemma 3, implies $\rho = p_2$. This shows that the only prime divisors potentially dividing cyclotomic polynomials with different bases in the $\mathbb{Z}[x]$-factorization from Proposition 4 are the bases themselves.

Lemma 4. *Let $p \in \mathbb{P}$ and $n = r \cdot p^a$ with $(r, p) = 1$. Then*

$$p \mid x^n - 1 \text{ if and only if } p \mid x^r - 1 \text{ and } p \mid \Phi_p\left(x^{r \cdot p^{i-1}}\right) \text{ for all } i \in \{1, ..., a\}.$$

Proof. Note that, by definition, we have

$$p \mid x^n - 1 \quad \text{if and only if} \quad x^n - 1 = (x^r)^{p^a} - 1 \equiv 0 \mod p.$$

By Fermat's little theorem, we observe that $0 \equiv (x^r)^p - (x^r) \equiv (x^r)^{p^a} - x^r \mod p$, implying $x^r \equiv (x^r)^{p^a} \equiv 1 \mod p$. We conclude that $p \mid x^r - 1$. Moreover, if $x^r \equiv 1 \mod p$, then, for any fixed $i \in \{1, ..., a\}$, we must have

$$\Phi_p\left(x^{r \cdot p^{i-1}}\right) \equiv \Phi_p\left(1^{p^{i-1}}\right) \equiv p \mod p.$$

Since $p \mid p$, the p-divisibility of $\Phi_p\left(x^{r \cdot p^{i-1}}\right)$ is clear. The reverse implication follows directly from Proposition 4. □

Reminiscent of the $n \in \mathbb{P}$ case, we partition the set of primes. For a given $n = \prod_{i=1}^{m} p_i^{a_i}$ and any $j \in [1, m-1]$, define the sets

$$\begin{aligned}
\Pi_n^m &:= \{\rho \in \mathbb{P} : \rho \equiv 1 \mod p_m\} \\
\Pi_n^j &:= \{\rho \in \mathbb{P} : \rho \equiv 1 \mod p_j \text{ and } \rho \not\equiv 1 \mod p_m, ..., p_{j+1}\} \\
\Pi_n^0 &:= \{\rho \in \mathbb{P} : \rho \not\equiv 1 \mod p_m, ..., p_1\}.
\end{aligned}$$

By construction, we have the disjoint union $\mathbb{P} = \bigsqcup_{j=0}^{m} \Pi_n^j$. Moreover, for $j \in [0, m]$, define the sets $\Omega_n(x) := \{\rho \in \mathbb{P} : \rho \mid x^n - 1\}$ and $\Omega_n^j(x) := \Omega_n(x) \cap \Pi_n^j$. Under the canonical ordering of the primes, denote the i^{th} element of Π_n^j by $r_{i,j}$. Using this notation, we have $\omega_n = |\Omega_n(x)|$. Thus we have the inequality

$$x^n - 1 \geq \prod_{\rho \in \Omega_n(x)} \rho = \prod_{\rho_0 \in \Omega_n^0(x)} \rho_0 \cdots \prod_{\rho_m \in \Omega_n^m(x)} \rho_m.$$

Recall the factorization $x^n - 1 = (x_m - 1) \prod_{j=1}^{a_m} \Phi_{p_m}\left(x_m^{j-1}\right)$ in $\mathbb{Z}[x]$. If $\rho \mid x^n - 1$ and $\rho \not\equiv 1 \mod p_m$, we must have $\rho \mid x_m - 1$. Thus $\rho \in \Omega_n^j(x)$ for some $j \in [0, m-1]$. Iterating this process, we obtain the collection of bounds

$$\begin{aligned}
x^n - 1 &\geq \prod_{\alpha=0}^{m} \prod_{\rho_\alpha \in \Omega_n^\alpha(x)} \rho_\alpha \quad \text{if and only if} \quad x \geq \left(1 + \prod_{\alpha=0}^{m} \prod_{\rho_\alpha \in \Omega_n^\alpha(x)} \rho_\alpha\right)^{1/n} \\
x_m - 1 &\geq \prod_{\alpha=0}^{m-1} \prod_{\rho_\alpha \in \Omega_n^\alpha(x)} \rho_\alpha \quad \text{if and only if} \quad x \geq \left(2 + \prod_{\alpha=0}^{m-1} \prod_{\rho_\alpha \in \Omega_n^\alpha(x)} \rho_\alpha\right)^{p_m^{a_m}/n} \\
&\vdots \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots \\
x_2 - 1 &\geq \prod_{\rho' \in \Omega_n^0(x) \cup \Omega_n^1(x)} \rho' \quad \text{if and only if} \quad x \geq \left(1 + \prod_{\rho' \in \Omega_n^0(x) \cup \Omega_n^1(x)} \rho'\right)^{1/p_1^{a_1}} \\
x - 1 &\geq \prod_{\rho_0 \in \Omega_n^0(x)} \rho_0 \quad \text{if and only if} \quad x \geq 1 + \prod_{\rho_0 \in \Omega_n^0(x)} \rho_0.
\end{aligned}$$

Combining these, we have the general bound

$$x \geq \max\left\{1 + \prod_{\rho_0 \in \Omega_n^0(x)} \rho_0, ..., \left(1 + \prod_{\rho_0 \in \Omega_n^0(x)} \rho_0 \cdot ... \cdot \prod_{\rho_m \in \Omega_n^m(x)} \rho_m\right)^{1/n}\right\}. \tag{3}$$

We are now in a position to prove Theorem 1 as a generalization of Proposition 2 for composite values of n.

Proof of Theorem 1. Set $k_s = |\Omega_n^s(x)| \in \mathbb{Z}^+$ for all $s \in \{0, ..., m\}$. By construction, we have $\sum_{s=0}^{m} k_s = \omega_n$. Moreover, by choosing the smallest possible candidates for $r_j \in \Omega_n^j(x)$, we obtain the inequalities $\prod_{r_j \in \Omega_n^j(x)} r_j \geq \prod_{i=1}^{k_j} r_{i,j}$ for all $j \in \{0, ..., m\}$. Applying the pointwise inequalities to the bound (3), we obtain

$$x \geq \max\left\{ \left(1 + \prod_{j=0}^{t} \prod_{\substack{i=1 \\ r_{i,j} \in \Pi_n^j}}^{k_j} r_{i,j} \right)^{T(t)} \; : \; t \in [0, m] \right\}.$$

A priori, the distribution of k_s is arbitrary, so we minimize over all valid values of the tuple $(k_0, ..., k_m) \in \mathbb{Z}^m$, obtaining the desired result. □

Note that this form of the hybrid bound is the correct generalization in the sense that it coincides with the prime bound in the special case when $n = p$. Indeed

$$\begin{aligned}
x &\geq \min\left\{ \max\left\{ \left(1 + \prod_{j=0}^{t} \prod_{\substack{i=1 \\ r_{i,j} \in \Pi_n^j}}^{k_j} r_{i,j} \right)^{T(t)} \; : \; t \in [0, m] \right\} \; : \; \sum_{s=0}^{m} k_s = \omega_n \right\} \\
&= \min\left\{ \max\left\{ \left(1 + \prod_{j=0}^{t} \prod_{\substack{i=1 \\ r_{i,j} \in \Pi_p^j}}^{k_j} r_{i,j} \right)^{T(t)} \; : \; t \in [0, 1] \right\} \; : \; k_0 + k_1 = \omega_n \right\} \\
&= \min_{k_0+k_1=\omega_n}\left\{ \max\left\{ 1 + \prod_{\substack{i=1 \\ r_{i,0} \in \Pi_p^0}}^{k_0} r_{i,0}, \left(1 + \prod_{\substack{i=1 \\ r_{i,0} \in \Pi_p^0}}^{k_0} r_{i,0} \prod_{\substack{i=1 \\ r_{i,1} \in \Pi_p^1}}^{k_1} r_{i,1} \right)^{1/p} \right\} \right\} \\
&= \min_{k_0+k_1=\omega_p}\left\{ \max\left\{ 1 + R_{k_0}^0, \left(1 + R_{k_0}^0 R_{k_0}^1 \right)^{1/p} \right\} \right\}.
\end{aligned}$$

This is a reformulation of the hybrid bound given in Proposition 2.

5. The Generalized Ramified Bound

In this section, we prove Theorem 2 as a generalization of Proposition 3 to composite n. Our refinement arises from the divisibility $p \mid x^n - 1$ for a given prime factor $p \mid n$. Let $n = \prod_{i=1}^{m} p_i^{a_i}$ where the factors p_i are ordered via $i < j$ implying $p_i < p_j$ and $x \in \mathbb{Z}^+$. Choose a distinguished prime divisor $p_\alpha \mid n$ and assume $p_\alpha \in \Pi_n^\tau$. Computations support the assertion that the best such choice should be the largest prime factor of n. It is clear that $\tau < \alpha$ since $1 < p_\alpha \leq p_r$ implies $p_\alpha \not\equiv 1 \mod p_r$, which holds for any $r \geq \alpha$.

Remark 3. If $p_\alpha \mid x^n-1$, then $p_\alpha \mid x_{\tau+1}-1$ and $p_\alpha \mid \Phi_{p_\alpha}\left(x_\alpha^{p_\alpha^{j-1}}\right)$ for any $j \in [1, a_\alpha]$. Thus, p_α must appear in the product $\prod_{\rho_\tau \in \Omega_n^\tau(x)} \rho_\tau$. Moreover, when the product $\prod_{\rho_\alpha \in \Omega_n^\alpha(x)} \rho_\alpha$ appears in our bound, we can replace this with $p_\alpha^{a_\alpha} \prod_{\rho_\alpha \in \Omega_n^\alpha(x)} \rho_\alpha$. The above argument gives the correct generalization of the ramified bound in Proposition 3.

Proof of Theorem 2. Assume $p_\alpha \mid x^n - 1$. Then, by the argument in Remark 3, p_α must appear in the product $\prod_{\rho_\tau \in \Omega_n^\tau(x)} \rho_\tau$. If $k_r \geq b$, then p_α is already a factor of the product. If instead $k_r < b$, then we can replace the largest factor in the product by p_α. Moreover, $\prod_{\rho_\alpha \in \Omega_n^\alpha(x)} \rho_\alpha$ can be multiplied with $p_\alpha^{a_\alpha}$ since $p_\alpha \mid x^n - 1$ implies $p_\alpha \mid \Phi_{p_\alpha}\left(x_\alpha^{p_\alpha^{j-1}}\right)$ for any $j \in [1, a_\alpha]$. If instead we assume $p_\alpha \nmid x^n - 1$, then we can exclude p_α from the product $\prod_{\rho_\tau \in \Omega_n^\tau(x)} \rho_\tau$. Thus, whenever $k_\tau > b$, we can replace p_α with the smallest prime $r_{k_\tau+1,\tau}$ in Π_n^τ which is not already a factor. In all other cases, we use the general hybrid bounds from Theorem 1. □

Remark 4. Whenever $n = 2^a$, Theorem 1 does not provide an improvement over the trivial bound in Equation (1). In essence, the hybrid bound relies on maximizing over bounds on $x^b - 1$ for $b \mid n$. Unfortunately, whenever n is a power of 2, we have $\Pi_n^0 = \{\rho \in \mathbb{P} \mid \rho \not\equiv 1 \mod 2\} = \{2\}$. Thus, $k_0 \in \{0, 1\}$ and we obtain

$$\begin{aligned}
x &\geq \min\left\{ \max\left\{ 1 + \prod_{j=1}^{k_0} 2, \left(1 + \prod_{j=1}^{k_0} 2 \prod_{\substack{i=1 \\ r_{i,1} \in \Pi_n^1}}^{\omega_n - k_0} r_{i,1} \right)^{1/n} \right\} \ : \ k_0 \in \{0,1\} \right\} \\
&= \min\left\{ \max\left\{ 1 + 2^{k_0}, \left(1 + 2^{k_0} \prod_{i=2}^{1+\omega_n-k_0} s_i \right)^{1/n} \right\} \ : \ k_0 \in \{0,1\} \right\} \\
&= \min\left\{ \left(1 + \prod_{i=2}^{1+\omega_n} s_i \right)^{1/n}, \left(1 + \prod_{i=1}^{\omega_n} s_i \right)^{1/n} \right\} \\
&= \left(1 + \prod_{i=1}^{\omega_n} s_i \right)^{1/n},
\end{aligned}$$

coinciding with Equation (1). Here s_i denotes the i^{th} prime. By applying Theorem 2, we obtain an improvement: If $2 \nmid x^n - 1$, exclude 2 as a potential factor in the

lower bound for $x^n - 1$. If instead $2 \mid x^n - 1$, then $2^{a+1} \mid x^n - 1$. Thus, we have

$$x \geq \left(1 + n \cdot \prod_{i=1}^{\omega_n} s_i\right)^{1/n} \qquad \text{for } 2 \mid x^n - 1$$

$$x \geq \left(1 + \prod_{i=2}^{\omega_n+1} s_i\right)^{1/n} \qquad \text{for } 2 \nmid x^n - 1.$$

Regardless of the divisibility case, we gain an improvement over the trivial bound. We have proved the following Corollary.

Corollary 1. *Let $n = 2^a$ and $x \in \mathbb{Z}^+$. Then*

$$x \geq min\left\{\left(1 + n \cdot \prod_{i=1}^{\omega_n} s_i\right)^{1/n}, \left(1 + \prod_{i=2}^{\omega_n+1} s_i\right)^{1/n}\right\}.$$

Note that, in the case when $2 \mid x^n - 1$, we can do better. For example, when $n = 4$, Corollary 1 relies on $2 \mid x^4 - 1$ if and only if $2^3 \mid x^4 - 1$ but, as shown by Cohen [2, Cor. 2.5], we can prove the stronger statement: $2 \mid x^4 - 1$ if and only if $2^4 \mid x^4 - 1$. This follows from the factorization $x^4 - 1 = (x-1)(x+1)(x^2+1)$ in $\mathbb{Z}[x]$ and that $2 \mid x^4 - 1$ implies $2 \mid x - 1$. Then $2 \mid x - 1, x + 1, x^2 + 1$ but also $x + 1 \equiv 2 + (x - 1) \equiv 0, 2 \mod 4$. Thus $4 \mid x - 1$ or $4 \mid x + 1$, proving Cohen's result. This principle extends to $n = 2^a$ for any $a \in \mathbb{Z}^+$, resulting in Theorem 3.

Proof of Theorem 3. Consider the $\mathbb{Z}[x]$-factorization

$$x^n - 1 = (x-1)(x+1)\prod_{i=2}^{a}\left(x^{2^{i-1}} + 1\right).$$

If $2 \mid x$, apply Theorem 2 with $p = 2$. If instead $2 \nmid x$, then $x \equiv 1 \mod 2$. Moreover, for any $k \in \mathbb{Z}^+$, $x^k \equiv 1 \mod 2$. As before, $x + 1 \equiv 2 + (x - 1) \equiv 0, 2 \mod 4$. Therefore $4 \mid x - 1$ or $4 \mid x + 1$. Thus, each of the $a + 1$ factors of $x^n - 1$ are divisible by 2 and at least one of them is divisible by 4. Then $2^{a+2} \mid x^n - 1$, and the claim follows from the same argument as in Corollary 1. □

6. Applications

In order to demonstrate the utility of these results, we consider two separate applications to existence problems in $\mathbb{F}_q$ extensions. In what follows, the *hybrid bound* will be taken to mean the bound given in Theorem 1 unless $n = 2^a$, where the *hybrid bound* will instead refer to the specialised version in Theorem 3. In the interest of presenting a cleaner argument and reducing computational complexity, we limit the discussion to the hybrid bounds. Note that the majority of results throughout the chapter can be improved further by applying Theorem 2 instead.

6.1. The Line Problem

Let $q \in \mathbb{Z}^+$ be a prime power and $\mathbb{F}_q$ the finite field of order q. Assume $\gamma_1, \gamma_2 \in \mathbb{F}_{q^n}$ with $\gamma_1, \gamma_2 \neq 0$, such that γ_1/γ_2 generates $\mathbb{F}_{q^n}$. Does there exist some $a \in \mathbb{F}_q$ such that $a\gamma_2 + \gamma_1$ is primitive in $\mathbb{F}_{q^n}$? Fix $n \in \mathbb{Z}^+$ and define:

$$\mathcal{L}_n = \left\{ q \in \mathbb{P}^m : \begin{array}{c} \text{for all } \gamma_1, \gamma_2 \in \mathbb{F}_{q^n} \setminus \{0\} \text{ such that } \frac{\gamma_1}{\gamma_2} \text{ generates } \mathbb{F}_{q^n}, \\ \text{there exists } a \in \mathbb{F}_q \text{ such that } a \cdot \gamma_2 + \gamma_1 \text{ primitive} \end{array} \right\}.$$

The *line problem* of degree n is to determine which prime powers q belong to $\mathcal{L}_n$. This problem has been completely solved in the cases where $n = 2$ by Cohen [2, Th. 1.1], and $n = 3$ by Bailey, Cohen, Sutherland and Trudgian [1, Th. 2]. Bailey et al. also made significant progress towards the $n = 4$ case. For fixed n, the standard approach is to take advantage of a sieve to guarantee that all sufficiently large q belong to $\mathcal{L}_n$. In particular, Cohen leveraged the following prime sieve criterion.

Proposition 5 ([2, Proposition 4.3])**.** *Let q be a prime power. For any s distinct prime divisors p_i of $q^n - 1$, define $\delta = \delta(p_1, ..., p_s) := 1 - \sum_{i=1}^{s} \frac{1}{p_i}$. Suppose that $\delta > 0$ for some choice of p_i. Then*

$$q > R_G := (n-1)^2 2^{2(\omega_n - s)} \left(\frac{s-1}{\delta} + 2 \right)^2 \quad \textit{implies} \quad q \in \mathcal{L}_n.$$

Thus, we aim to choose p_i such that R_G is minimal. For any fixed s, this amounts to maximizing δ. Thus, we wish for $\sum_{i=1}^{s} p_i^{-1}$ to be small. In practice, we choose the largest s distinct prime factors p_i of $q^n - 1$. When the explicit factorization of $q^n - 1$ is unknown, we bound R_G above by taking p_i to be the $(\omega_n + 1 - s)$-th through ω_n-th smallest primes. Minimizing across valid s for which $\delta > 0$, we obtain an upper bound for R_G.

Remark 5. Note that, if we choose $s = 0$, then trivially $\delta = 1 > 0$. Thus

$$q > (n-1)^2 4^{\omega_n} \text{ implies } q \in \mathcal{L}_n.$$

For a fixed n, consider the trivial lower bound on q via (1). If $q^n - 1 \geq \prod_{i=1}^{\omega_n} s_i$, then $q > \prod_{i=1}^{\omega_n} s_i^{1/n} > (n-1)^2 4^{\omega_n}$ for all sufficiently large ω_n. In that case, we obtain $q \in \mathcal{L}_n$ automatically.

The difficulty then lies in finding a small upper bound on ω_n for which $q \notin \mathcal{L}_n$ is a possibility. Call the largest value of ω_n for which it is possible that there exists some $q \notin \mathcal{L}_n$ the ω_n *cut-off* detected by a given lower bound on q. Varying across $n \in [2, 30]$, we compare the effectiveness of the hybrid bound to the trivial bound in detecting ω_n cut-offs and present these calculations in Table 6.1. The *search space* column in Table 6.1 provides the percentage of potential exceptional q values to check when comparing the hybrid and trivial bounds. The rows for which

n	$\omega_n \leq \#$		$q \leq \#$		search space
	Trivial	Hybrid	Trivial	Hybrid	
2	8	7	3712	2040	55%
3	13	13	142862	142862	100%
4	18	18	$1.2 \cdot 10^6$	$1.2 \cdot 10^6$	100%
5	23	20	$6.1 \cdot 10^6$	$3.3 \cdot 10^6$	54%
6	29	28	$2.8 \cdot 10^7$	$2.3 \cdot 10^7$	84%
7	34	26	$9.0 \cdot 10^7$	$2.4 \cdot 10^7$	27%
8	39	38	$2.1 \cdot 10^8$	$1.9 \cdot 10^8$	90%
9	44	41	$4.5 \cdot 10^8$	$3.4 \cdot 10^8$	75%
10	49	43	$9.0 \cdot 10^8$	$5.2 \cdot 10^8$	58%
11	54	39	$1.7 \cdot 10^9$	$4.4 \cdot 10^8$	26%
12	59	58	$3.0 \cdot 10^9$	$2.8 \cdot 10^9$	92%
13	64	45	$5.3 \cdot 10^9$	$1.1 \cdot 10^9$	21%
14	69	57	$8.9 \cdot 10^9$	$3.6 \cdot 10^9$	41%
15	74	66	$1.5 \cdot 10^{10}$	$8.3 \cdot 10^9$	56%
16	80	79	$2.6 \cdot 10^{10}$	$2.4 \cdot 10^{10}$	93%
17	85	56	$4.1 \cdot 10^{10}$	$5.1 \cdot 10^9$	12%
18	90	85	$6.4 \cdot 10^{10}$	$4.7 \cdot 10^{10}$	73%
19	95	62	$9.1 \cdot 10^{10}$	$1.0 \cdot 10^{10}$	11%
20	101	91	$1.3 \cdot 10^{11}$	$8.4 \cdot 10^{10}$	64%
21	106	88	$1.8 \cdot 10^{11}$	$8.0 \cdot 10^{10}$	44%
22	111	83	$2.5 \cdot 10^{11}$	$6.2 \cdot 10^{10}$	25%
23	116	75	$3.4 \cdot 10^{11}$	$3.9 \cdot 10^{10}$	12%
24	121	120	$4.5 \cdot 10^{11}$	$4.3 \cdot 10^{11}$	96%
25	126	103	$6.0 \cdot 10^{11}$	$2.3 \cdot 10^{11}$	38%
26	132	96	$8.3 \cdot 10^{11}$	$1.8 \cdot 10^{11}$	22%
27	137	124	$1.1 \cdot 10^{12}$	$6.5 \cdot 10^{11}$	59%
28	142	119	$1.4 \cdot 10^{12}$	$5.7 \cdot 10^{11}$	40%
29	148	93	$2.0 \cdot 10^{12}$	$2.0 \cdot 10^{11}$	10%
30	153	138	$2.6 \cdot 10^{12}$	$1.4 \cdot 10^{12}$	55%

Table 1: The trivial and hybrid bounds compared across varying n.

$n \in \mathbb{P}$ are highlighted by grey. Computations support the assertion that the hybrid bound is most effective at the primes, when compared to the trivial bound. It is worth noting that even an incremental improvement on the q-range will drastically improve computation time. For a specific value q, we are essentially factoring $q^n - 1$, which becomes increasingly infeasible when n grows large.

We consider the specific case when $n = 5$. By applying the trivial bound in Equation (1) directly and comparing this to Proposition 5, we have that $\omega_5 \geq 24$ implies $q \in \mathcal{L}_5$. We initially find a value $\omega_5 = k$ for which Remark 5 leads to $q \in \mathcal{L}_5$ directly. In this case it is sufficient to choose $k = 500$ since

$$\prod_{i=1}^{500} s_i^{1/5} \approx 8.9 \cdot 10^{303} \quad \text{and} \quad (5-1)^2 4^{500} \approx 1.7 \cdot 10^{302}.$$

Next, we check each value $\omega_5 < 500$ by choosing $s \in [0, \omega_5]$ such that $\delta > 0$ and R_G is minimized in Proposition 5. Comparing R_G with the trivial bound, we are able

to rule out $\omega_5 > 23$. For example, if $\omega_5 = 24$ and $s = 21$, we have:

$$\prod_{i=1}^{24} s_i^{1/5} \approx 7.5 \cdot 10^6, \quad R_G \approx 7.4 \cdot 10^6 \quad \text{and } \delta \approx 0.24.$$

Thus, any non-members of $\mathcal{L}_5$ would have to satisfy $\omega_5 \leq 23$ and be in the range $q \leq R_G \approx 6.1 \cdot 10^6$, where the value of R_G is given by choosing $s = 20$ for $\omega_5 = 23$. If we apply Theorem 1 in place of the trivial bound, we can knock out more ω_5 values: if $\omega_5 > 20$ then $q \in \mathcal{L}_5$. By the same argument as before, any non-members must lie in the range $q \leq R_G \approx 3.3 \cdot 10^6$. In general, if $q \notin \mathcal{L}_5$ then q is bounded below by the hybrid bound and bounded above by the prime sieve in Proposition 5. We calculate the q-intervals for each $\omega_5 \in [1, 20]$, which are recorded in Table 6.1.

ω_5	$\# \leq q$	$q \leq \#$
20	2 160 476	3 336 768
19	881 791	2 689 898
18	397 068	2 150 020
17	132 575	1 696 702
16	46 411	1 327 972
15	25 794	1 022 189
14	9023	771 455
13	3190	571 449
12	1910	397 505
11	701	260 365
10	265	164 401
9	179	101 825
8	72	59 399
7	31	32 641
6	22	16 925
5	10	7834
4	7	3175
3	4	1024
2	3	256
1	2	64

Table 2: The hybrid bound intervals.

Since the upper bound on q is sufficiently small, we enumerate all potential prime powers q in each ω_5-interval. For any such q, we determine whether $\omega(q^5 - 1) = k$. The number of values of q satisfying the ω_5 criterion in each interval is shown in Table 6.1. For $\omega_5 \in [15, 20]$, all values of q are members of $\mathcal{L}_5$.

In order to whittle down the potential exceptions further, we introduce more sophisticated sieves. In what follows, the radical $\mathrm{Rad}(x)$ of a number x is taken to mean the product of the distinct prime factors of x.

ω_5	# of options
14	1
13	5
12	19
11	72
10	214
9	438
8	683
7	763
6	625
5	303
4	68
3	22
2	2
1	1
Total	3215

Table 3: q-value options in hybrid intervals.

Proposition 6 ([2, Proposition 6.3])**.** *Let q be a prime power and $\omega_n \geq 2$. Consider s distinct prime factors p_i of $q^n - 1$ and some other prime factor l. Define the quantity $\delta := \delta(p_1, ..., p_s)$ and set $k = Rad(q^n - 1)/(l \cdot \prod_{i=1}^{s} p_i)$. Moreover, suppose $\delta > 1/(l \cdot \phi(k))$. Then*

$$q > (n-1)^2 \left(\frac{2^{\omega_n - s - 1}\phi(k)(s - 1 + 2\delta) + 1 - \frac{1}{l}}{\phi(k)\delta - \frac{1}{l}} - 1 \right)^2 \quad \textit{implies} \quad q \in \mathcal{L}_n.$$

We shall refer to this sieving criteria as the *modified prime sieve*. In practice, l is always chosen to be the largest prime factor of $q^n - 1$ and k to be the product of the smallest factors. Bailey et al. proved a generalized version, aptly named the *general prime sieve*.

Proposition 7 ([1, Lemma 1])**.** *Let q be a prime power and write the radical of $q^n - 1$ as $Rad(q^n - 1) = k \cdot (\prod_{i=1}^{s} p_i)(\prod_{j=1}^{r} l_j)$. Set $\delta = 1 - \sum_{i=1}^{s} \frac{1}{p_i}$, $\epsilon = \sum_{j=1}^{r} \frac{1}{l_j}$ and $m = \phi(k)/k$. If $\delta m > \epsilon$ then*

$$q > (n-1)^2 \left(\frac{2^{\omega_n - s - r} m(s - 1 + 2\delta) - \delta m + r - \epsilon}{\delta m - \epsilon} \right)^2 \quad \textit{implies} \quad q \in \mathcal{L}_n.$$

Returning to the line problem for $n = 5$, we iterate the prime, modified, and general sieves to filter out more q values. When applying the sieves, we factor the radical $\mathrm{Rad}(q^n - 1) = k \cdot (\prod_{i=1}^{s} p_i)(\prod_{j=1}^{r} l_j)$ in such a way that the sieve bound is as small as possible. For any $\rho \in \mathbb{P}$ with $\rho \mid k$ and any i, j, we always factor $\mathrm{Rad}(q^n - 1)$ such that $\rho < p_i < l_j$. Then, minimizing the sieves amounts to choosing only the number r and s of factors p_i and l_j, respectively. The numbers of unsieved q-values for each sieve appear in Table 6.1, all values of which are known explicitly. As is apparent, only a small set of prime powers can be non-members

ω_5	Prime sieve	Modified sieve	General sieve
14	0	0	0
13	0	0	0
12	1	1	1
11	10	10	10
10	25	19	18
9	48	37	35
8	143	112	111
7	189	144	144
6	197	161	161
5	136	115	115
4	42	33	33
3	22	16	16
2	2	2	2
1	1	1	1
Totals	816	651	647

Table 4: Unsieved q-values in hybrid intervals.

of $\mathcal{L}_5$. For convenience, we record this partial computational verification in the following result.

Proposition 8. *Let q be a prime power and E_5 be the set of 647 prime powers described in the appendix, the largest of which is 62791. If $q \notin E_5$, then $q \in \mathcal{L}_5$.*

Remark 6. Let us generalize our approach for tackling the line problem in the case where $n = 5$ to any fixed $n \in \mathbb{Z}^+$. For some distinguished set $\mathcal{A}_n$, we want to determine for which prime powers q we have the membership $q \in \mathcal{A}_n$. In the case of the line problem, this set $\mathcal{A}_n$ is $\mathcal{L}_n$. We have a sieve criterion of the form

$$q > S(n, \omega_n) \quad \text{implies} \quad q \in \mathcal{A}_n,$$

where $S(n, \omega_n)$ is some function of n and ω_n. In Proposition 5, we might take $s = 0$, obtaining the criterion $q > (n-1)^2 2^{2\omega_n}$ implies $q \in \mathcal{A}_n$. Cohen used this naive sieve in his original work for $\mathcal{L}_3$, see [2, Cor. 2.4]. This allows us to describe a general procedure for the line problem; see Steps 1–5 below. A similar approach extends to other existence problems for primitive elements in finite fields.

`Step 1:` Finiteness. For fixed ω_n, we compare the sieve criterion $S(n, \omega_n)$ with a lower bound $B(n, \omega_n)$ on q, dependant on n and ω_n. Then, if

$$q \geq B(n, \omega_n) > S(n, \omega_n),$$

we conclude that $q \in \mathcal{A}_n$. By Remark 5, when ω_n is sufficiently large, this will always be the case. We obtain a cut-off value c for ω_n, above which it is guaranteed that $q \in \mathcal{A}_n$. The sharpness of the the cut-off will be dependent on the sophistication of both $S(n, \omega_n)$ and $B(n, \omega_n)$. This is where Theorems 1 and 2 become powerful tools for reducing ω_n.

`Step 2:` Intervals. For each $\omega_n \leq c$, we construct the intervals

$$I_{\omega_n} = [B(n, \omega_n), S(n, \omega_n)].$$

Thus, if $q \notin \mathcal{A}_n$, then $q \in I_{\omega_n}$ for some value of ω_n. For the line problem, these intervals are described in Table 6.1. Using Theorem 1 over the trivial bound in (1), shortens these intervals by increasing $B(n, \omega_n)$.

`Step 3:` Enumeration. If the previous steps have reduced I_{ω_n} sufficiently, we enumerate the possible prime powers in each interval. For a given prime power in the interval I_{ω_n}, we check if indeed $q^n - 1$ has ω_n distinct prime factors. This is summarized in Table 6.1.

`Step 4:` Sieving. For the remaining potential counterexamples $q \notin \mathcal{A}_n$, we reapply our sieve criterion. Since the exact value of q is known, we obtain a better sieve bound in Proposition 5 by including specific information about q. In a similar vein, we apply other sieves to eliminate more values of q.

`Step 5:` Direct verification. Once we exhaust all theoretical sieving techniques, we return to the specific problem of finding a primitive element on a line inside $\mathbb{F}_{q^n}$. Given that the list of potential counterexamples is small enough to be computable, we verify directly if there exists such primitive elements.

The set E_5 of potential counterexamples is expected to contain very few genuine non-members $q \notin \mathcal{L}_5$. In the case of $n = 3$, Cohen [2, Theorem 6.4] proved that the number of genuine non-members $q \notin \mathcal{L}_3$ was at most 183. By contrast, Bailey et al. [1, Theorem 2] proved that $q \notin \mathcal{L}_3$ if and only if $q \in \{3, 4, 5, 7, 9, 11, 13, 31, 37\}$. In the same paper, they gave a set of 1469 potential non-members $q \notin \mathcal{L}_4$ but only 21 of these were proven to be genuine in the above sense. See [1, Theorems 3 & 5].

6.2. Primitive Element Sums

Let $q \in \mathbb{Z}^+$ be a prime power and consider the following problem. For which pairs (q, n) does there exist a primitive element $\alpha \in \mathbb{F}_{q^n}$ such that $\alpha + \alpha^{-1}$ is also primitive? Fix n and define

$$\mathcal{U}_n := \{q = p^m : \text{ there exists } \alpha \in \mathbb{F}_{q^n} \text{ such that } \alpha, \alpha + \alpha^{-1} \text{ primitive}\}.$$

Liao, Li and Pu provided a partial answer to this question and a sufficient condition for membership $q \in \mathcal{U}_n$.

Proposition 9 ([7, Theorem 1.3]). *Let $n \in \mathbb{Z}^+$ and q a prime power coprime to n. Then $q^{n/2} > 2^{2\omega_n}$ implies $q \in \mathcal{U}_n$.*

Remark 7. The criterion in Proposition 9 is equivalent to

$$q > 2^{4\omega_n/n} \quad \text{implies} \quad q \in \mathcal{U}_n.$$

Thus, for $n > 4\omega_n$, we have $q \notin \mathcal{U}_n$ implies $q \leq 2^{4\omega_n/n} < 2$ which in turn results in $q = 1$. Since q is assumed to be a prime power, this never occurs. Therefore, for any choice of ω_n, we need only check $n \leq 4\omega_n$. Given fixed n and ω_n, we have the trivial bound $q^n > q^n - 1 \geq \prod_{i=1}^{\omega_n} s_i$. Thus, if $q \notin \mathcal{U}_n$, then q^n must lie in the interval $\prod_{i=1}^{\omega_n} s_i < q^n \leq 2^{4\omega_n} = 16^{\omega_n}$.

Proposition 10. *Let $\omega_n \in \mathbb{Z}^+$. Then $\omega_n < 16$ if and only if $\prod_{i=1}^{\omega_n} s_i < 16^{\omega_n}$.*

Proof. A quick calculation shows that the right-hand side is true whenever $\omega_n < 16$. Moreover, for $\omega_n = 16$, we have $\prod_{i=1}^{16} s_i > 16^{16}$. If $\omega_n = 16 + k$ for $k \in \mathbb{Z}^+$, then

$$16^{-\omega_n} \cdot \prod_{i=1}^{\omega_n} s_i = 16^{-k} \prod_{i=17}^{16+k} s_i \cdot \left(16^{-16} \cdot \prod_{i=1}^{16} s_i \right) > 16^{-k} \prod_{i=17}^{16+k} s_i = \prod_{i=17}^{16+k} \frac{s_i}{16}.$$

Since $s_i > 16$ for any $i > 6$, we conclude that indeed $16^{-\omega_n} \cdot \prod_{i=1}^{\omega_n} s_i > 1$. □

Corollary 2. *If $q \notin \mathcal{U}_n$, then $\omega_n \leq 15$.*

Proof. This follows immediately from the fact that $q^n \in (\prod_{i=1}^{\omega_n} s_i, 16^{\omega_n}]$ which is non-empty if and only if $\omega_n \leq 15$. □

Thus, any possible exceptions $q \notin \mathcal{U}_n$ must satisfy $\omega_n \leq 15$ and, by Remark 7, also $n \leq 4\omega_n \leq 60$. Note that, for $n = 1$, this question has been completely resolved by Cohen, Silva, Sutherland and Trudgian.

Proposition 11 ([3, Corollary 2])**.** *Let q be a prime power. Then*

$$q \notin \{2, 3, 4, 5, 7, 9, 13, 25, 121\} \quad \text{if and only if} \quad q \in \mathcal{U}_1.$$

In what follows, assume that $n > 1$. For fixed values of $\omega_n \in \{1, ..., 15\}$ we could now check which pairs (q, n) give rise to a value $q^n \in (\prod_{i=1}^{\omega_n} s_i, 16^{\omega_n}]$. If instead we apply the hybrid bound $H(n, \omega_n)$ and iterate over $n \in \{1, ..., 4\omega_n\}$, we need only check if we have any $q^n \in (H(n, \omega_n)^n, 16^{\omega_n}]$. The search intervals for the trivial and hybrid bounds are given in Figures 6.2 and 6.2, respectively. Empty search

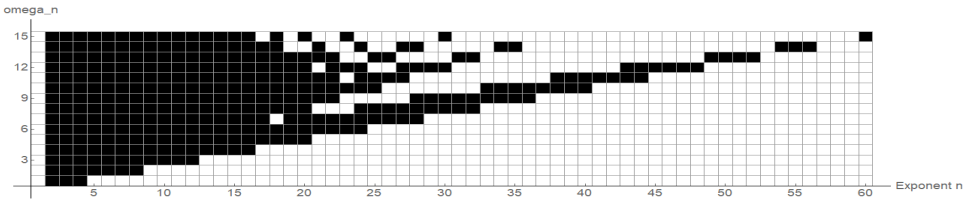

Figure 1: The trivial bound intervals for primitive element sums.

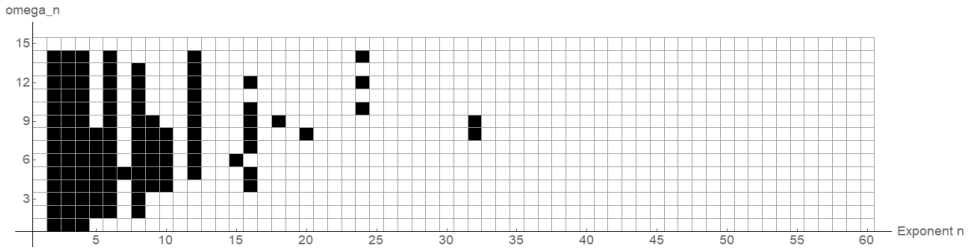

Figure 2: The hybrid bound intervals for primitive element sums.

interval pairs (n, ω_n) are unmarked, whereas potential exceptions are marked black. The hybrid bound is much more efficient at ruling out potential counterexamples compared to the trivial bound. So far, we have only checked the non-emptiness of each interval $(H(n,\omega_n)^n, 16^{\omega_n}]$. The natural next step is to incorporate the presumed value of ω_n in such an interval. For each pair (n, ω_n) with non-empty search interval, we check if there exists any prime power $q \in (H(n,\omega_n), 16^{\omega_n/n}]$ satisfying $\omega(q^n - 1) = \omega_n$. This dramatically reduces our search space and leaves us with only a small list of exceptional pairs (n, ω_n), marked black in Figure 6.2. Our computation gives a sufficient condition for membership of $\mathcal{U}_n$.

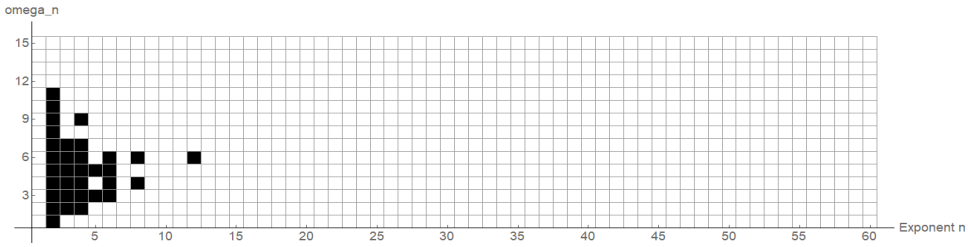

Figure 3: Existence of q-values in hybrid intervals.

Proposition 12. *Let q be a prime power and $\mathcal{E}_{\mathcal{U}}$ be the set of 33 pairs $(a,b) \in \mathbb{Z}^2$ described in the appendix. Then $(n,\omega_n) \notin \mathcal{E}_{\mathcal{U}}$ implies $q \in \mathcal{U}_n$.*

Although the primitive element sum problem is not completely resolved, the techniques used highlight the relative effectiveness of our hybridised bounds over the trivial bound. As in Proposition 8, we should expect that most of the pairs $(n,\omega_n) \in \mathcal{E}_{\mathcal{U}}$ do not give rise to any genuine non-members $q \notin \mathcal{U}_n$.

Acknowledgment. The author is grateful to the referee for a thorough reading of this manuscript, and for supplying constructive feedback.

References

[1] G. Bailey, S. D. Cohen, N. Sutherland, and T. Trudgian, Existence results for primitive elements in cubic and quartic extensions of a finite field, *Math. Comp.* **88** (316) (2019), 931–947.

[2] S. D. Cohen, Primitive elements on lines in extensions of finite fields, *Contemp. Math.* **518** (2010), 113–127.

[3] S. D. Cohen, T. Oliveira e Silva, N. Sutherland, and T. Trudgian, Linear combinations of primitive elements of a finite field, *Finite Fields Appl.* **51** (2018), 388–406.

[4] G. Kapetanakis, R. K. Sharma, and S. Takshak, $\mathbb{F}_q$-primitive points on varieties over finite fields, *Finite Fields Appl.* **103** (2025), Article #102582, 8 pp.

[5] S. Laishram, R. Sarma, and J. Sharma, Fields with primitive elements having primitive image under rational functions, *Comm. Algebra* **52** (2024), 1–16.

[6] A. Lemos, V. G. L. Neumann, and S. Ribas, On arithmetic progressions in finite fields, *Des. Codes Cryptogr.* **91** (6) (2023), 23 pp.

[7] J. Li, Q. Liao, and K. Pu, On the existence for some special primitive elements in finite fields, *Chinese Ann. Math. Ser. B* **37** (2016), 259–266.

[8] M. Rani, A. K. Sharma, S. K. Tiwari, and A. Panigrahi, Inverses of r-primitive k-normal elements over finite fields, *Ramanujan J.* **64** (2024), 723–747.

[9] H. Sharma and R. K. Sharma, Existence of primitive pairs with prescribed traces over finite fields, *Commun. Algebra* **49** (4) (2021), 7 pp.

[10] H. Sharma and R. K. Sharma, Existence of primitive normal pairs with one prescribed trace over finite fields, *Des. Codes Cryptogr.* **89** (10) (2021), 2841—2855.

[11] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1997.

Appendix

We record the set E_5 of potential exceptions referenced in Proposition 8:
$E_5 = \{$ 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29, 31, 32, 37, 41, 43, 47, 49, 53, 59, 61, 64, 67, 71, 73, 79, 81, 83, 89, 97, 101, 103, 107, 109, 113, 121, 125, 127, 128, 131, 137, 139, 149, 151, 157, 163, 167, 169, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 243, 251, 256, 257, 269, 271, 277, 281, 283, 289, 293, 307, 311, 313, 317, 331, 337, 343, 347, 349, 353, 361, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 487, 491, 499, 509, 512, 521, 523, 529, 541, 547, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 625, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 729, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 811, 821, 823, 827, 829, 839, 841, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 961, 967, 971, 977, 991, 997, 1009, 1013, 1019, 1021, 1024, 1031, 1033, 1039, 1051, 1061, 1063, 1069, 1087, 1091, 1093, 1097, 1103, 1109, 1117, 1123, 1151, 1153, 1163,

1171, 1181, 1193, 1213, 1217, 1223, 1229, 1231, 1237, 1259, 1277, 1279, 1283, 1289, 1291, 1301, 1303, 1307, 1321, 1327, 1331, 1361, 1367, 1369, 1373, 1381, 1399, 1409, 1423, 1429, 1433, 1439, 1447, 1451, 1453, 1471, 1483, 1489, 1499, 1511, 1531, 1543, 1549, 1567, 1571, 1583, 1597, 1607, 1609, 1621, 1627, 1637, 1667, 1669, 1681, 1693, 1697, 1699, 1709, 1721, 1723, 1741, 1747, 1753, 1759, 1777, 1783, 1789, 1801, 1831, 1849, 1861, 1867, 1871, 1873, 1879, 1901, 1907, 1933, 1949, 1951, 1993, 1999, 2003, 2011, 2017, 2027, 2029, 2053, 2081, 2083, 2087, 2089, 2113, 2131, 2137, 2141, 2143, 2161, 2179, 2197, 2203, 2209, 2221, 2237, 2251, 2267, 2269, 2281, 2293, 2297, 2311, 2333, 2341, 2347, 2357, 2371, 2377, 2381, 2389, 2393, 2401, 2411, 2437, 2467, 2473, 2503, 2521, 2531, 2539, 2551, 2557, 2593, 2621, 2633, 2647, 2659, 2671, 2683, 2689, 2707, 2713, 2731, 2749, 2767, 2791, 2797, 2803, 2809, 2833, 2851, 2857, 2861, 2887, 2927, 2953, 2963, 2971, 3001, 3011, 3019, 3023, 3037, 3041, 3061, 3067, 3109, 3121, 3125, 3181, 3187, 3191, 3217, 3221, 3253, 3259, 3271, 3301, 3319, 3331, 3361, 3391, 3433, 3457, 3463, 3481, 3511, 3529, 3541, 3547, 3571, 3583, 3607, 3613, 3631, 3643, 3691, 3697, 3721, 3727, 3733, 3739, 3767, 3821, 3823, 3851, 3853, 3877, 3907, 3911, 3919, 3931, 3943, 4003, 4019, 4021, 4051, 4057, 4096, 4111, 4129, 4159, 4201, 4219, 4229, 4231, 4243, 4261, 4271, 4273, 4327, 4441, 4447, 4489, 4513, 4519, 4523, 4561, 4567, 4591, 4603, 4621, 4651, 4657, 4663, 4691, 4733, 4759, 4783, 4789, 4813, 4831, 4909, 4931, 4933, 4951, 4957, 4999, 5011, 5041, 5101, 5119, 5167, 5179, 5329, 5437, 5449, 5503, 5521, 5531, 5581, 5591, 5641, 5659, 5701, 5743, 5779, 5791, 5839, 5851, 5857, 5881, 5923, 6007, 6037, 6043, 6073, 6091, 6121, 6133, 6163, 6217, 6241, 6247, 6271, 6301, 6361, 6373, 6421, 6427, 6451, 6571, 6581, 6619, 6637, 6679, 6691, 6733, 6763, 6781, 6791, 6841, 6859, 6889, 6991, 7039, 7177, 7243, 7351, 7411, 7417, 7549, 7561, 7573, 7591, 7603, 7687, 7723, 7753, 7921, 7951, 8011, 8089, 8161, 8191, 8317, 8353, 8419, 8431, 8647, 8737, 8779, 8821, 8893, 8941, 8971, 9001, 9091, 9109, 9199, 9241, 9283, 9409, 9421, 9521, 9631, 9661, 9769, 9781, 9871, 10141, 10201, 10321, 10531, 10609, 10651, 10711, 10831, 10861, 10891, 11047, 11071, 11131, 11257, 11311, 11317, 11449, 11551, 11701, 11719, 11731, 11881, 11971, 12391, 12433, 12541, 12769, 13171, 13399, 13567, 13831, 13921, 14281, 14479, 14551, 14821, 15331, 15511, 15541, 15601, 15625, 15877, 15991, 16339, 16927, 17161, 17491, 17791, 17851, 18181, 18481, 18769, 19321, 19501, 19891, 20011, 20431, 20749, 21211, 21751, 22201, 22621, 23011, 23311, 24781, 25117, 26041, 27691, 28561, 28771, 29671, 30661, 32761, 41611, 42331, 46411, 51871, 60901, 62791}.

We record the set $\mathcal{E}_{\mathcal{U}}$ of potential exception pairs referenced in Proposition 12: $\mathcal{E}_{\mathcal{U}} :=$ { (2,1), (2,2), (2,3), (2,4), (2,5), (2,6), (2,7), (2,8), (2,9), (2,10), (2,11), (3,2), (3,3), (3,4), (3,5), (3,6), (3,7), (4,2), (4,3), (4,4), (4,5), (4,6), (4,7), (4,9), (5,3), (5,5), (6,3), (6,4), (6,5), (6,6), (8,4), (8,6), (12,6)}.