M. Zoeteman

A Siegel–Walfisz theorem for Artin primes and applications

Bachelor thesis

June 30, 2017

Thesis supervisor: Dr. E. Sofos

Leiden University
Mathematical Institute

Contents

1 Introduction

Notation. The letter p will always refer to a prime throughout this thesis.
We denote by ϕ the Euler-phi function, that is $\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$.

1.1 The prime number theorem and the Siegel–Walfisz theorem

One of the most important quantities in number theory is the number of primes up to a certain bound. The *prime number theorem* states that the number of primes not exceeding x, which we denote by $\#\{p \leq x\}$, satisfies

$$\lim_{x\to\infty} \frac{\#\{p \leq x\}}{\frac{x}{\log x}} = 1.$$

This was conjectured by Legendre and Gauss before 1850. In 1896 it was proved independently by Hadamard and de la Vallée Poussin. They proved a stronger statement called the prime number theorem with error term, which states that there is a constant $c > 0$ such that

$$\#\{p \leq x\} = \mathrm{li}(x) + O\left(x\mathrm{e}^{-c\sqrt{\log x}}\right),$$

where $\mathrm{li}(x) := \int_2^x \frac{1}{\log u}\mathrm{d}u = \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right)$.

The *prime number theorem for arithmetic progressions* states that, for $a, q \in \mathbb{N}$ coprime,

$$\lim_{x\to\infty} \frac{\#\{p \leq x : p \equiv a \mod q\}}{\frac{1}{\phi(q)}\frac{x}{\log x}} = 1. \tag{1.1}$$

With the prime number theorem in mind, loosely speaking we can say that a fraction $\frac{1}{\phi(q)}$ of all the primes is $a \mod q$, and that the primes are equidistributed over the coprime residue classes mod q. The *Siegel–Walfisz theorem* [19], proved in 1935, is a version of (1.1) with error term. It states the following: for each $A > 0$ there is a constant $c(A) > 0$ such that for all $a, q \in \mathbb{N}$ coprime with $q \leq (\log x)^A$ we have

$$\#\{p \leq x : p \equiv a \mod q\} = \frac{1}{\phi(q)}\mathrm{li}(x) + O\left(x\mathrm{e}^{-c(A)\sqrt{\log x}}\right), \tag{1.2}$$

where the implied error term only depends on A.

1.1.1 Applications of the Siegel–Walfisz theorem

Almost every big progress in the last 100 years for problems about the distribution of primes was made using the Siegel–Walfisz theorem, due to the uniformity of the error term on q. The ternary Goldbach conjecture states that every odd number larger than 5 is a sum of 3 primes. Vinogradov [20] proved this in 1937 for every large enough odd integer, using the Siegel–Walfisz theorem. Other applications of the Siegel–Walfisz theorem are certain counting problems, e.g. the following results were obtained using the Siegel–Walfisz theorem.
1) *For each $A > 0$, the number of primes $p \leq x$ for which $p - 1$ is squarefree equals*

$$\mathrm{li}(x)\prod_p \left(1 - \frac{1}{p(p-1)}\right) + O_A\left(\frac{x}{(\log x)^A}\right), \tag{1.3}$$

where the implied constant in the error term only depends on A.
2) *For each $A > 0$, the number of ways to write $N \in \mathbb{N}$ as a sum $N = p + s$ with p prime and s squarefree, equals*

$$\mathrm{li}(N) \prod_p \left(1 - \frac{1}{p(p-1)}\right) \prod_{p|N} \left(1 + \frac{1}{p^2 - p - 1}\right) + O_A\left(\frac{x}{(\log x)^A}\right), \tag{1.4}$$

where the implied constant in the error term only depends on A.

The known proofs of (1.3) (see [12]) and (1.4) (see [21]) don't work if one uses (1.1) instead of Siegel–Walfisz.

1.2 Artin's primitive root conjecture

Recall that for a prime p the finite field $\mathbb{F}_p$ with p elements has cyclic unit group $\mathbb{F}_p^*$ of order $p - 1$.

Definition 1.1. Let p be a prime and $g \in \mathbb{Z}$. Then g is called a *primitive root mod p* if $g \mod p$ is a generator of the group $\mathbb{F}_p^*$.

Thus, g is a primitive root mod p if and only if $g \mod p$ has order $p - 1$ in $\mathbb{F}_p^*$.

Definition 1.2. Let p be a prime. We call p an *Artin prime* if 2 is a primitive root mod p.

Definition 1.2 is not standard. In the literature p is called an *Artin prime for the root g* if g is a primitive root mod p. However, in this thesis we will only consider the case $g = 2$ to ease the exposition.

Artin conjectured in 1927 that if $g \in \mathbb{Z} \setminus \{-1, 0, 1\}$ is not a square, then g is a primitive root mod p for infinitely many primes p. In fact, he conjectured something more precise, namely that for $g \in \mathbb{Z}$,

$$\#\{p \leq x : \langle g \rangle = \mathbb{F}_p^*\} = A(g)\frac{x}{\log x} + o\left(\frac{x}{\log x}\right), \tag{1.5}$$

where $A(g)$ is a constant which is is positive whenever $g \neq -1, 0, 1$ and g is not a square. This is called *Artin's conjecture on primitive roots*, see Conjecture 1 from [15] for the definition of $A(g)$. Numerical experiments led Artin to reformulate the definition of $A(g)$ to take into account certain entanglement phenomena.

In 1967 Hooley [5] proved, under assumption of the generalized Riemann hypothesis (GRH) that indeed for $g \neq -1, 0, 1$ not a square there are infinitely many primes p with $\langle g \rangle = \mathbb{F}_p^*$. He also obtained an asymptotic like (1.5) with an explicit error term, namely

$$\#\{p \leq x : \langle g \rangle = \mathbb{F}_p^*\} = A(g)\frac{x}{\log x} + O\left(\frac{x \log\log x}{(\log x)^2}\right). \tag{1.6}$$

For the special case $g = 2$ we have

$$A(2) = C_{Artin} := \prod_p \left(1 - \frac{1}{p(p-1)}\right).$$

In 1977, Lenstra [8] proved an asymptotic for Artin primes in arithmetic progressions. Namely, he proved, under GRH, that for $g \in \mathbb{Z}$ and $a, q \in \mathbb{N}$ coprime,

$$\#\{p \leq x : \langle g \rangle = \mathbb{F}_p^*,\ p \equiv a \mod q\} = \delta(g; q, a)\frac{x}{\log x} + o\left(\frac{x}{\log x}\right), \tag{1.7}$$

for some constant $\delta(g; q, a)$. Later, more work was done by Moree, Stevenhagen and Lenstra [14], [9] to simplify the expression for $\delta(g; q, a)$. This constant $\delta(g; q, a)$ can also be 0 if $g \neq -1, 0, 1$ is not a square, e.g. for $g = 2$ there are no primes $p \equiv \pm 1 \mod 8$ with $\langle 2 \rangle = \mathbb{F}_p^*$. Namely, for such a prime p, there is an $x \in \mathbb{Z}$ such that $x^2 \equiv 2 \mod p$, so by Fermat's little theorem we have $2^{\frac{p-1}{2}} = x^{p-1} \equiv 1 \mod p$.

Without GRH, there is not much proved yet. In 1985, Heath-Brown [4] proved unconditionally that for infinitely many primes p, either 2,3 or 5 is a primitive root.

1.3 New results: a Siegel–Walfisz theorem for Artin primes

The main topic of this thesis will be to prove a version of (1.7) with an explicit error term for the case $g = 2$. We shall focus on the case $g = 2$ for convenience of notation, but our arguments can be made to work for every admissible g. In [9] it is proved that the constant $\delta(2; m, a)$ in (1.7) equals

$$\delta(m, a) := \delta(2; m, a) = \frac{\mathbb{1}_{\{(a,m)=1\}}}{\phi(m)} \prod_{p \nmid m} \left(1 - \frac{1}{p(p-1)}\right) \prod_{\substack{p \mid m \\ p \mid a-1}} \left(1 - \frac{1}{p}\right) \left(1 - \mathbb{1}_{\{8|m\}} \left(\frac{2}{a}\right)\right), \tag{1.8}$$

where

$$\left(\frac{2}{a}\right) = \begin{cases} 1, & \text{if } a \equiv \pm 1 \mod 8, \\ -1, & \text{if } a \equiv \pm 3 \mod 8, \\ 0, & \text{if } 2 | a. \end{cases}$$

In the literature it's usual to denote the modulus of a progression with the letter q, but we switch to the letter m. This is because in [5] and in §3 the letter q denotes a prime.

Definition 1.3. Let

$$\pi_A(x; m, a) := \#\{p \leq x : \langle 2 \rangle = \mathbb{F}_p^*, p \equiv a \mod m\}.$$

The following theorem is the main result of this thesis.

Theorem 1.4. *Assume GRH. Let $J(x)$ be any function such that $\lim_{x \to \infty} J(x) = \infty$. Then for all $a, m \in \mathbb{N}$ with $(a, m) = 1$ and $2 \leq m \leq x^{\frac{1}{J(x)}}$, we have*

$$\pi_A(x; m, a) = \delta(m, a)\frac{x}{\log x} + O\left(\frac{x}{\phi(m) \log x} \frac{1}{\min\{J(x), \frac{\log x}{\log \log x}\}}\right),$$

where the implied constant in the error term is absolute.

This is the first time in the literature that the error term in Lenstra's result is made explicit. We will follow Hooley's proof of (1.6) for the case $g = 2$, as given in Chapter III from [6]. It is not difficult to modify the arguments of Hooley to obtain the error term $O\left(\frac{x}{\log x}\frac{1}{\min\{J(x),\frac{\log x}{\log\log x}\}}\right)$ with an implied constant depending on m, but we shall make the effort to get the extra saving from $\frac{1}{\phi(m)}$. This is important in applications, since it means that the error term becomes better when the modulus of the progression increases.

Lemma 1.5. *Let a, m and J be as in Theorem 1.4, and assume that $\delta(m,a) \neq 0$. If $\lim_{x\to\infty} \frac{\log\log x}{J(x)} = 0$, then*

$$\frac{x}{\phi(m)\log x}\frac{1}{\min\{J(x),\frac{\log x}{\log\log x}\}} = o\left(\delta(m,a)\frac{x}{\log x}\right).$$

This means that Theorem 1.4 gives a meaningful asymptotic if $\log\log x = o(J(x))$.

Proposition 1.6. *Assume GRH. Let $J(x)$ be any function such that $\lim_{x\to\infty} J(x) = \infty$. Fix $0 < \epsilon < \frac{1}{10}$. Then for all $2 \leq m \leq x^{\frac{1}{J(x)}}$ except at most $10\epsilon x^{\frac{1}{J(x)}}$, we get for all a coprime to m with $\delta(m,a) \neq 0$ that*

$$\pi_A(x;m,a) = \delta(m,a)\frac{x}{\log x}\left(1 + O\left(\frac{1}{\min\{J(x),\frac{\log x}{\log\log x}\}}\right)\right),$$

where the implied constant in the error term is absolute.

This means that Theorem 1.4 gives a meaningful asymptotic for all $m \leq x^{\frac{1}{J(x)}}$ except for at most $10\epsilon x^{\frac{1}{J(x)}}$ exceptional cases, *if $J(x)$ tends to infinity arbitrarily slowly.*

Choosing $J(x) = \frac{\log x}{B\log\log x}$ in Theorem 1.4, we get $x^{\frac{1}{J(x)}} = (\log x)^B$, which gives a slightly weaker formulation that is more suitable for applications.

Theorem 1.7. *Assume GRH, and let $B > 0$. Then for all $a, m \in \mathbb{N}$ with $(a,m) = 1$ and $2 \leq m \leq (\log x)^B$, we have*

$$\pi_A(x;m,a) = \delta(m,a)\frac{x}{\log x} + O\left(\frac{\max\{1,B\}}{\phi(m)}\frac{x\log\log x}{(\log x)^2}\right),$$

where the implied constant in the error term is absolute.

Theorems 1.4 and 1.7 can be viewed as an analogue of the Siegel–Walfisz theorem for Artin primes. Namely, one gets an asymptotic with an explicit error term for the number of Artin primes in an arithmetic progression under the assumption that the modulus of the progression is not too large compared to x. The error term of the Siegel–Walfisz theorem is better with respect to x, namely for each $C, D > 0$ one has $(\log x)^D = o\left(\mathrm{e}^{C\sqrt{\log x}}\right)$. However, Theorem 1.4 has the advantage that it can be applied for m in a much larger range, namely $m \leq x^{\frac{1}{J(x)}}$ compared to $m \leq (\log x)^A$ in the Siegel–Walfisz theorem. For example, choosing $J(x) = \sqrt{\log x}$ we can see that for each $A > 0$,

$$x^{\frac{1}{J(x)}} = \mathrm{e}^{\sqrt{\log x}} \gg (\log x)^A.$$

Most of §3 will be devoted to the proof of Theorem 1.4, and in the last part we prove Lemma 1.5 and Proposition 1.6.

1.4 New results: applications of Theorem 1.7

1.4.1 Artin primes p for which $p-1$ is squarefree

If p is a prime different from 3, then $p-1$ is not a prime. However, $p-1$ can still be squarefree.

Definition 1.8. Let $\pi_{A,S}(x)$ denote the number of Artin primes $p \leq x$ for which $p-1$ is squarefree.

Definition 1.9. For $a, q \in \mathbb{N}$ coprime, let

$$\delta^\natural(q,a) := \frac{\delta(q,a)}{C_{\text{Artin}}}.$$

That is, $\delta^\natural(q,a)$ is the density of Artin primes congruent to a mod q *within the Artin primes.*

Heuristically we can view $\delta^\natural(q,a)$ as the conditional probability that a prime p is a mod q, given that $\langle 2 \rangle = \mathbb{F}_p^*$.

Theorem 1.10. *Assume GRH. Then*

$$\pi_{A,S}(x) = C_{\text{Artin}} \left(\prod_l \left(1 - \delta^\natural(l^2,1)\right) \right) \frac{x}{\log x} + O\left(\frac{x \log\log x}{(\log x)^2} \right),$$

where the product is taken over all primes l. This product is absolutely convergent and positive.

The counting function $\pi_{A,S}(x)$ has not been studied before in the literature. We can give this theorem the following heuristical interpretation. Assume p is a random Artin prime. We can view $1 - \delta^\natural(l^2,1)$ as the probability that $l^2 \nmid (p-1)$. Assuming these events are pairwise independent for primes l, the probability that $p-1$ is squarefree equals $\prod_l \left(1 - \delta^\natural(l^2,1)\right)$. Then for p a random prime, the probability that p is an Artin prime and $p-1$ is squarefree, equals $C_{\text{Artin}} \prod_l \left(1 - \delta^\natural(l^2,1)\right)$. By Theorem 1.10, this is the density of such primes in the primes.

1.4.2 Integers as a sum of an Artin prime and a squarefree integer

The Goldbach conjecture states that every even number larger than 2 can be written as a sum of 2 primes. This is one of the most famous unsolved problems in number theory. However, by (1.4) we know that every large enough integer can be represented as the sum of a prime and a squarefree number.

Definition 1.11. For $N \in \mathbb{N}$, let $R(N)$ be the number of ways of writing N as a sum of an Artin prime and a squarefree number.

Theorem 1.12. *Assume GRH. Then*

$$R(N) = C_{Artin} \left(\prod_l \left(1 - \delta^\natural(l^2,N)\right) \right) \frac{N}{\log N} + O\left(\frac{N \log\log N}{(\log N)^2} \right).$$

The product $\prod_l \left(1 - \delta^\natural(l^2,N)\right)$ is absolutely convergent and positive.

The above theorem has also not been proved before. By Theorem 1.12, $R(N) \asymp \frac{N}{\log N} \to \infty$ as $N \to \infty$, so $R(N) > 0$ for N large enough.

Corollary 1.13. *Assume GRH. Then every large enough positive integer N can be written as $N = p + s$, with p an Artin prime and $s \in \mathbb{N}$ squarefree.*

We can give Theorem 1.12 the following heuristical interpretation. Assume $p \leq N - 1$ is a random Artin prime. Then from a heuristic similar to the one given for Theorem 1.10, we see that $\prod_l \left(1 - \delta^\natural(l^2, N)\right)$ is the probability that $N - p$ is squarefree. Now the number of Artin primes not exceeding $N - 1$ is roughly $C_{Artin} \frac{N}{\log N}$, hence we expect that there are $C_{\text{Artin}} \prod_l \left(1 - \delta^\natural(l^2, N)\right) \frac{N}{\log N}$ Artin primes $p \leq N$ for which $s = N - p$ is squarefree.

1.4.3 Proofs

Recall that (1.3) resp. (1.4) were proved using the Siegel–Walfisz theorem. To prove Theorem 1.10 and Theorem 1.12, in §4 we will follow the proofs of (1.3) resp. (1.4) as given in [12] resp. [21], but replace the Siegel–Walfisz theorem by Theorem 1.7. The proofs don't work if one uses (1.7) instead of Theorem 1.7, because they depend on the uniformity of the error term on m.

1.5 The Goldbach conjecture and the twin prime conjecture

A very famous open problem is the Goldbach conjecture, which states that every even integer larger than 2 is the sum of two primes. The Goldbach conjecture implies that every odd number larger than 5 is the sum of three primes, because one can add 3 to all even numbers. These problems are respectively called binary and ternary Goldbach.

Binary Goldbach is still unproved. However, using the circle method, Hardy and Littlewood [2] proved that, under assumption of GRH, every large enough odd integer is the sum of 3 primes. Improving the part of their proof concerning the so called minor arcs, Vinogradov managed to prove this unconditionally in 1937 [20]. More precisely, he proved that for each $A > 0$ the number of ways to write an integer N as a sum of 3 primes equals

$$\frac{N^2}{2(\log N)^3} \mathfrak{S}(N) + O\left(\frac{N^2}{(\log N)^A}\right),$$

where

$$\mathfrak{S}(N) = \prod_{p|N} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p \nmid N} \left(1 + \frac{1}{(p+1)^3}\right).$$

Another famous open problem is the twin prime conjecture. A prime twin is a pair of primes (p_1, p_2) with $p_2 = p_1 + 2$. The twin prime conjecture states that there are infinitely many of such pairs. In 2013, Zhang [22] proved that there are infinitely many pairs of primes with difference at most 70 million. This bound was reduced to 600 by Maynard [10], and then to 246 by various mathematicians in a Polymath project. Pollack [17] showed under assumption of GRH, that for some $C > 0$ are infinitely many pairs of Artin primes with difference at most C.

Hardy and Littlewood [2] conjectured that the number of twin primes not exceeding x is

$$2\left(\prod_{p\neq 2}\left(1-\frac{1}{(p-1)^2}\right)\right)\frac{x}{(\log x)^2}+o\left(\frac{x}{(\log x)^2}\right).$$

1.6 Diophantine equations & Artin's conjecture

Notation. Let $\mathcal{P}$ denote the set of all primes.

1.6.1 Goldbach conjecture with Artin primes

In §5, we consider a variant of the Goldbach problem: we shall study the number of representations of an integer as a sum of k Artin primes, for $k \geq 2$. This question has not been studied before in the literature.

Definition 1.14. Let, for $k \in \mathbb{Z}_{\geq 2}$,

$$A_k(N) := \#\big\{(p_1,...,p_k) \in \mathcal{P}^k : N = p_1 + ... + p_k,\ \forall i : \langle 2\rangle = \mathbb{F}_{p_i}^*\big\}.$$

Conjecture 1.15. *We have*

$$A_k(N) = \frac{C_{Artin}^k}{(k-1)!}\left(\prod_p \mathfrak{S}_p(N)\right)\frac{N^{k-1}}{(\log N)^k}+o\left(\frac{N^{k-1}}{(\log N)^k}\right),$$

where for $p > 2$,

$$\mathfrak{S}_p(N) := 1+\left(p-1-\frac{1}{p}\right)^{-k}\left((-1)^{k+1}\left(1+\frac{1}{p}\right)^k+(-1)^k p\sum_{\substack{0\leq m\leq k\\ m\equiv N \mod p}}\frac{\binom{k}{m}}{p^m}\right),$$

and where $\mathfrak{S}_2(N)$ is defined through table 1.1.

There is a natural way to define the p-adic factors, and this will be given in (5.1). However, the expression in (5.1) is not explicit and in particular it is not obvious whether it vanishes or not. The main aim of §5 is to use exponential sums to convert the expression from (5.1) into the explicit expression $\mathfrak{S}_p(N)$ defined in Conjecture 1.15. At the end of §5 we also prove the following proposition.

Proposition 1.16. *The product $\prod_p \mathfrak{S}_p(N)$ is absolutely convergent and for all $p > 2$ we have $\mathfrak{S}_2(N) > 0$. Hence, $\prod_p \mathfrak{S}_p(N) > 0$ if and only if $\mathfrak{S}_2(N) > 0$.*

Conjecture 1.15 and Proposition 1.16 combined suggest that $A_k(N) \to \infty$ for $\mathfrak{S}_2(N) > 0$, which suggests the following conjecture.

Table 1.1: Values of $\mathfrak{S}_2(N)$.

$N \mod 8$	$\mathfrak{S}_2(N)$	$\mathfrak{S}_2(N)$ if k is even	$\mathfrak{S}_2(N)$ if k is odd
0	$1+(-1)^k+\frac{2}{(\sqrt{2})^k}\left(1+(-1)^k\right)$	$2+\frac{4}{(\sqrt{2})^k}$	0
1	$1+(-1)^{k+1}+\frac{1}{(\sqrt{2})^{k-1}}\left((-1)^k-1\right)$	0	$2-\frac{2}{(\sqrt{2})^{k-1}}$
2	$1+(-1)^k$	2	0
3	$1+(-1)^{k+1}+\frac{1}{(\sqrt{2})^{k-1}}\left(1-(-1)^k\right)$	0	$2+\frac{2}{(\sqrt{2})^{k-1}}$
4	$1+(-1)^k-\frac{2}{(\sqrt{2})^k}\left(1+(-1)^k\right)$	$2-\frac{4}{(\sqrt{2})^k}$	0
5	$1+(-1)^{k+1}+\frac{1}{(\sqrt{2})^{k-1}}\left(1-(-1)^k\right)$	0	$2+\frac{2}{(\sqrt{2})^{k-1}}$
6	$1+(-1)^k$	2	0
7	$1+(-1)^{k+1}+\frac{1}{(\sqrt{2})^{k-1}}\left((-1)^k-1\right)$	0	$2-\frac{2}{(\sqrt{2})^{k-1}}$

Conjecture 1.17.
- *If $k \geq 4$ is even, then every large enough even integer N can be written as the sum of exactly k Artin primes.*
- *If $k \geq 3$ is odd, then every large enough odd integer N can be written as the sum of exactly k Artin primes.*
- *Every large enough integer N with $N \equiv 0, 2, 6 \mod 8$ can be written as the sum of exactly 2 Artin primes.*

Remark 1.18. Recall that Artin primes are $\pm 3 \mod 8$. Thus, if $p_1, ..., p_k$ are Artin primes, then $\sum_{i=1}^{k} p_i$ is even if k is even, and odd if k is odd. This explains why $\mathfrak{S}_2(N)$ is 0 if N is even and k is odd, and also if N is odd and k is even.
The only other case where $\mathfrak{S}_2(N)$ vanishes, is when $k = 2$ and $N \equiv 4 \mod 8$. If p_1 and p_2 are Artin primes, one easily checks that $p_1 + p_2 \equiv 0, 2, \text{ or } 6 \mod 8$. For $k > 2$ even, this problem disappears, because one has a sum of k terms

$$(3+3+3+3)+(3-3)+(3-3)+...+(3-3) \equiv 4 \mod 8.$$

1.6.2 Twin Artin primes

Next we consider pairs of Artin primes (p_1, p_2), with $p_1, p_2 \leq x$, such that $p_2 = p_1 + 2k$ for some fixed k. For the special case $k = 1$ these pairs are twin Artin primes.

Definition 1.19. Let

$$B_k(x) := \#\{(p_1, p_2) : \forall i \in \{1, 2\} : \langle 2 \rangle = \mathbb{F}_{p_i}^* \text{ and } p_i \leq x,\ p_2 = p_1 + 2k\}.$$

That is, $B_k(x)$ is the number of pairs of Artin primes up to x with difference $2k$.

First we investigate for which k the number $B_k(x)$ is non-zero. Recall that every Artin prime is congruent to 3 or 5 modulo 8. Assume that p_1 and p_2 are Artin primes such that $p_2 = p_1 + 2k$. Then the following are the possible cases for p_1 and p_2 mod 8:

- We have $p_1 \equiv p_2 \mod 8$ (both 3 or both 5 mod 8) if and only if $2k \equiv 0 \mod 8$, which is equivalent to $k \equiv 0 \mod 4$;
- We have $p_1 \equiv 3 \mod 8$ and $p_2 \equiv 5 \mod 8$ if and only if $2k \equiv 2 \mod 8$, which is equivalent to $k \equiv 1 \mod 4$;
- We have $p_1 \equiv 5 \mod 8$ and $p_2 \equiv 3 \mod 8$ if and only if $2k \equiv 6 \mod 8$, which is equivalent to $k \equiv 3 \mod 4$;

So we see that we cannot have $k \equiv 2 \mod 4$. In that case $2k \equiv 4 \mod 8$, but $3+4 \equiv 7 \mod 8$ and $5+4 \equiv 1 \mod 8$, so if p_1 is an Artin prime then $p_1 + 2k$ is not. So for $k \equiv 2 \mod 4$ we have $B_k(x) = 0$. Also, from these observations, heuristically one would expect that $B_k(x)$ is larger for $k \equiv 0 \mod 4$ than for k congruent to 1 or 3 mod 4. Namely, for $k \equiv 0 \mod 4$ there are two possibilities for p_1 and p_2 mod 8, and for k congruent to 1 or 3 mod 4 there is only one possibility for p_1 and p_2 mod 8.

Conjecture 1.20. *If $k \not\equiv 2 \mod 4$, then*

$$B_k(x) = U(k)C_{\text{Artin}}^2 \prod_{\substack{p>2 \\ p|k}} \left(1 + \frac{p^3-p^2-p-1}{(p^2-p-1)^2}\right) \prod_{\substack{p>2 \\ 2k \equiv \pm 1 (p)}} \left(1 - \frac{2p+1}{(p^2-p-1)^2}\right)$$
$$\prod_{\substack{p \nmid 2k \\ p \nmid (2k+1) \\ p \nmid (2k-1)}} \left(1 - \frac{(p+1)^2}{(p^2-p-1)^2}\right) \frac{x}{(\log x)^2} + o\left(\frac{x}{(\log x)^2}\right),$$

where

$$U(k) = \begin{cases} 4 & \text{if } k \equiv 0 \mod 4, \\ 2 & \text{if } k \equiv 1, 3 \mod 4. \end{cases}$$

The above conjecture is also original.

Remark 1.21. Note that in Conjecture 1.20 all the involved products have factors of the form $1 + O\left(\frac{1}{p^2}\right)$ and are therefore absolutely convergent. Because all the factors are positive, we see that these products are positive.

Remark 1.22. The fact that $U(k)$ is 2 times as big for $k \equiv 0 \mod 8$, may correspond to our observation that one can choose $p_1, p_2 \mod 8$ in 2 times as many ways. However, this does not take into account how the other 3 products behave as a function of k, so we have to be careful with this heuristical observation.

Substituting $k = 1$ in Conjecture 1.20 we get the following special case.

Conjecture 1.23. *The number of Artin prime twins up to x, that is $B_1(x)$, satisfies*

$$B_1(x) = \frac{36}{25} C_{\text{Artin}}^2 \prod_{p>3} \left(1 - \frac{(p+1)^2}{(p^2-p-1)^2}\right) \frac{x}{(\log x)^2} + o\left(\frac{x}{(\log x)^2}\right).$$

Conjecture 1.20 suggests that for $k \equiv 0, 1, 3 \mod 4$, there are infinitely many pairs of Artin primes with difference $2k$. We don't give the heuristic for Conjecture 1.20 in this thesis, because it is very similar to the heuristic for Conjecture 1.15.

2 Preliminaries

2.1 Notation

The following notations will be used throughout the thesis.

- For real-valued functions f, g, we use the following notations:
  - $f(x) = O(g(x))$, or $f(x) \ll g(x)$, if there are constants $x_0 \in \mathbb{R}$ and $C > 0$, such that for all $x > x_0$ we have $|f(x)| \leq C|g(x)|$;
  - For $A \subset \mathbb{R}$ we say that $f(x) \ll g(x)$ or $f(x) = O(g(x))$ for all $x \in A$, if there is a constant $C > 0$ such that for all $x \in A$ we have $|f(x)| \leq C|g(x)|$;
  - $f(x) = o(g(x))$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$;
  - $f(x) \asymp g(x)$ if there are constants $C, D > 0$ and $x_0 \in \mathbb{R}$ such that for all $x > x_0$ we have $C|g(x)| \leq |f(x)| \leq D|g(x)|$.
- We use the notation $\mathbb{N} = \{1, 2, 3....\} = \{n \in \mathbb{Z} : n > 0\}$.
- The letter p, p_i or p' will always denote a prime number.
- For $n \in \mathbb{N}$, $\tau(n)$ denotes the number of positive divisors of n, and $\omega(n)$ denotes the number of prime divisors of n.
- For $x \geq 2$, $\pi(x)$ denotes the number of primes not exceeding x, that is

$$\pi(x) := \sum_{p \leq x} 1 = \#\{p \leq x\}.$$

- For $q, a \in \mathbb{N}$ and $x \geq 2$, let

$$\pi(x; q, a) := \#\{p \leq x : p \equiv a \mod q\}.$$

- For $x \geq 2$ let

$$\mathrm{li}(x) := \int_2^x \frac{1}{\log u} \mathrm{d}u.$$

- For $a, b \in \mathbb{N}$, we use the notation $(a, b) := \gcd(a, b)$ and $[a, b] := \mathrm{lcm}(a, b)$.

2.2 Analytic number theory prerequisites

In this section we discuss some facts and techniques from analytic number theory that will be used.

Definition 2.1. Let A and B be subsets of $\mathbb{N}$ such that $B \subset A$. If the limit

$$\lim_{x\to\infty} \frac{\#\{n \in B : n \leq x\}}{\#\{n \in A : n \leq x\}}$$

exists, then it is called *the natural density of B in A*.

Lemma 2.2. *For each $n \in \mathbb{Z}_{>0}$ and each $\epsilon > 0$ we have*

$$2^{\omega(n)} \leq \tau(n) \ll n^{\epsilon}.$$

Proof. Because $2^{\omega(n)}$ is the number of squarefree divisors of n, we get $2^{\omega(n)} \leq \tau(n)$. See equation (2.19) and Theorem 2.11 from [13] for the proof of the upper bound for $\tau(n)$. □

Lemma 2.3. *For each integer $n \geq 10$ we have*

$$\phi(n) \gg \frac{n}{\log \log n}.$$

Proof. See Theorem 2.9 from [13]. □

We will also use a sharper bound for the number of prime divisors.

Lemma 2.4. *There exists a $C > 0$ such that for all $n \geq 10$ and let $2 \leq z \leq n$,*

$$\#\{p|n : p > z\} \leq \min\left\{\frac{C \log n}{\log \log n}, \frac{\log n}{\log z}\right\}.$$

Proof. In Theorem 2.10 from [13] it is proved that there is a $C > 0$ such that for all $n \geq 10$,

$$\omega(n) \leq \frac{C \log n}{\log \log n},$$

and we have the trivial bound

$$\{p|n : p > z\} \leq \omega(n).$$

If $p_1, ..., p_k$ are the different prime divisors of n greater than z, then $n \geq p_1 \cdots p_k > z^k$. Therefore $k \leq \frac{\log n}{\log z}$. □

Lemma 2.5. *For $x \geq 2$ we have*

$$\prod_{p \leq x} p \leq 4^x.$$

Proof. This was proved by Chebychev. In [3], paragraph 22.3, Bertrand's Postulate is proved, and this lemma is a part of the proof. Bertrand's postulate states that for every $n \in \mathbb{Z}_{\geq 2}$ there is a prime $n < p < 2n$. □

Lemma 2.6. ***(Brun–Titchmarsh)*** *There is an absolute constant $C > 0$ such that for all $a, q \in \mathbb{N}$ coprime with $q \leq x$ we have*

$$\pi(x; q, a) \leq \frac{Cx}{\phi(q) \log\left(\frac{2x}{q}\right)}. \tag{2.1}$$

Proof. In fact, at page 153 from [16] it's stated that for each $\epsilon > 0$ there is an $x_0(\epsilon) > 0$ such that for all $a, q \in \mathbb{N}$ coprime with $q \leq x$ and $x > x_0(\epsilon)$, (2.1) holds with $C = 2 + \epsilon$. □

There is also a trivial bound for $\pi(x; q, a)$, which for large q is more useful than Lemma 2.6.

Lemma 2.7. *Let $a, q \in \mathbb{N}$ and let $x \geq 1$. Then*

$$\pi(x; q, a) \leq 1 + \frac{x}{q}.$$

Proof. We can bound $\pi(x; q, a)$ by the total number of integers $1 \leq n \leq x$ with $n \equiv a \mod q$, which is at most $\frac{x}{q} + 1$. □

Definition 2.8. A map $f : \mathbb{N} \to \mathbb{C} \setminus \{0\}$ is called *multiplicative* if for all $a, b \in \mathbb{N}$ coprime, we have $f(ab) = f(a)f(b)$.

Equation (1.11) from [7] is presented in the following lemma.

Lemma 2.9. ***(Euler product)*** *Let $f : \mathbb{N} \to \mathbb{C} \setminus \{0\}$ be a multiplicative function. If the series $\sum_{n=1}^{\infty} f(n)$ converges absolutely, then it equals*

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} \left(\sum_{j=0}^{\infty} f(p^j) \right).$$

For $f : \mathbb{N} \to \mathbb{C}$ multiplicative, we write

$$\sigma_p(f) := \sum_{j=0}^{\infty} f\left(p^j\right) p^{-j},$$

if the above series is absolutely convergent.

Lemma 2.10. *Let $f : \mathbb{N} \to \mathbb{R}_{\geq 1}$ be a multiplicative function which is non-decreasing on the prime powers, that is for each prime p and each $n \geq \mathbb{N}$ we have $f\left(p^n\right) \geq f\left(p^{n-1}\right)$. Then, for each $x \geq 1$ we have*

$$\sum_{n \leq x} f(n) \leq x \prod_{p \leq x} \sigma_p(f) \left(1 - \frac{1}{p}\right).$$

Proof. See equation (1.79) in [7]. □

The Euler–Maclaurin summation formula helps us to estimate a sum as an integral. It is treated in Appendix B from [13].

Lemma 2.11. *Let $a, b \in \mathbb{R}$ with $a < b$ and let $f : [a, b] \to \mathbb{C}$ be a continuously differentiable function. Then*

$$\sum_{a \leq n \leq b} f(n) = \int_a^b f(u)\mathrm{d}u + f(a) + \int_a^b (u - [u]) f'(u)\mathrm{d}u.$$

Lemma 2.12. *For every $N \in \mathbb{Z}_{>0}$,*

$$\mathrm{li}(x) = \frac{x}{\log x} + \frac{2!x}{(\log x)^2} + ... + \frac{N!x}{(\log x)^N} + O_N\left(\frac{x}{(\log x)^{N+1}}\right).$$

Proof. This follows by induction to N and partial integration. □

Before we state the next theorem, we recall that the Euler–Mascheroni constant γ is defined by

$$\gamma := \lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{1}{k} - \log n\right).$$

Lemma 2.13. ***(Mertens' estimates)*** *(i) There is a constant $c \in \mathbb{R}$ such that for all $x \geq 2$ we have*

$$\sum_{p\leq x}\frac{1}{p} = \log\log x + c + O\left(\frac{1}{\log x}\right).$$

(ii) For $x \geq 2$, we have

$$\prod_{p\leq x}\left(1-\frac{1}{p}\right) = \frac{e^{-\gamma}}{\log x}\left(1+O\left(\frac{1}{\log x}\right)\right).$$

Proof. See [11]. □

3 Artin primes in arithmetic progressions

3.1 Preparations for the proof of Theorem 1.4

Notation. In this section the letter q will always denote a prime.

The proof of the next lemma is standard.

Lemma 3.1. *Let p be an odd prime. Then the following assertions are equivalent.*
i) *2 is a primitive root mod p;*
ii) *for every prime divisor q of $p-1$ we have $2^{\frac{p-1}{q}} \not\equiv 1 \mod p$;*
iii) *for every prime divisor q of $p-1$ there is no $x \in \mathbb{Z}$ such that $x^q \equiv 2 \mod p$.*

Definition 3.2. We let $\mathfrak{P}_1$ be the set of all primes, and for any prime q,

$$\mathfrak{P}_q := \{p : q|p-1 \text{ and } 2^{\frac{p-1}{q}} \equiv 1 \mod p\}.$$

For $k \in \mathbb{N}$ squarefree, we let

$$\mathfrak{P}_k := \bigcap_{q|k}\mathfrak{P}_q.$$

From Lemma 3.1 it follows that

$$\pi_A(x;m,a) = \#\{p \leq x : p \equiv a \mod m, \forall q : p \notin \mathfrak{P}_q\}.$$

If $p \in \mathfrak{P}_q$ and $p \leq x$, then $q|p-1$ and thus $q \leq x-1$, therefore

$$\pi_A(x;m,a) = \#\{p \leq x : p \equiv a \mod m, \forall q \leq x-1 : p \notin \mathfrak{P}_q\}.$$

The proof of the next lemma is also standard.

Lemma 3.3. *For $k \in \mathbb{N}$ squarefree, we have $\mathfrak{P}_k = \{p : k|p-1$ and $2^{\frac{p-1}{k}} \equiv 1 \mod p\}$.*

Definition 3.4. Let $m \in \mathbb{N}$ and let $1 \leq a \leq m$ be coprime to m.
Let, for $x, \eta \in \mathbb{R}_{>0}$,

$$N_{m,a}(x,\eta) := \#\{p \leq x : p \equiv a \mod m \text{ and } \forall\ q \leq \eta : p \notin \mathfrak{P}_q\}.$$

For $x, \eta_1, \eta_2 \in \mathbb{R}_{>0}$ with $\eta_2 > \eta_1$, let

$$M_{m,a}(x,\eta_1,\eta_2) := \#\{p \leq x : p \equiv a \mod m \text{ and } \exists\ \eta_1 < q \leq \eta_2 : p \in \mathfrak{P}_q\}.$$

Definition 3.5. Let $m \in \mathbb{N}$ and let $1 \leq a \leq m$ be coprime to m. For k squarefree and $x > 0$, let

$$\pi_k(x;m,a) := \#\{p \leq x : p \equiv a \mod m \text{ and } p \in \mathfrak{P}_k\}.$$

It turns out that $p \in \mathfrak{P}_k$ if and only if p splits completely in the number field $\mathbb{Q}(e^{\frac{2\pi i}{k}}, \sqrt[k]{2})$. The following theorem is standard and can be deduced by combining the work of Serre [18] with the algebraic number theory arguments in [8], [9] and [14].

Lemma 3.6. *Assume GRH. Let $k \in \mathbb{N}$ be squarefree, let $m \in \mathbb{N}$ and let $1 \leq a \leq m$ be coprime to m. Assume that $2 \leq m \leq x$ and that $1 \leq k \leq x$. Then*

$$\pi_k(x;m,a) = \frac{c(k,m,a)}{k\phi([m,k])}\mathrm{li}(x) + O\left(\sqrt{x}\log x\right),$$

where

$$c(k,m,a) = \begin{cases} 0, & \text{if } a \not\equiv 1 \mod (m,k), \\ 0, & \text{if } a \equiv 1 \mod (m,k) \text{ and } 2|k \text{ and } 8|m \text{ and } a \equiv \pm 3 \mod 8, \\ \epsilon(m,k), & \text{else,} \end{cases}$$

$$\epsilon(m,k) = \begin{cases} 2, & \text{if } 2|k \text{ and } 8|m, \\ 1, & \text{else,} \end{cases}$$

and the implied constant is absolute.

Proof of Theorem 1.4

Let $0 < \xi_1 < \xi_2 < \xi_3 < x-1$ be functions such that $\lim_{x\to\infty} \xi_i(x) = \infty$ $(i = 1,2,3)$. We will choose the functions ξ_i at the end of the proof. It is obvious that

$$N_{m,a}(x,\xi_1) - \pi_A(x;m,a) \ll \sum_{i=1}^{2} M_{m,a}(x,\xi_i,\xi_{i+1}) + M_{m,a}(x,\xi_3,x-1). \tag{3.1}$$

3.2 Bounding $M_{m,a}(x,\xi_3,x-1)$

If p is counted by $M_{m,a}(x,\xi_3,x-1)$, then there is a $\xi_3 < q \leq x-1$ such that $q|(p-1)$ and $p|\left(2^{\frac{p-1}{q}}-1\right)$. Because $\frac{p-1}{q} \leq \frac{x}{\xi_3}$, we see that p divides the product $\prod_{1\leq t\leq \frac{x}{\xi_3}} (2^t-1)$. Therefore,

$$M_{m,a}(x,\xi_3,x-1) \leq \#\left\{p : p \equiv a \mod m \text{ and } p|\prod_{1\leq t\leq \frac{x}{\xi_3}} \left(2^t-1\right)\right\}.$$

Letting $p_1 < p_2 < ... < p_l$ be counted on the right side, we get

$$\prod_{1\leq t\leq \frac{x}{\xi_3}} \left(2^t - 1\right) \geq p_1 p_2 \cdots p_l \geq a(a+m)(a+2m)\cdots(a+(l-1)m) \geq m^{l-1}.$$

It follows from this that $(l-1)\log m$ is at most

$$\sum_{1\leq t\leq \frac{x}{\xi_3}} \log\left(2^t - 1\right) \ll \frac{x^2}{{\xi_3}^2}. \tag{3.2}$$

Combining the estimates so far yields the next result.

Lemma 3.7. *If $\xi_3 \leq x - 1$, then the following holds with an absolute implied constant,*

$$M_{m,a}(x, \xi_3, x-1) \ll \frac{x^2}{{\xi_3}^2 \log(2m)}.$$

3.3 Bounding $M_{m,a}(x, \xi_2, \xi_3)$

It is obvious that

$$M_{m,a}(x, \xi_2, \xi_3) \leq \sum_{\xi_2 < q \leq \xi_3} \#\{p \leq x : p \equiv a \mod m \text{ and } p \equiv 1 \mod q\}. \tag{3.3}$$

The two progressions can be combined into a single progression mod $[m, q]$. By Lemma 2.6 we get a good upper bound if $[m, q]$ is large, which happens when $q \nmid m$. The cases $q|m$ give a bad upper bound but we will see that they are rare.

Case i) Assume $q|m$. If $a \equiv 1 \mod q$, then the condition $p \equiv a \mod m$ implies the other condition $p \equiv 1 \mod q$. If $a \not\equiv 1 \mod q$, then the conditions $p \equiv a \mod m$ and $p \equiv 1 \mod q$ cannot both be satisfied. We conclude that in this case

$$\{p \leq x : p \equiv a \mod m \text{ and } p \equiv 1 \mod q\} = \mathbb{1}_{\{a \equiv 1 \mod q\}} \pi(x; m, a),$$

which by Lemma 2.6 and Lemma 2.7 is

$$\ll \min\left\{\frac{x}{\phi(m)\log\left(\frac{2x}{m}\right)}, \frac{x}{m}\right\}.$$

Case ii) Assume $q \nmid m$. By the Chinese remainder theorem there is a unique $y \mod mq$ such that

$$p \equiv a \mod m \text{ and } p \equiv 1 \mod q \iff p \equiv y \mod mq.$$

Thus we get, again by Lemma 2.6 and Lemma 2.7,

$$\{p \leq x : p \equiv a \mod m \text{ and } p \equiv 1 \mod q\} \leq \min\left\{\frac{2x}{\phi(m)(q-1)\log\left(\frac{2x}{mq}\right)}, \frac{x}{mq} + 1\right\}.$$

Now we split the sum in (3.3) in terms with $q|m$ and terms with $q \nmid m$, and apply the above cases to bound $M_{m,a}(x, \xi_2, \xi_3)$ by

$$\ll \sum_{\substack{\xi_2 < q \le \xi_3 \\ q|m}} \min\left\{\frac{x}{\phi(m)\log\left(\frac{2x}{m}\right)}, \frac{x}{m}\right\} + \sum_{\substack{\xi_2 < q \le \xi_3 \\ q\nmid m}} \min\left\{\frac{x}{\phi(m)(q-1)\log\left(\frac{2x}{mq}\right)}, \frac{x}{mq}+1\right\}. \quad (3.4)$$

Clearly, in the first sum the number of terms is bounded by the number of prime divisors of m which are greater than ξ_2. Therefore by Lemma 2.4 this first sum in (3.4) is

$$\ll \min\left\{\frac{\log m}{\log\log m}, \frac{\log m}{\log \xi_2}\right\} \cdot \min\left\{\frac{x}{\phi(m)\log\left(\frac{2x}{m}\right)}, \frac{x}{m}\right\}. \quad (3.5)$$

Assuming that $m\xi_3 \le x$, the second sum in (3.4) is

$$\ll \frac{x}{m} \sum_{\substack{\xi_2 < q \le \xi_3 \\ q\nmid m}} \frac{1}{q} \ll \frac{x}{m} \sum_{\xi_2 < q \le \xi_3} \frac{1}{q}.$$

Assuming $\xi_3 \ge \mathrm{e}^{\mathrm{e}}\xi_2$, we have by Lemma 2.13,

$$\sum_{\xi_2 < q \le \xi_3} \frac{1}{q} = \log\left(\frac{\log \xi_3}{\log \xi_2}\right) + O\left(\frac{1}{\log \xi_2}\right).$$

The second sum in (3.4) is also bounded by

$$\ll \frac{x}{\phi(m)\log\left(\frac{2x}{m\xi_3}\right)} \sum_{\xi_2 < q \le \xi_3} \frac{1}{q} \ll \frac{x}{\phi(m)\log\left(\frac{2x}{m\xi_3}\right)} \log\left(\frac{\log \xi_3}{\log \xi_2}\right). \quad (3.6)$$

We have therefore proved the following estimate.

Lemma 3.8. *If $m\xi_3 \le x$ and $\xi_3 \ge \mathrm{e}^{\mathrm{e}}\xi_2$, then*

$$M_{m,a}(x, \xi_2, \xi_3) \ll \min\left\{\frac{\log m}{\log\log m}, \frac{\log m}{\log \xi_2}\right\} \min\left\{\frac{x}{\phi(m)\log\left(\frac{2x}{m}\right)}, \frac{x}{m}\right\} + \frac{x\log\left(\frac{\log \xi_3}{\log \xi_2}\right)}{\max\left\{m, \phi(m)\log\left(\frac{2x}{m\xi_3}\right)\right\}}.$$

Corollary 3.9. *Assume that $m\xi_3 \le x$, $\xi_3 \ge \mathrm{e}^{\mathrm{e}}\xi_2$, and that there is an $0 < A < 1$ such that $m \le \frac{x^{1-A}}{\xi_3}$. Then*

$$M_{m,a}(x, \xi_2, \xi_3) \ll \frac{x}{\phi(m)\log x}\left(\frac{\log m}{\log \xi_2} + \log\left(\frac{\log \xi_3}{\log \xi_2}\right)\right),$$

where the implied constant depends at most on A.

Proof. In this case we have $\log\left(\frac{2x}{m}\right) \gg \log x$. Therefore we can bound the first term in Lemma 3.8 by

$$\ll \frac{\log m}{\log \xi_2} \frac{x}{\phi(m)\log\left(\frac{2x}{m}\right)} \ll \frac{\log m}{\log \xi_2} \frac{x}{\phi(m)\log x}.$$

Also $\frac{x}{m\xi_3} \gg x^A$, so $\log\left(\frac{2x}{m\xi_3}\right) \gg \log x$. Therefore we can bound the second term in Lemma 3.8 by

$$\ll \frac{x}{\phi(m)\log x} \log\left(\frac{\log \xi_3}{\log \xi_2}\right).$$

□

3.4 Bounding $M_{m,a}(x, \xi_1, \xi_2)$

By Lemma 3.6 we can bound $M_{m,a}(x, \xi_1, \xi_2)$ by

$$\ll \sum_{\xi_1 < q \le \xi_2} \pi_q(x; m, a) \ll \sum_{\xi_1 < q \le \xi_2} \left(\frac{\mathrm{li}(x)}{q\phi([m,q])} + O\left(\sqrt{x}\log x\right) \right).$$

Using $\pi(\xi_2) \ll \frac{\xi_2}{\log \xi_2}$, the second term makes the following contribution,

$$\ll \frac{\xi_2}{\log \xi_2} \sqrt{x} \log x.$$

We split the first sum over q in terms with $q|m$ and terms with $q \nmid m$. If $q \nmid m$, then by the identity $\phi([m,q]) = \phi(m)(q-1)$ we get

$$\sum_{\substack{\xi_1 < q \le \xi_2 \\ q \nmid m}} \left(\frac{1}{q\phi([m,q])} \right) \ll \frac{1}{\phi(m)} \sum_{\xi_1 < q \le \xi_2} \frac{1}{q^2} \ll \frac{1}{\phi(m)} \frac{1}{\xi_1 \log \xi_1},$$

where the estimate $\sum_{q > \alpha} \frac{1}{q^2} \ll \frac{1}{\alpha \log \alpha}$ can be easily proved via partial summation.

For $q|m$ we have $[q,m] = m$, so

$$\sum_{\substack{\xi_1 < q \le \xi_2 \\ q | m}} \frac{1}{q\phi([m,q])} = \frac{1}{\phi(m)} \sum_{\substack{\xi_1 < q \le \xi_2 \\ q | m}} \frac{1}{q}.$$

By Lemma 2.4, m has at most $\frac{\log m}{\log \xi_1}$ prime divisors $q > \xi_1$, therefore

$$\sum_{\substack{\xi_1 < q \le \xi_2 \\ q | m}} \frac{1}{q} \le \frac{\log m}{\log \xi_1} \frac{1}{\xi_1}.$$

Lemma 3.10. *We have*

$$M_{m,a}(x, \xi_1, \xi_2) \ll \frac{\log m}{\phi(m)\xi_1 \log \xi_1} \frac{x}{\log x} + \sqrt{x} \log x \frac{\xi_2}{\log \xi_2}.$$

3.5 The main term $N_{m,a}(x, \xi_1)$

In this subsection we assume that $4^{\xi_1} \le x$, and for $k \in \mathbb{N}$ we denote by $P^+(k)$ the greatest prime divisor of k. By the inclusion-exclusion principle we have

$$N_{m,a}(x, \xi_1) = \sum_{\substack{k \in \mathbb{N} \\ P^+(k) \le \xi_1}} \mu(k) \pi_k(x; m, a).$$

By Lemma 2.5, every k in the sum is

$$\le \prod_{p \le \xi_1} p \le 4^{\xi_1} \le x.$$

By Lemma 3.6 we have

$$N_{m,a}(x,\xi_1) = \sum_{\substack{k\in\mathbb{N}\\ P^+(k)\le\xi_1}} \mu(k)\left(\frac{c(k,m,a)}{k\phi([m,k])}\mathrm{li}(x) + O\left(\sqrt{x}\log x\right)\right),$$

and the error term is $\ll 4^{\xi_1}\sqrt{x}\log x$.

$$\pi_k(x;m,a) = \frac{c(k,m,a)}{k\phi([m,k])}\mathrm{li}(x) + O\left(\sqrt{x}\log x\right),$$

Because of the identity $\phi([m,k]) = \frac{\phi(m)\phi(k)}{\phi((m,k))}$ we have thus far proved

$$N_{m,a}(x,\xi_1) = \frac{\mathrm{li}(x)}{\phi(m)} \sum_{\substack{k\in\mathbb{N}\\ P^+(k)\le\xi_1}} \frac{\mu(k)c(k,m,a)\phi((m,k))}{k\phi(k)} + O\left(4^{\xi_1}\sqrt{x}\log x\right). \tag{3.7}$$

We will now complete the series trying to minimize the error in the tail. To get the best bound we need to make use of the multiplicative properties of $c(k,m,a)$.

3.5.1 Case 1: 8 does not divide m

Definition 3.11. Define the functions

$$\mathbb{1} : \mathbb{N} \to \{0,1\},\ \mathbb{1}(k) := \begin{cases} 1, & \text{if } a \equiv 1 \mod (m,k), \\ 0, & \text{else,} \end{cases}$$

and

$$g : \mathbb{N} \to \mathbb{R},\ g(k) := \frac{\mu(k)\phi((m,k))}{k\phi(k)}\mathbb{1}(k).$$

We see from this definition that

$$\sum_{\substack{k\in\mathbb{N}\\ P^+(k)\le\xi_1}} \frac{\mu(k)c(k,m,a)\phi((m,k))}{k\phi(k)} = \sum_{\substack{k\in\mathbb{N}\\ P+(k)\le\xi_1}} g(k). \tag{3.8}$$

It is easy to check that g is multiplicative, hence

$$\sum_{\substack{k\in\mathbb{N}\\ P+(k)\le\xi_1}} g(k) = \prod_p (1+g(p)) \prod_{p>\xi_1}\left(\frac{1}{1+g(p)}\right). \tag{3.9}$$

To justify the last step, note that $\prod_p(1+g(p))$ is a non-zero absolutely convergent product,

because $|g(p)| \leq \frac{m}{p(p-1)}$ and $g(p) \neq -1$. Now using $\log\left(\frac{1}{1-x}\right) = O(x)$ when $|x| \leq \frac{1}{2}$, we get

$$\begin{aligned}\log\left(\prod_{p>\xi_1}\frac{1}{1+g(p)}\right) &= \sum_{p>\xi_1}\log\left(\frac{1}{1+g(p)}\right)\\ &\ll \sum_{p>\xi_1}|g(p)|\\ &\ll \sum_{p>\xi_1}\frac{\phi((m,p))}{p(p-1)}\\ &= \sum_{\substack{p>\xi_1\\ p|m}}\frac{1}{p}+\sum_{\substack{p>\xi_1\\ p\nmid m}}\frac{1}{p(p-1)} \ll \frac{\log(2m)}{\xi_1\log\xi_1}.\end{aligned}$$

Now we use the above estimate together with $e^x = 1+O(x)$, when $|x| \leq \frac{1}{2}$, to get

$$\prod_{p>\xi_1}\frac{1}{1+g(p)} = \mathrm{e}^{\log\left(\prod_{p>\xi_1}\frac{1}{1+g(p)}\right)} = 1+O\left(\frac{\log(2m)}{\xi_1\log\xi_1}\right)$$

Putting everything together we get

$$\sum_{\substack{k\in\mathbb{N}\\ P^+(k)\leq\xi_1}} g(k) = \prod_p(1+g(p))\left(1+O\left(\frac{\log(2m)}{\xi_1\log\xi_1}\right)\right).$$

Next we calculate the product $\prod_p(1+g(p))$. If $p|m$ then $(m,p)=p$, so

$$\mathbb{1}(p) = \begin{cases}1, & \text{if } a\equiv 1 \mod p,\\ 0, & \text{else.}\end{cases}$$

If $p\nmid m$ then $(m,p)=1$, so $\mathbb{1}(p)=1$. Using this we get

$$\prod_p(1+g(p)) = \prod_{\substack{p|m\\ p|a-1}}\left(1-\frac{1}{p}\right)\prod_{p\nmid m}\left(1-\frac{1}{p(p-1)}\right).$$

Because the above is an absolutely convergent product, we have the next result.

Lemma 3.12. *One has*

$$\sum_{\substack{k\in\mathbb{N}\\ P^+(k)\leq\xi_1}} g(k) = \prod_{\substack{p|m\\ p|a-1}}\left(1-\frac{1}{p}\right)\prod_{p\nmid m}\left(1-\frac{1}{p(p-1)}\right)+O\left(\frac{\log(2m)}{\xi_1\log\xi_1}\right).$$

Substituting this in (3.8) yields the next result.

Lemma 3.13. *If $8\nmid m$, then*

$$\sum_{\substack{k\in\mathbb{N}\\ P^+(k)\leq\xi_1}}\frac{\mu(k)c(k,m,a)\phi((m,k))}{k\phi(k)} = \prod_{\substack{p|m\\ p|a-1}}\left(1-\frac{1}{p}\right)\prod_{p\nmid m}\left(1-\frac{1}{p(p-1)}\right)+O\left(\frac{\log(2m)}{\xi_1\log\xi_1}\right).$$

3.5.2 Case 2: 8 divides m and $a \equiv \pm 3 \mod 8$

Definition 3.14. Define the function $R : \mathbb{N} \to \{0, 1\}$ by

$$R(k) := \begin{cases} 1, & \text{if } k \text{ is odd,} \\ 0, & \text{if } k \text{ is even.} \end{cases}$$

In this case we have

$$\sum_{\substack{k \in \mathbb{N} \\ P^+(k) \leq \xi_1}} \frac{\mu(k)c(k, m, a)\phi((m, k))}{k\phi(k)} = \sum_{\substack{k \in \mathbb{N} \\ P^+(k) \leq \xi_1}} g(k)R(k). \tag{3.10}$$

In the same manner how we proved Lemma 3.12, one can prove that

$$\sum_{\substack{k \in \mathbb{N} \\ P^+(k) \leq \xi_1}} g(k)R(k) = 2 \prod_p (1 + g(p)) \prod_{p > \xi_1} \left(\frac{1}{1 + g(p)} \right). \tag{3.11}$$

Applying the calculations of case 1 we now get the next result.

Lemma 3.15. *If* $8|m$ *and* $a \equiv \pm 3 \mod 8$*, then*

$$\sum_{\substack{k \in \mathbb{N} \\ P^+(k) \leq \xi_1}} \frac{\mu(k)c(k, m, a)\phi((m, k))}{k\phi(k)} = 2 \prod_{\substack{p|m \\ p|a-1}} \left(1 - \frac{1}{p}\right) \prod_{p \nmid m} \left(1 - \frac{1}{p(p-1)}\right) + O\left(\frac{\log(2m)}{\xi_1 \log \xi_1}\right).$$

3.5.3 Case 3: 8 divides m and $a \equiv \pm 1 \mod 8$

In this case we have

$$\sum_{\substack{k \in \mathbb{N} \\ P^+(k) \leq \xi_1}} \frac{\mu(k)c(k, m, a)\phi((m, k))}{k\phi(k)} = 2 \sum_{k=1}^{\infty} g(k) - \sum_{k=1}^{\infty} g(k)R(k). \tag{3.12}$$

Combining this with (3.9) and (3.11) yields the next result.

Lemma 3.16. *If* $8|m$ *and* $a \equiv \pm 1 \mod 8$*, then*

$$\sum_{\substack{k \in \mathbb{N} \\ P^+(k) \leq \xi_1}} \frac{\mu(k)c(k, m, a)\phi((m, k))}{k\phi(k)} = 0.$$

3.5.4 Putting it all together

Recalling the definition of $\delta(m, a)$, we see that the next result follows from the Lemma's 3.13, 3.15 and 3.16.

Lemma 3.17. *We have*

$$\sum_{\substack{k \in \mathbb{N} \\ P^+(k) \leq \xi_1}} \frac{\mu(k)c(k, m, a)\phi((m, k))}{k\phi(k)} = \phi(m)\delta(m, a) + O\left(\frac{\log(2m)}{\xi_1 \log \xi_1}\right). \tag{3.13}$$

Substituting (3.13) in (3.7) yields the final expression for the main term, given in the next lemma.

Lemma 3.18. *Assume that* $4^{\xi_1} \le x$. *Then*

$$N_{m,a}(x,\xi_1) = \delta(m,a)\mathrm{li}(x) + O\left(\frac{x}{\phi(m)\log x}\frac{\log(2m)}{\xi_1\log\xi_1}\right) + O(4^{\xi_1}\sqrt{x}\log x).$$

3.6 Conclusion of the proof of Theorem 1.4

Combining (3.1) with the Lemma's 3.7, 3.8, 3.10, and 3.18 yields the next result.

Proposition 3.19. *If* $m\xi_3 \le x$, $\xi_3 \ge \mathrm{e}^{\mathrm{e}}\xi_2$ *and* $4^{\xi_1} \le x$, *then* $\pi_A(x;m,a) - \delta(m,a)\mathrm{li}(x)$ *is*

$$\ll 4^{\xi_1}\sqrt{x}\log x + \frac{x}{\phi(m)\log x}\frac{\log(2m)}{\xi_1\log\xi_1} \tag{3.14}$$

$$+ \frac{x^2}{{\xi_3}^2\log(2m)} + \sqrt{x}\log x\frac{\xi_2}{\log\xi_2} \tag{3.15}$$

$$+ \min\left\{\frac{\log m}{\log\log m}, \frac{\log m}{\log\xi_2}\right\}\min\left\{\frac{x}{\phi(m)\log\left(\frac{2x}{m}\right)}, \frac{x}{m}\right\} + \frac{x\log\left(\frac{\log\xi_3}{\log\xi_2}\right)}{\max\left\{m, \phi(m)\log\left(\frac{2x}{m\xi_3}\right)\right\}}. \tag{3.16}$$

Remark 3.20. By Corollary 3.9, if there is an $0 < A < 1$ such that $m \le \frac{x^{1-A}}{\xi_3}$, then we can replace the terms in (3.16) by

$$\frac{x}{\phi(m)\log x}\left(\log\left(\frac{\log\xi_3}{\log\xi_2}\right) + \frac{\log m}{\log\xi_2}\right).$$

Let $J(x)$ be a function with $\lim_{x\to\infty} J(x) = \infty$, and assume that $m \le x^{\frac{1}{J(x)}}$. Let's choose

$$\xi_1 = \frac{1}{6}\log x, \quad \xi_2 = \sqrt{x}(\log x)^{-2}x^{-\frac{1}{J(x)}}, \quad \xi_3 = \sqrt{x}(\log x)^2 x^{\frac{1}{J(x)}}.$$

Note that the conditions from Proposition 3.19 are satisfied. Now the goal is to prove Theorem 1.4 by estimating all the error terms in Proposition 3.19.

3.6.1 Error terms in (3.14)

We have $4^{\xi_1} = x^{\frac{1}{6}\log 4}$, and thus $4^{\xi_1}\sqrt{x}\log x \ll x^{0.9}$. Because $m \le x^{\frac{1}{J(x)}}$, we have $\log m \le \frac{1}{J(x)}\log x$, so the second term in (3.14) is

$$\ll \frac{x}{\phi(m)\log x}\frac{1}{J(x)\log\log x}.$$

3.6.2 Error terms in (3.15)

Because $\phi(m) \le m \le x^{\frac{1}{J(x)}}$ and $\log(2m) \gg 1$, we have

$$\frac{x^2}{{\xi_3}^2\log(2m)} \ll \frac{x}{(\log x)^4 x^{\frac{2}{J(x)}}} \ll \frac{x}{\phi(m)(\log x)^2},$$

Notice that

$$\xi_2 \ll \frac{\sqrt{x}}{(\log x)^2\phi(m)},$$

and because $\log \xi_2 \gg \log x$, we get

$$\sqrt{x}\log x\frac{\xi_2}{\log \xi_2} \ll \frac{x}{\phi(m)(\log x)^2}.$$

3.6.3 Error terms in (3.16)

We have $m \leq \frac{x^{1-A}}{\xi_3}$ for $A = \frac{1}{4}$. Indeed, we have $\xi_3 \ll_\epsilon x^{\frac{1}{2}+\epsilon}$, so

$$\frac{x^{1-\frac{1}{4}}}{\xi_3} \gg_\epsilon x^{\frac{1}{4}-\epsilon} \geq m.$$

So the error term in (3.16) is, as explained in Remark 3.20,

$$\ll \frac{x}{\phi(m)\log x}\left(\log\left(\frac{\log \xi_3}{\log \xi_2}\right) + \frac{\log m}{\log \xi_2}\right).$$

We have $\log \xi_2 \gg \log x$ and $\log m \ll \frac{1}{J(x)}\log x$, and thus

$$\frac{\log m}{\log \xi_2} \ll \frac{1}{J(x)}.$$

Furthermore, due to our choice of ξ_2 and ξ_3 we have

$$\log\left(\frac{\log \xi_3}{\log \xi_2}\right) = \log\left(\frac{\frac{1}{2}\log x + 2\log\log x + \frac{1}{J(x)}\log x}{\frac{1}{2}\log x - 2\log\log x - \frac{1}{J(x)}\log x}\right) = \log\left(\frac{1 + \frac{4\log\log x}{\log x} + \frac{2}{J(x)}}{1 - \left(\frac{4\log\log x}{\log x} + \frac{2}{J(x)}\right)}\right).$$

For $|\epsilon| < \frac{1}{2}$, we have the Taylor expansion

$$\log\left(\frac{1+\epsilon}{1-\epsilon}\right) = 2\left(\epsilon + \frac{\epsilon^3}{3} + \frac{\epsilon^5}{5} + ...\right) = 2\epsilon + O\left(\epsilon^3\right) \ll \epsilon.$$

Using this with $\epsilon = \frac{4\log\log x}{\log x} + \frac{2}{J(x)}$ we see that

$$\log\left(\frac{\log \xi_3}{\log \xi_2}\right) \ll \frac{4\log\log x}{\log x} + \frac{2}{J(x)}.$$

Thus we see that the term in (3.16) is

$$\ll \frac{x}{\phi(m)\log x}\max\left\{\frac{1}{J(x)}, \frac{\log\log x}{\log x}\right\} = \frac{x}{\phi(m)\log x}\frac{1}{\min\{J(x), \frac{\log x}{\log\log x}\}}.$$

We note that the error term from (3.16) comes from the hardest case in Hooley's argument, and also gives us the largest error term. Because all the error terms in Proposition 3.19 are of order $\frac{x}{\phi(m)\log x}\frac{1}{\min\{J(x), \frac{\log x}{\log\log x}\}}$, we have proved Theorem 1.4.

3.7 Proofs of Lemma 1.5 and Proposition 1.6

3.7.1 Proof of Lemma 1.5

By Lemma 2.3 we have

$$\prod_{\substack{p|m\\ p|(a-1)}}\left(1-\frac{1}{p}\right)\geq\prod_{p|m}\left(1-\frac{1}{p}\right)=\frac{\phi(m)}{m}\gg\frac{1}{\log\log m},\tag{3.17}$$

and thus $\delta(m,a)\gg\frac{1}{\phi(m)\log\log m}$. Therefore it suffices to prove that

$$\frac{\log\log m}{\min\left\{J(x),\frac{\log x}{\log\log x}\right\}}=o(1).\tag{3.18}$$

If $\min\left\{J(x),\frac{\log x}{\log\log x}\right\}=\frac{\log x}{\log\log x}$, (3.18) follows trivially because $m\leq x$.
If $\min\left\{J(x),\frac{\log x}{\log\log x}\right\}=J(x)$, (3.18) follows because $m\leq x$ and $\log\log x=o\left(J(x)\right)$.

3.7.2 Proof of Proposition 1.6

Lemma 3.21. *For each $\epsilon>0$ and $y\geq 1$ one has*

$$\frac{1}{y}\#\left\{m\leq y:\frac{\phi(m)}{m}<\epsilon\right\}\leq 10\epsilon.$$

Proof. We have

$$\frac{1}{y}\#\left\{m\leq y:\frac{\phi(m)}{m}<\epsilon\right\}\leq\frac{\epsilon}{y}\sum_{m\leq y}\frac{m}{\phi(m)}.$$

Letting $f(m):=\frac{m}{\phi(m)}$, for a prime p and $j\geq 1$ we get $f(p^j)=\frac{p}{p-1}$. Therefore, by Lemma 2.10 we get

$$\sum_{m\leq y}\frac{m}{\phi(m)}\leq y\prod_{p\leq y}\sigma_p(f)\left(1-\frac{1}{p}\right).$$

Using the geometric series $\sum_{j=0}^{\infty}p^{-j}=\frac{1}{1-\frac{1}{p}}$ one obtains $\sigma_p(f)=1+\frac{p}{(p-1)^2}$, and thus

$$\begin{aligned}\sigma_p(f)\left(1-\frac{1}{p}\right)&=1-\frac{1}{p}+\frac{1}{p-1}\\&\leq 1+\frac{2}{p^2}\\&\leq\left(1+\frac{1}{p^2}\right)^2\leq\frac{1}{\left(1-\frac{1}{p^2}\right)^2}.\end{aligned}$$

Putting everything together we get

$$\frac{1}{y}\#\left\{m \leq y : \frac{\phi(m)}{m} < \epsilon\right\} \leq \epsilon \prod_p \frac{1}{\left(1-\frac{1}{p^2}\right)^2}.$$

Now note that for $\zeta(s) := \sum_{n=1}^{\infty} n^{-s}$ the Riemann zeta function, by Lemma 2.9,

$$\prod_p \frac{1}{\left(1-\frac{1}{p^2}\right)^2} = \zeta(2)^2 = \left(\frac{\pi^2}{6}\right)^2 \leq 10.$$

□

Using the above lemma we now prove Proposition 1.6. By Theorem 1.4 it suffices to prove that for the non-exceptional m we have $\frac{1}{\phi(m)} \ll \delta(m,a)$. Let $0 < \epsilon < \frac{1}{10}$. By Lemma 3.21 for all $m \leq x^{\frac{1}{J(x)}}$ except $10\epsilon x^{\frac{1}{J(x)}}$ we have $\frac{\phi(m)}{m} \geq \epsilon \gg 1$. By (3.17) we get for such m that

$$\delta(m,a) \gg \frac{1}{\phi(m)}\frac{\phi(m)}{m} = \frac{1}{m} \gg \frac{1}{\phi(m)},$$

which concludes the proof of Proposition 1.6.

4 Applications of Theorem 1.7

4.1 Proof of Theorem 1.10

Let $n \in \mathbb{N}$. Then we can write $n = n_1 n_2$ in such a way that n_1 is squarefree and for p a prime, $p^2|n$ if and only if $p|n_2$. Now n is squarefree if and only if $n_2 = 1$. Using Möbius inversion we get

$$\sum_{d^2|n} \mu(d) = \sum_{d|n_2} \mu(d) = \begin{cases} 1, & \text{if } n \text{ is squarefree,} \\ 0, & \text{else.} \end{cases} \tag{4.1}$$

Applying (4.1) to $n = p-1$ and then interchanging the order of summation, we get

$$\pi_{A,S}(x) = \sum_{\substack{p \leq x \\ \langle 2 \rangle = \mathbb{F}_p^*}} \sum_{\substack{d \in \mathbb{N} \\ d^2|p-1}} \mu(d) = \sum_{d \leq \sqrt{x}} \mu(d)\, \pi_A\left(x; d^2, 1\right).$$

By splitting the interval $[1, \sqrt{x}]$ in two parts $[1, y]$ and $(y, x]$, where $y := (\log x)^2$, we see that

$$\pi_{A,S}(x) = \sum_{d \leq y} \mu(d)\, \pi_A\left(x; d^2, 1\right) + \sum_{y < d \leq \sqrt{x}} \mu(d)\, \pi_A\left(x; d^2, 1\right). \tag{4.2}$$

4.1.1 Bounding the sum for $y < d \leq \sqrt{x}$

By the triangle inequality and Lemma 2.7 we have

$$\left| \sum_{y<d\leq\sqrt{x}} \mu(d)\, \pi_A\left(x; d^2, 1\right) \right| \leq \sum_{y<d\leq\sqrt{x}} \left(\frac{x}{d^2} + 1\right) \tag{4.3}$$

$$\leq x \int_y^{\infty} \frac{1}{u^2} du + \sqrt{x} \ll \frac{x}{(\log x)^2}. \tag{4.4}$$

4.1.2 Calculating the sum for $d \leq y$

For $d \leq y$ we have $d^2 \leq (\log x)^4$, so by Theorem 1.7 we have

$$\sum_{d\leq y} \mu(d)\, \pi_A\left(x; d^2, 1\right) = \sum_{d\leq y} \mu(d) \left(\delta\left(d^2, 1\right) \frac{x}{\log x} + O\left(\frac{x \log\log x}{\phi(d^2)(\log x)^2}\right)\right).$$

For the error term, notice that by Lemma 2.3, $\sum\limits_{d\leq y} \frac{1}{\phi(d^2)} = O(1)$. Hence

$$\sum_{d\leq y} \mu(d)\, \pi_A\left(x; d^2, 1\right) = \sum_{d\leq y} \mu(d)\, \delta\left(d^2, 1\right) \frac{x}{\log x} + O\left(\frac{x \log\log x}{(\log x)^2}\right). \tag{4.5}$$

Here we see the use of Theorem 1.7. Because for all $d \leq y$ we have an error term with a factor $\frac{1}{\phi(d)^2}$, and an absolute implied constant, we get a bound for the sum of all these error terms for $d \leq y$ which is good enough. Next we use the identity

$$\frac{\phi\left(d^2\right)}{d^2} = \prod_{p|d^2} \left(1 - \frac{1}{p}\right) \tag{4.6}$$

to get

$$\delta\left(d^2, 1\right) = \frac{1}{d^2} C_{\text{Artin}} \left(1 - \mathbb{1}_{\{8|d^2\}}\right) \prod_{p|d^2} \left(1 - \frac{1}{p\,(p-1)}\right)^{-1}.$$

Thus we have

$$\sum_{d\leq y} \mu(d)\, \pi_A\left(x; d^2, 1\right) = \frac{x}{\log x} C_{\text{Artin}} \sum_{d\leq y} \frac{\mu(d)}{d^2} \prod_{p|d} \left(1 - \frac{1}{p\,(p-1)}\right)^{-1} + O\left(\frac{x \log\log x}{(\log x)^2}\right). \tag{4.7}$$

By Lemma 2.2 we see that

$$\left| \frac{\mu(d)}{d^2} \prod_{p|d} \left(1 - \frac{1}{p\,(p-1)}\right)^{-1} \right| \ll_\epsilon \frac{1}{d^2} 2^{\omega(d)} \ll_\epsilon d^{-2+\epsilon}. \tag{4.8}$$

Hence, the series $\sum_{d=1}^{\infty}\left(\frac{\mu(d)}{d^2}\prod_{p|d}\left(1-\frac{1}{p(p-1)}\right)^{-1}\right)$ is absolutely convergent. We also get

$$\begin{aligned}\sum_{d>y}\frac{\mu(d)}{d^2}\prod_{p|d}\left(1-\frac{1}{p(p-1)}\right)^{-1} &\ll_\epsilon \sum_{d>y} d^{-2+\epsilon}\\ &\ll_\epsilon \int_y^{\infty} u^{-2+\epsilon}\mathrm{d}u \ll_\epsilon (\log x)^{-2+\epsilon}.\end{aligned}$$

Therefore,

$$\sum_{d\le y}\mu(d)\,\pi_A\left(x;d^2,1\right)=\frac{x}{\log x}C_{\mathrm{Artin}}\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}\prod_{p|d}\left(1-\frac{1}{p(p-1)}\right)^{-1}+O\left(\frac{x\log\log x}{(\log x)^2}\right). \quad (4.9)$$

4.1.3 Writing the main term with an Euler product

The map $d\mapsto\frac{\mu(d)}{d^2}\prod_{p|d}\left(1-\frac{1}{p(p-1)}\right)^{-1}$ is multiplicative, and we saw its associated Dirichlet series $\sum_{d=1}^{\infty}\left(\frac{\mu(d)}{d^2}\prod_{p|d}\left(1-\frac{1}{p(p-1)}\right)^{-1}\right)$ is absolutely convergent. Therefore, by Lemma 2.9 this series equals

$$\prod_p\sum_{j=0}^{\infty}\left(\frac{\mu\left(p^j\right)}{p^{2j}}\prod_{p'|p^j}\left(1-\frac{1}{p'(p'-1)}\right)^{-1}\right)=\prod_p\left(1-\frac{p-1}{p^3-p^2-p}\right).$$

An easy calculation shows that, for a prime p, we have

$$\delta^\natural(p^2,1)=\frac{p-1}{p^3-p^2-p}.$$

Substituting these two results in (4.9) yields the expression for $\pi_{A,S}(x)$ stated in Theorem 1.10.

4.1.4 The Euler product is absolutely convergent and positive

For all primes p we have $p-1<p^3-p^2-p$ and thus $1-\frac{p-1}{p^3-p^2-p}>0$. Because $\frac{p-1}{p^3-p^2-p}=O\left(\frac{1}{p^2}\right)$, the product $\prod_p\left(1-\frac{p-1}{p^3-p^2-p}\right)$ is absolutely convergent with all its factors positive, hence is positive itself. This completes the proof of Theorem 1.10.

4.2 Proof of Theorem 1.12

Because the proof of Theorem 1.12 will be very similar to the proof of Theorem 1.10, we will skip some steps which are the same as in the proof of Theorem 1.10.
Let $z:=(\log(N-1))^2$. Completely similar to how we proved (4.2) we get

$$R(N)=\sum_{d\le z}\mu(d)\,\pi_A\left(N-1;d^2,N\right)+\sum_{z<d\le\sqrt{N}}\mu(d)\,\pi_A\left(N-1;d^2,N\right). \quad (4.10)$$

4.2.1 Bounding the sum for $(d,N)>1$ and for $z<d\leq\sqrt{N}$

If $(d,N)>1$ then there can be at most 1 prime $p\equiv N \mod d$, hence the terms in (4.10) with $(d,N)>1$ contribute an amount $\ll\sqrt{N}$. Similar to how we proved (4.3), we get that the terms in (4.10) with $z<d\leq\sqrt{N}$ contribute an amount $\ll\frac{N}{(\log N)^2}$.

4.2.2 Calculating the sum for $d\leq z$ with $(d,N)=1$

Applying Theorem 1.7 in the same way as we did to prove (4.5), we get

$$\sum_{\substack{d\leq z\\(d,N)=1}}\mu(d)\,\pi_A\left(N-1;d^2,N\right)=\sum_{\substack{d\leq z\\(d,N)=1}}\mu(d)\,\delta\left(d^2,N\right)\frac{N}{\log(N)}+O\left(\frac{N\log\log N}{(\log N)^2}\right).$$

Again this is the part where we see the use of Theorem 1.7. Because for all $d\leq z$ we have an error term with a factor $\frac{1}{\phi(d^2)}$, and an absolute implied constant, we get a bound for the sum of all these error terms for $d\leq z$ which is good enough.
Using (4.6) one easily obtains $\frac{1}{\phi(d^2)}=\frac{1}{d\phi(d)}$. Using this we get

$$\delta\left(d^2,N\right)=\frac{1}{d\phi(d)}\prod_{p\nmid d^2}\left(1-\frac{1}{p(p-1)}\right)\prod_{\substack{p\mid d^2\\p\mid N-1}}\left(1-\frac{1}{p}\right)\left(1-\mathbb{1}_{\{8\mid d^2\}}\left(\frac{2}{N}\right)\right).$$

Therefore $\sum_{\substack{d\leq z\\(d,N)=1}}\mu(d)\,\pi_A\left(N-1;d^2,N\right)$ is equal to

$$C_{\text{Artin}}\frac{N}{\log N}\sum_{\substack{d\leq z\\(d,N)=1}}\frac{\mu(d)}{d\phi(d)}\prod_{p\mid d}\left(1-\frac{1}{p(p-1)}\right)^{-1}\prod_{\substack{p\mid d\\p\mid N-1}}\left(1-\frac{1}{p}\right)+O\left(\frac{N\log\log N}{(\log N)^2}\right)$$

Combining Lemma 2.3 with (4.8) reveals that

$$\left|\frac{\mu(d)}{d\phi(d)}\prod_{p\mid d}\left(1-\frac{1}{p(p-1)}\right)^{-1}\prod_{\substack{p\mid d\\p\mid N-1}}\left(1-\frac{1}{p}\right)\right|\ll_\epsilon(\log d)d^{-2+\epsilon}\cdot 1\ll_\epsilon d^{-2+\epsilon},$$

which shows that the series $\sum_{\substack{d\geq 1\\(d,N)=1}}\frac{\mu(d)}{d\phi(d)}\prod_{p\mid d}\left(1-\frac{1}{p(p-1)}\right)^{-1}\prod_{\substack{p\mid d\\p\mid N-1}}\left(1-\frac{1}{p}\right)$ converges absolutely.
Using this estimate we also get

$$\sum_{\substack{d>z\\(d,N)=1}}\frac{\mu(d)}{d\phi(d)}\prod_{p\mid d}\left(1-\frac{1}{p(p-1)}\right)^{-1}\prod_{\substack{p\mid d\\p\mid N-1}}\left(1-\frac{1}{p}\right)\ll_\epsilon(\log(N))^{-2+\epsilon}. \tag{4.11}$$

Putting everything together, we see that $R(N)$ equals

$$C_{\text{Artin}}\frac{N}{\log N}\sum_{\substack{d\geq 1\\(d,N)=1}}\frac{\mu(d)}{d\phi(d)}\prod_{p\mid d}\left(1-\frac{1}{p(p-1)}\right)^{-1}\prod_{\substack{p\mid d\\p\mid N-1}}\left(1-\frac{1}{p}\right)+O\left(\frac{N\log\log N}{(\log N)^2}\right). \tag{4.12}$$

4.2.3 Writing the main term with an Euler product

Now we write

$$\sum_{\substack{d\geq 1\\(d,N)=1}} \frac{\mu(d)}{d\phi(d)} \prod_{p|d} \left(1-\frac{1}{p(p-1)}\right)^{-1} \prod_{\substack{p|d\\p|N-1}} \left(1-\frac{1}{p}\right) = \sum_{n=1}^{\infty} f(n)$$

by putting

$$f(n) := \begin{cases} \frac{\mu(d)}{d\phi(d)} \prod_{p|d} \left(1-\frac{1}{p(p-1)}\right)^{-1} \prod_{\substack{p|d\\p|N-1}} \left(1-\frac{1}{p}\right), & \text{if } (d,N)=1,\\ 0, & \text{else.} \end{cases}$$

Now $f(n)$ is multiplicative and the associated Dirichlet series $\sum_{n=1}^{\infty} f(n)$ converges absolutely, so we can write it as an Euler product

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} \sum_{j=0}^{\infty} f\left(p^j\right) = \prod_{p|N-1} \left(1-\frac{p-1}{p^3-p^2-p}\right) \prod_{\substack{p\nmid N\\p\nmid N-1}} \left(1-\frac{1}{p^2-p-1}\right). \tag{4.13}$$

A straightforward calculation shows that for p a prime we have

$$\delta^{\natural}(p^2,N) = \begin{cases} \frac{p-1}{p^3-p^2-p}, & \text{if } p|N-1,\\ \frac{1}{p^2-p-1}, & \text{if } p\nmid N-1 \text{ and } p\nmid N,\\ 0, & \text{if } p|N. \end{cases}$$

Combining this with (4.13) and (4.12) yields the expression in Theorem 1.12.

4.2.4 The Euler product is absolutely convergent and positive

Both the products in (4.13) have factors of the form $1+O(\frac{1}{p^2})$, and are therefore absolutely convergent. In §4.1.4 we showed that the first product is positive. The factors of the second product become 0 only if $p=2$, but 2 divides either N or $N-1$.

5 Diophantine equations and Artin's conjecture

Notation.

- Let $\mathcal{P}$ denote the set of all primes.
- For $\alpha\in\mathbb{R}$, let $\mathrm{e}(\alpha) := \mathrm{e}^{2\pi i\alpha}$.
- For $q\in\mathbb{N}$ and $f:\mathbb{Z}/q\mathbb{Z}\to\mathbb{C}$, we use the notations

$$\sum_{b(q)} f(q) = \sum_{b \bmod q} f(q) = \sum_{b\in\mathbb{Z}/q\mathbb{Z}} f(q),$$

and

$$\sum_{b(q)^{\times}} f(q) = \sum_{b\in(\mathbb{Z}/q\mathbb{Z})^*} f(q).$$

- Vectors are denoted as $(b_1, ..., b_k) = \mathbf{b}$.
- For $m \in \mathbb{N}$ and a prime p, let $\nu_p(m) := \max\{n \in \mathbb{Z}_{\geq 0} : p^n | m\}$.

Note that $\mathrm{e}(\alpha)$ is periodic in α with period 1 and that $\mathrm{e}(x+y) = \mathrm{e}(x)\mathrm{e}(y)$.

5.1 Heuristics for Conjecture 1.15

For the classical ternary Goldbach problem, Vinogradov proved that

$$\#\{(p_1,p_2,p_3) \in \mathcal{P}^3 : p_1+p_2+p_3 = N\} = \sigma_\infty(N)\prod_p \sigma_p(N)\left(\frac{N}{(\log N)}\right)^3 + o\left(\frac{N^2}{(\log N)^4}\right),$$

where $\sigma_\infty(N) := \frac{1}{2N}$ and

$$\sigma_p(N) := \begin{cases} 1 - \frac{1}{(p-1)^2}, & \text{if } p|N, \\ 1 + \frac{1}{(p-1)^3}, & \text{if } p \nmid N. \end{cases}$$

There is a natural way to explain these densities. Firstly, the number of solutions of $n_1+n_2+n_3 = N$ in the positive integers is $\binom{N-1}{3-1}$, so

$$\sum_{\substack{1\leq n_1,n_2,n_3\leq N \\ n_1+n_2+n_3=N}} \frac{1}{N^3} = \frac{1+o(1)}{2N} = \sigma_\infty(N)(1+o(1)).$$

Also, it is not hard to see that

$$\lim_{m\to\infty} \frac{\sum\limits_{\substack{\mathbf{b}\in((\mathbb{Z}/p^m\mathbb{Z})^*)^3 \\ b_1+b_2+b_3\equiv N \mod p^m}} \frac{1}{\phi(p^m)^3}}{\sum\limits_{\substack{\mathbf{b}\in(\mathbb{Z}/p^m\mathbb{Z})^3 \\ b_1+b_2+b_3\equiv N \mod p^m}} \frac{1}{p^{3m}}} = \sigma_p(N).$$

Therefore the p-adic density $\sigma_p(N)$ is the ratio between the probability of a "prime solution mod p^m" to the probability of a solution mod p^m in general. The factor $\frac{1}{\phi(p^m)^3}$ is the product of the densities of primes in the arithmetic progressions $b_i \bmod p^m$ for $i = 1, 2, 3$.

By the prime number theorem, there are $\left(\frac{N}{\log N}\right)^3(1+o(1))$ triplets of primes (p_1,p_2,p_3) with $p_i \leq N$. We can interpret $\sigma_\infty(N)$ as the probability of solving $n_1+n_2+n_3 = N$ in the positive integers. We can view $\prod_p \sigma_p(N)$ as a correction factor, because we look for solutions in the primes.

Therefore, it is natural to make the following conjecture. Recall Definition 1.14.

Conjecture 5.1. *Fix $k \in \mathbb{Z}_{\geq 2}$. Let $\tau_\infty(N) := \binom{N-1}{k-1}N^{-k}$ and*

$$\tau_p(N) := \lim_{m\to\infty} \frac{\sum\limits_{\substack{\mathbf{b}\in((\mathbb{Z}/p^m\mathbb{Z})^*)^k \\ b_1+\ldots+b_k\equiv N \mod p^m}} \prod\limits_{i=1}^{k} \delta^\natural(p^m, b_i)}{\sum\limits_{\substack{\mathbf{b}\in(\mathbb{Z}/p^m\mathbb{Z})^k \\ b_1+\ldots+b_k\equiv N \mod p^m}} \frac{1}{p^{mk}}}. \tag{5.1}$$

Then

$$A_k(N) = \tau_\infty(N)\left(\prod_p \tau_p(N)\right)\left(C_{Artin}\frac{N}{\log N}\right)^k + o\left(\frac{N^{k-1}}{(\log N)^k}\right).$$

Note that $\delta^\natural(p^m, b_i)$ is the natural density of Artin primes in the progression $b_i \bmod p^m$ and $\binom{N-1}{k-1} = \frac{N^{k-1}}{(k-1)!}(1+o(1))$. In the next subsections, we will prove that $\tau_p(N) = \mathfrak{S}_p(N)$ for each prime p, where $\mathfrak{S}_p(N)$ was defined in Conjecture 1.15. Then clearly Conjecture 5.1 implies Conjecture 1.15.

Remark 5.2. Another heuristic for Conjecture 1.15 can be given by applying the circle method in the same way as Vinogradov did for ternary Goldbach, as exposed in Chapter 26 of [1], but without estimating the minor arcs.

5.2 First calculations of $\tau_p(N)$

The denominator in (5.1) equals

$$\sum_{\substack{\mathbf{b}\in(\mathbb{Z}/p^m\mathbb{Z})^k \\ b_1+\ldots+b_k\equiv N \mod p^m}} \frac{1}{p^{mk}} = \frac{p^{m(k-1)}}{p^{mk}} = \frac{1}{p^m}. \tag{5.2}$$

For the numerator in (5.1), the following lemma helps us to detect solutions of an equation modulo q. Its proof is standard.

Lemma 5.3. *For $a, q \in \mathbb{N}$ one has*

$$\frac{1}{q}\sum_{c(q)} \mathrm{e}\left(\frac{ac}{q}\right) = \begin{cases} 1, & \text{if } a \equiv 0 \mod q, \\ 0, & \text{else.} \end{cases}$$

Definition 5.4. For $a, q \in \mathbb{N}$, let

$$S(q,a) := \sum_{b(q)^\times} \mathrm{e}\left(\frac{a}{q}b\right) \prod_{\substack{p|q \\ p|b-1}} \left(1-\frac{1}{p}\right)\left(1-\mathbb{1}_{\{8|q\}}\left(\frac{2}{b}\right)\right).$$

For $q \in \mathbb{N}$, let

$$S(q) := \sum_{a(q)^\times} \mathrm{e}\left(-\frac{a}{q}N\right) S(q,a)^k,$$

and

$$f(q) := \frac{S(q)}{\phi(q)^k} \prod_{p|q} \left(1-\frac{1}{p(p-1)}\right)^{-k}.$$

Lemma 5.5. *One has*

$$\tau_p(N) = \sum_{d=0}^{\infty} f(p^d). \tag{5.3}$$

Proof. Let $m \in \mathbb{Z}_{\geq 3}$. Choosing $q = p^m$ and $a = b_1 + \ldots + b_k - N$ in Lemma 5.3 we see that the

numerator in (5.1) equals

$$\begin{aligned}
&\sum_{\substack{\mathbf{b}\in((\mathbb{Z}/p^m\mathbb{Z})^*)^k \\ b_1+\ldots+b_k\equiv N \mod p^m}} \prod_{i=1}^{k} \delta^\natural(p^m, b_i) \\
&= \sum_{\mathbf{b}\in((\mathbb{Z}/p^m\mathbb{Z})^*)^k} \frac{1}{p^m} \sum_{c(p^m)} \mathrm{e}\left(\frac{c(b_1+\ldots+b_k-N)}{p^m}\right) \prod_{i=1}^{k} \delta^\natural(p^m, b_i) \\
&= \frac{1}{p^m} \sum_{c(p^m)} \mathrm{e}\left(\frac{-cN}{p^m}\right) \left(\sum_{b(p^m)^\times} \mathrm{e}\left(\frac{cb}{p^m}\right) \delta^\natural(p^m, b)\right)^k \\
&= \frac{1}{p^m} \left(1 + \sum_{1\le c<p^m} \mathrm{e}\left(\frac{-cN}{p^m}\right) \left(\sum_{b(p^m)^\times} \mathrm{e}\left(\frac{cb}{p^m}\right) \delta^\natural(p^m, b)\right)^k\right),
\end{aligned} \tag{5.4}$$

using in the last step that the natural densities add up to 1. For $1 \le c < p^m$, we can write $\nu_p(c) = m - d$ with $1 \le d \le m$, and $c = p^{m-d}a$ with $1 \le a \le p^d$ coprime to p. Using this substitution we get

$$\begin{aligned}
&\sum_{1\le c<p^m} \mathrm{e}\left(\frac{-cN}{p^m}\right) \left(\sum_{b(p^m)^\times} \mathrm{e}\left(\frac{cb}{p^m}\right) \delta^\natural(p^m, b)\right)^k \\
&= \sum_{d=1}^{m} \sum_{a(p^d)^\times} \mathrm{e}\left(\frac{-aN}{p^d}\right) \left(\sum_{b(p^m)^\times} \mathrm{e}\left(\frac{ab}{p^d}\right) \delta^\natural(p^m, b)\right)^k \\
&= \sum_{d=1}^{m} \sum_{a(p^d)^\times} \mathrm{e}\left(\frac{-aN}{p^d}\right) \left(\sum_{x(p^d)^\times} \mathrm{e}\left(\frac{ax}{p^d}\right) \sum_{\substack{b(p^m) \\ b\equiv x \mod p^d}} \delta^\natural(p^m, b)\right)^k,
\end{aligned} \tag{5.5}$$

using the periodicity of $\mathrm{e}(\cdot)$.

Let $1 \le d \le m$. Making the substitution $b \mapsto y$ given by $b = x + yp^d$ for $1 \le y \le p^{m-d}$ we can write the innermost sum in (5.5) as

$$\sum_{x(p^d)^\times} \mathrm{e}\left(\frac{ax}{p^d}\right) \sum_{\substack{b(p^m) \\ b\equiv x \mod p^d}} \delta^\natural(p^m, b) = \sum_{x(p^d)^\times} \mathrm{e}\left(\frac{ax}{p^d}\right) \sum_{y(p^{m-d})} \delta^\natural(p^m, x+yp^d) \tag{5.6}$$

The next lemma helps us calculate the inner sum above.

Lemma 5.6. *Let p be a prime, $1 \le d \le m$, x coprime to p^d, and $1 \le y \le p^{m-d}$. Assume that $p \ne 2$, or $p = 2$ and $d \ge 3$. Then $\delta^\natural(p^m, x+yp^d) = \delta^\natural(p^m, x)$.*

Proof. Recall (1.8) and Definition 1.9, and recall that we assumed at the beginning of the proof of Lemma 5.5 that $m \ge 3$. Firstly, note that $p|(x+yp^d-1)$ if and only if $p|(x-1)$. Secondly,

we have $(x+yp^d, p^m) = 1$ if and only if $(x, p^m) = 1$.
Case 1: If $p \neq 2$, then we have $8 \nmid p^m$ and hence

$$\begin{aligned}\delta^\natural(p^m, x+yp^d) &= \frac{\mathbb{1}_{\{(x+yp^d,p^m)=1\}}}{\phi(p^m)} \frac{1}{1-\frac{1}{p(p-1)}}\left(1-\frac{1}{p}\right)\mathbb{1}_{\{p|x+yp^d-1\}} \\ &= \frac{\mathbb{1}_{\{(x,p^m)=1\}}}{\phi(p^m)} \frac{1}{1-\frac{1}{p(p-1)}}\left(1-\frac{1}{p}\right)\mathbb{1}_{\{p|x-1\}} = \delta^\natural(p^m, x).\end{aligned}$$

Case 2: If $p = 2$ and $d \geq 3$, then we have $\left(\frac{2}{x+y2^d}\right) = \left(\frac{2}{x}\right)$, by the periodicity of $\left(\frac{2}{\cdot}\right)$ mod 8, and by almost the same calculation as in case 1 we get $\delta^\natural(p^m, x+y2^d) = \delta^\natural(p^m, x)$. □

Lemma 5.7. *If p is a prime, $(a,p) = 1$ and $1 \leq d \leq m$, then*

$$\sum_{x (p^d)^\times} \mathrm{e}\left(\frac{ax}{p^d}\right) \sum_{\substack{b (p^m) \\ b \equiv x \mod p^d}} \delta^\natural(p^m, b) = \frac{S(p^d, a)}{\phi(p^d)\left(1-\frac{1}{p(p-1)}\right)}.$$

Proof. If $p \neq 2$, or $p = 2$ and $d \geq 3$, by Lemma 5.6 we can write (5.6) as

$$\begin{aligned}\sum_{x (p^d)^\times} \mathrm{e}\left(\frac{ax}{p^d}\right) \sum_{\substack{b (p^m) \\ b \equiv x \mod p^d}} \delta^\natural(p^m, b) &= \sum_{x (p^d)^\times} \mathrm{e}\left(\frac{ax}{p^d}\right) p^{m-d}\delta^\natural(p^m, x) \\ &= \frac{S(p^d, a)}{\phi(p^d)\left(1-\frac{1}{p(p-1)}\right)}.\end{aligned}$$

The remaining cases are $p = 2$, $d = 1$ and $p = 2, d = 2$, and we'll check these by using the values of $S(2^d, a)$ given in Lemma 5.8. We have not yet proved that lemma, but its proof is completely independent, so we can use it here. For $p = 2, d = 1$ the only coprime $x \mod 2$ is $x = 1$, hence

$$\begin{aligned}\sum_{x (2)^\times} \mathrm{e}\left(\frac{ax}{2}\right) \sum_{\substack{b (2^m) \\ b \equiv x \mod 2}} \delta^\natural(2^m, b) &= -\sum_{\substack{b (2^m) \\ b \equiv 1 \mod 2}} \delta^\natural(p^m, b) \\ &= -1 = \frac{S(2, a)}{\phi(2)\left(1-\frac{1}{2(2-1)}\right)},\end{aligned}$$

because the natural densities add up to 1. For $p = 2$, $d = 2$ we have

$$\begin{aligned}\sum_{x (4)^\times} \mathrm{e}\left(\frac{ax}{4}\right) \sum_{\substack{b (2^m) \\ b \equiv x \mod 4}} \delta^\natural(2^m, b) &= \pm i \sum_{\substack{b (2^m) \\ b \equiv 1 \mod 4}} \delta^\natural(2^m, b) \mp i \sum_{\substack{b (2^m) \\ b \equiv 3 \mod 4}} \delta^\natural(2^m, b) \\ &= 0 = \frac{S(4, a)}{\phi(4)\left(1-\frac{1}{2(2-1)}\right)}.\end{aligned}$$

where $\pm$ and $\mp$ denote opposed signs. Namely, from the definition one finds

$$\delta^\natural(2^m, b) = \begin{cases} 0, & \text{if } b \equiv 1, 7 \mod 8, \\ 2\frac{1}{\phi(2^m)}\frac{1}{1-\frac{1}{2(2-1)}}(1-\frac{1}{2}) & \text{if } b \equiv 3, 5 \mod 8, \end{cases}$$

because $8|2^m$, and $\left(\frac{2}{b}\right) = 0$ for $b \equiv 1, 7 \mod 8$, and $\left(\frac{2}{b}\right) = 1$ for $b \equiv 3, 5 \mod 8$. Hence,

$$\begin{aligned}
\sum_{\substack{b(2^m) \\ b\equiv 1 \mod 4}} \delta^\natural(2^m, b) &= \sum_{\substack{b(2^m) \\ b\equiv 1,5 \mod 8}} \delta^\natural(2^m, b) \\
&= \sum_{\substack{b(2^m) \\ b\equiv 1,5 \mod 8}} \frac{1}{\phi(2^m)} \frac{1}{1-\frac{1}{2(2-1)}}(1-\frac{1}{2}) \\
&= \sum_{\substack{b(2^m) \\ b\equiv 3,7 \mod 8}} \frac{1}{\phi(2^m)} \frac{1}{1-\frac{1}{2(2-1)}}(1-\frac{1}{2}) \\
&= \sum_{\substack{b(2^m) \\ b\equiv 1,5 \mod 8}} \delta^\natural(2^m, b) = \sum_{\substack{b(2^m) \\ b\equiv 3 \mod 4}} \delta^\natural(2^m, b).
\end{aligned}$$

□

Substituting the result from the above lemma into (5.5) we get

$$\sum_{1\le c<p^m} \mathrm{e}\left(\frac{-cN}{p^m}\right)\left(\sum_{b(p^m)^\times} \mathrm{e}\left(\frac{cb}{p^m}\right)\delta^\natural(p^m, b)\right)^k = \sum_{d=1}^{m} \sum_{a(p^d)^\times} \mathrm{e}\left(\frac{-aN}{p^d}\right) \frac{S(p^d, a)^k}{\phi(p^d)^k\left(1-\frac{1}{p(p-1)}\right)^k}.$$

Combining this with (5.4) and the fact that $f(1) = 1$ we get

$$\begin{aligned}
\sum_{\substack{\mathbf{b}\in((\mathbb{Z}/p^m\mathbb{Z})^*)^k \\ b_1+\ldots+b_k\equiv N \mod p^m}} \prod_{i=1}^{k} \delta^\natural(p^m, b_i) &= \frac{1}{p^m}\left(f(1) + \sum_{d=1}^{m} \sum_{a(p^d)^\times} \mathrm{e}\left(\frac{-aN}{p^d}\right) \frac{S(p^d, a)^k}{\phi(p^d)^k\left(1-\frac{1}{p(p-1)}\right)^k}\right) \\
&= \frac{1}{p^m}\sum_{d=0}^{m} f(p^d).
\end{aligned} \tag{5.7}$$

Substituting (5.2) and (5.7) in (5.1) completes the proof of Lemma 5.5.

□

5.3 The sum $S(q)$

With Lemma 5.5 in mind, our next goal is to calculate $S(p^l)$ on prime powers p^l.

5.3.1 The sum $S(p^l, a)$

Let p be a prime and $l \in \mathbb{N}$ such that $8 \nmid p^l$. Let $a \in \mathbb{N}$ be such that $p \nmid a$. Then we have

$$S\left(p^l, a\right) = \sum_{\substack{b(p^l) \\ p\nmid b}} \mathrm{e}(\frac{a}{p^l}b) - \frac{1}{p}\sum_{\substack{b(p^l) \\ p|b-1}} \mathrm{e}(\frac{a}{p^l}b). \tag{5.8}$$

In the second sum, we write $b = px + 1$ with $1 \leq x \leq p^{l-1}$, which gives

$$\sum_{\substack{b(p^l) \\ p|b-1}} \mathrm{e}\left(\frac{a}{p^l}b\right) = \mathrm{e}\left(\frac{a}{p^l}\right) \sum_{x=1}^{p^{l-1}} \mathrm{e}\left(\frac{ax}{p^{l-1}}\right) = \mathbb{1}_{\{l=1\}} \mathrm{e}\left(\frac{a}{p}\right). \tag{5.9}$$

Namely, for $l = 1$ we have $\mathrm{e}\left(\frac{a}{p^{l-1}}\right) = 1$, and for $l \geq 2$ we have a geometric sum

$$\begin{aligned}\sum_{x=1}^{p^{l-1}} \mathrm{e}\left(\frac{ax}{p^{l-1}}\right) &= \mathrm{e}\left(\frac{a}{p^{l-1}}\right) \sum_{x=0}^{p^{l-1}-1} \mathrm{e}\left(\frac{a}{p^{l-1}}\right)^x \\ &= \mathrm{e}\left(\frac{a}{p^{l-1}}\right) \frac{\mathrm{e}\left(\frac{a}{p^{l-1}}\right)^{p^{l-1}} - 1}{\mathrm{e}\left(\frac{a}{p^{l-1}}\right) - 1} = 0,\end{aligned}$$

because $p^{l-1} \nmid a$. The other sum equals

$$\sum_{\substack{b(p^l) \\ p \nmid b}} \mathrm{e}\left(\frac{a}{p^l}b\right) = \sum_{b(p^l)} \mathrm{e}\left(\frac{a}{p^l}b\right) - \sum_{\substack{b(p^l) \\ p|b}} \mathrm{e}\left(\frac{a}{p^l}b\right).$$

Again we have a geometric sum $\sum_{b(p^l)} \mathrm{e}(\frac{a}{p^l}b) = 0$ because $p^l \nmid a$. For $l = 1$ the other sum equals $\sum_{\substack{b(p) \\ p|b}} \mathrm{e}\left(\frac{a}{p}b\right) = \mathrm{e}(0) = 1$. For $l \geq 2$ we write $b = yp$ for $1 \leq y \leq p^{l-1}$, which gives

$$\sum_{\substack{b(p^l) \\ p|b}} \mathrm{e}\left(\frac{a}{p^l}b\right) = \sum_{y=1}^{p^{l-1}} \mathrm{e}\left(\frac{ay}{p^{l-1}}\right) = 0,$$

because this is again a geometric sum and $p^{l-1} \nmid a$. We conclude that

$$\sum_{\substack{b(p^l) \\ p \nmid b}} \mathrm{e}\left(\frac{a}{p^l}b\right) = -\mathbb{1}_{\{l=1\}}. \tag{5.10}$$

Combining equations (5.8) up to (5.10) results in the following lemma.

Lemma 5.8. *For p a prime and $l \in \mathbb{N}$, such that $8 \nmid p^l$, and $a \in \mathbb{Z}$ coprime to p we have*

$$S\left(p^l, a\right) = \begin{cases} -1 - \frac{1}{p}\mathrm{e}\left(\frac{a}{p}\right), & \text{if } l = 1, \\ 0, & \text{if } l \geq 2. \end{cases}$$

The remaining case is that p is a prime and $l \in \mathbb{N}$ such that $8|p^l$, which happens if and only if $p = 2$ and $l \geq 3$. For a an odd number we have

$$S\left(8, a\right) = \sum_{\substack{b(8) \\ b \equiv \pm 1, \pm 3 \mod 8}} \mathrm{e}\left(\frac{a}{8}b\right) \prod_{\substack{p|8 \\ p|b-1}} \left(1 - \frac{1}{p}\right)\left(1 - \left(\frac{2}{b}\right)\right).$$

For $b \equiv \pm 1 \mod 8$ we have $\left(\frac{2}{b}\right) = 1$ and the term vanishes. For $b \equiv \pm 3 \mod 8$ we have $\left(\frac{2}{b}\right) = -1$, so $1 - \left(\frac{2}{b}\right) = 2$. Furthermore, 8 and $p-1$ have exactly one common prime divisor, namely 2, so $\prod_{\substack{p|8 \\ p|b-1}} \left(1 - \frac{1}{p}\right) = \frac{1}{2}$. This gives

$$S(8,a) = \mathrm{e}\left(\frac{3a}{8}\right) + \mathrm{e}\left(\frac{-3a}{8}\right) = \mathrm{e}\left(\frac{3a}{8}\right) + \overline{\mathrm{e}\left(\frac{3a}{8}\right)}$$
$$= 2\Re\left(\mathrm{e}\left(\frac{3a}{8}\right)\right) = 2\cos\left(\frac{3a}{4}\pi\right).$$

Secondly, let $l \in \mathbb{Z}_{\geq 4}$. Then the same arguments as we used for $S(8,a)$ show

$$S\left(2^l, a\right) = \sum_{\substack{b \left(2^l\right) \\ b=3 \mod 8}} \mathrm{e}\left(\frac{a}{2^l}b\right) + \sum_{\substack{b \left(2^l\right) \\ b=-3 \mod 8}} \mathrm{e}\left(\frac{a}{2^l}b\right).$$

Via the substitution $b \mapsto x$ given by $b = 8x+3$ for $1 \leq x \leq 2^{l-3}$ the first sum can be written as

$$\sum_{\substack{b \left(2^l\right) \\ b=3 \mod 8}} \mathrm{e}\left(\frac{a}{2^l}b\right) = \sum_{x=1}^{2^{l-3}} \mathrm{e}\left(\frac{a}{2^l}(8x+3)\right) = \mathrm{e}\left(\frac{3a}{2^l}\right)\mathrm{e}\left(\frac{a}{2^{l-3}}\right)\frac{\mathrm{e}\left(\frac{a}{2^{l-3}}\right)^{2^{l-3}} - 1}{\mathrm{e}\left(\frac{a}{2^{l-3}}\right) - 1} = 0,$$

where again the geometric sum is used. The calculation goes through because a is odd and 2^{l-3} is even, so $\mathrm{e}\left(\frac{a}{2^{l-3}}\right) \neq 1$. In exactly the same way it follows that the second sum also vanishes.

Lemma 5.9. *For $l \in \mathbb{Z}_{\geq 3}$ and a an odd number we have*

$$S\left(2^l, a\right) = \begin{cases} 2\cos\left(\frac{3a}{4}\pi\right) & \text{if } l = 3, \\ 0, & \text{if } l \geq 4. \end{cases}$$

5.3.2 The sum $S(p^l)$

Having calculated the values of $S\left(p^l, a\right)$ allows us to calculate the values of $S\left(p^l\right)$ (for p a prime, $l \in \mathbb{N}$, and a coprime to p).
Firstly, if p is a prime and $l \in \mathbb{Z}_{\geq 2}$ such that $8 \nmid p^l$, then by Lemma 5.8 we have $S\left(p^l\right) = 0$.
For $l = 1$ and p prime Lemma 5.8 gives

$$S(p) = \sum_{\substack{a(p) \\ (a,p)=1}} \mathrm{e}\left(-\frac{a}{p}N\right)\left(-1 - \frac{1}{p}\mathrm{e}\left(\frac{a}{p}\right)\right)^k$$
$$= -\left(-1 - \frac{1}{p}\right)^k + \sum_{a(p)} \mathrm{e}\left(-\frac{a}{p}N\right)\left(-1 - \frac{1}{p}\mathrm{e}\left(\frac{a}{p}\right)\right)^k$$
$$= (-1)^{k+1}\left(1 + \frac{1}{p}\right)^k + \sum_{a(p)} \mathrm{e}\left(-\frac{a}{p}N\right)(-1)^k \sum_{m=0}^{k} \frac{\binom{k}{m}}{p^m}\mathrm{e}\left(\frac{am}{p}\right), \text{ by the binomial theorem,}$$
$$= (-1)^{k+1}\left(1 + \frac{1}{p}\right)^k + (-1)^k \sum_{m=0}^{k} \frac{\binom{k}{m}}{p^m} \sum_{a(p)} \mathrm{e}\left(\frac{a(m-N)}{p}\right).$$

A special case of Lemma 5.3 is the following,

$$\sum_{a(p)} \mathrm{e}\left(\frac{a\,(m-N)}{p}\right) = \begin{cases} p, & \text{if } p|m-N, \\ 0, & \text{otherwise.} \end{cases}$$

Combining the last two claims yields the succeeding result.

Lemma 5.10. *For any prime p we have*

$$S\,(p) = (-1)^{k+1}\left(1+\frac{1}{p}\right)^k + (-1)^k\,p \sum_{\substack{0\le m\le k \\ m\equiv N \mod p}} \frac{\binom{k}{m}}{p^m}.$$

For $l \in \mathbb{Z}_{\ge 2}$ such that $8 \nmid p^l$ we have $S\left(p^l\right) = 0$.

Using the definitions of $S(q)$ and $S(q,a)$, one can prove the succeeding lemma via a straightforward calculation.

Lemma 5.11. *We have*

$$S\,(2) = (-1)^{k+N}\,2^{-k}.$$

The remaining case is when $p = 2$ and $l \ge 3$. By Lemma 5.9, for $l \in \mathbb{Z}_{\ge 4}$ we have $S\left(2^l\right) = 0$. For $l = 3$, Lemma 5.9 reveals that

$$\begin{aligned} S\,(8) &= 2^k \sum_{a=1,3,5,7} \mathrm{e}\left(-\frac{a}{8}N\right)\left(\cos\left(\frac{3a}{4}\pi\right)\right)^k \\ &= \left(\sqrt{2}\right)^k\left((-1)^k\,\mathrm{e}\left(-\frac{1}{8}N\right) + \mathrm{e}\left(-\frac{3}{8}N\right) + \mathrm{e}\left(-\frac{5}{8}N\right) + (-1)^k\,\mathrm{e}\left(-\frac{7}{8}N\right)\right). \end{aligned}$$

Because the function $\mathrm{e}\,(x)$ is periodic in x with period 1, we see that the value of $S\,(8)$ completely depends on the residue class of N modulo 8. The e-function can be calculated with the formula $\mathrm{e}\,(x) = \mathrm{e}^{2\pi i x} = \cos\,(2\pi x) + i\sin\,(2\pi x)$. The enthousiastic reader can check that Table 5.1 gives the values for $S\,(8)$.

5.4 Concluding that $\tau_p(N) = \mathfrak{S}_p(N)$

By combining our calculations of $S(q)$ in §5.3 with (5.3) and Table 1.1 we get

$$\tau_2(N) = 1 + (-1)^{k+N} + \frac{S(8)}{2^k} = \mathfrak{S}_2(N),$$

and for $p > 2$ we get

$$\tau_p(N) = 1 + \left(p - 1 - \frac{1}{p}\right)^{-k}\left((-1)^{k+1}\left(1+\frac{1}{p}\right)^k + (-1)^k\,p \sum_{\substack{0\le m\le k \\ m\equiv N \mod p}} \frac{\binom{k}{m}}{p^m}\right) = \mathfrak{S}_p(N).$$

Hence we have proved that Conjecture 5.1 implies Conjecture 1.15, which conludes our heuristic for Conjecture 1.15.

Table 5.1: Values of $S(8)$.

$N \mod 8$	$S(8)$	$S(8)$ is k is even	$S(8)$ is k is odd
0	$2\left(\sqrt{2}\right)^{k}\left(1+(-1)^{k}\right)$	$4\left(\sqrt{2}\right)^{k}$	0
1	$\left(\sqrt{2}\right)^{k+1}\left((-1)^{k}-1\right)$	0	$-2\left(\sqrt{2}\right)^{k+1}$
2	0	0	0
3	$\left(\sqrt{2}\right)^{k+1}\left(1-(-1)^{k}\right)$	0	$2\left(\sqrt{2}\right)^{k+1}$
4	$-2\left(\sqrt{2}\right)^{k}\left(1+(-1)^{k}\right)$	$-4\left(\sqrt{2}\right)^{k}$	0
5	$\left(\sqrt{2}\right)^{k+1}\left(1-(-1)^{k}\right)$	0	$2\left(\sqrt{2}\right)^{k+1}$
6	0	0	0
7	$\left(\sqrt{2}\right)^{k+1}\left((-1)^{k}-1\right)$	0	$-2\left(\sqrt{2}\right)^{k+1}$

5.5 Proof of Proposition 1.16

5.5.1 The product $\prod_p \mathfrak{S}_p(N)$ is absolutely convergent

The series $\sum_p \left(\mathfrak{S}_p(N)-1\right)$is absolutely convergent, because for $p > kN$ we have

$$\left|\mathfrak{S}_p(N)-1\right| \leq 2^k\left(p-1-\frac{1}{p}\right)^{-k} \ll p^{-2}.$$

Therefore the product $\prod_p \mathfrak{S}_p(N)$ is absolutely convergent.

5.5.2 Positivity of the p-adic densities for $p > 2$

Next, we prove that for all $p > 2$ and all $N \in \mathbb{N}$ we have $\mathfrak{S}_p(N) > 0$.

Because $p \geq 3$ we have $p - 1 - \frac{1}{p} \geq 3 - 1 - \frac{1}{3} > 0$. Therefore we have

$$\begin{aligned}\mathfrak{S}_p(N) > 0 &\iff \left(p-1-\frac{1}{p}\right)^{-k}\left((-1)^{k+1}\left(1+\frac{1}{p}\right)^{k}+(-1)^{k}p\sum_{\substack{0\leq m\leq k\\ m\equiv N \mod p}}\frac{\binom{k}{m}}{p^m}\right) > -1\\ &\iff (-1)^{k}p\sum_{\substack{0\leq m\leq k\\ m\equiv N \mod p}}\frac{\binom{k}{m}}{p^m} > -\left(p-1-\frac{1}{p}\right)^{k}+(-1)^{k}\left(1+\frac{1}{p}\right)^{k}.\end{aligned}$$

We'll prove this last inequality case by case. For even k we get

$$\mathfrak{S}_p(N) > 0 \iff p\sum_{\substack{0\leq m\leq k\\ m\equiv N \mod p}}\frac{\binom{k}{m}}{p^m} > -\left(p-1-\frac{1}{p}\right)^{k}+\left(1+\frac{1}{p}\right)^{k}.$$

Because $p-1-\frac{1}{p} \geq 3-1-\frac{1}{3} > \frac{3}{2} > 1+\frac{1}{p}$ the right side in the above inequality is negative, while the left side is non-negative, so the inequality is satisfied.

For odd k we get by multiplying both sides with -1 that

$$\mathfrak{S}_p(N) > 0 \iff p \sum_{\substack{0 \leq m \leq k \\ m \equiv N \mod p}} \frac{\binom{k}{m}}{p^m} < \left(p-1-\frac{1}{p}\right)^k + \left(1+\frac{1}{p}\right)^k.$$

We have by the binomial theorem

$$p \sum_{\substack{0 \leq m \leq k \\ m \equiv N \mod p}} \frac{\binom{k}{m}}{p^m} \leq p\left(1+\frac{1}{p}\right)^k \leq \left(\frac{4}{3}\right)^k p.$$

Thus, for odd k it is sufficient to prove

$$\left(\frac{4}{3}\right)^k p < \left(p-1-\frac{1}{p}\right)^k + \left(1+\frac{1}{p}\right)^k. \tag{5.11}$$

For odd k we have $k \geq 3$, hence for all $p \geq 7$ we have

$$\begin{aligned}\left(p-1-\frac{1}{p}\right)^k &= p\left(p^{1-\frac{1}{k}} - p^{-\frac{1}{k}} - p^{-1-\frac{1}{k}}\right)^k \\ &\geq p\left(p^{\frac{2}{3}} - 2\right)^k > \left(\frac{4}{3}\right)^k p.\end{aligned}$$

For $p = 3$ and $p = 5$, one can check by hand that (5.11) holds for $k = 3$, and hence for all odd $k > 3$, because in (5.11) the right side grows faster with k than the left side.

We thus see that for all $p > 2$ and $N \in \mathbb{N}$ we have $\mathfrak{S}_p(N) > 0$. This concludes the proof of Proposition 1.16.

References

[1] H. Davenport, *Multiplicative number theory*, 3rd ed., ser. Graduate Texts in Mathematics. Springer-Verlag, New York, 2000, vol. 74.

[2] G. H. Hardy and J. E. Littlewood, "Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes," *Acta Math.*, vol. 44, no. 1, pp. 1–70, 1923. [Online]. Available: http://dx.doi.org/10.1007/BF02403921

[3] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 6th ed. Oxford University Press, Oxford, 2008.

[4] D. R. Heath-Brown, "Artin's conjecture for primitive roots," *Quart. J. Math. Oxford Ser. (2)*, vol. 37, no. 145, pp. 27–38, 1986. [Online]. Available: http://dx.doi.org/10.1093/qmath/37.1.27

[5] C. Hooley, "On Artin's conjecture," *J. reine angew. Math.*, vol. 225, pp. 209–220, 1967. [Online]. Available: http://dx.doi.org/10.1515/crll.1967.225.209

[6] ——, *Applications of sieve methods to the theory of numbers*. Cambridge University Press, Cambridge-New York-Melbourne, 1976.

[7] H. Iwaniec and E. Kowalski, *Analytic number theory*, ser. American Mathematical Society Colloquium Publications. American Mathematical Society, Providence, RI, 2004, vol. 53.

[8] H. W. Lenstra, Jr., "On Artin's conjecture and Euclid's algorithm in global fields," *Invent. Math.*, vol. 42, pp. 201–224, 1977.

[9] H. W. Lenstra, Jr., P. Stevenhagen, and P. Moree, "Character sums for primitive root densities," *Math. Proc. Cambridge Philos. Soc.*, vol. 157, no. 3, pp. 489–511, 2014.

[10] J. Maynard, "Small gaps between primes," *Ann. of Math. (2)*, vol. 181, no. 1, pp. 383–413, 2015. [Online]. Available: http://dx.doi.org/10.4007/annals.2015.181.1.7

[11] F. Mertens, "Ein Beitrag zur analytischen Zahlentheorie," *J. reine angew. Math.*, vol. 78, pp. 46–62, 1874. [Online]. Available: http://dx.doi.org/10.1515/crll.1874.78.46

[12] L. Mirsky, "The number of representations of an integer as the sum of a prime and a k-free integer," *Amer. Math. Monthly*, vol. 56, pp. 17–19, 1949.

[13] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, ser. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2007, vol. 97.

[14] P. Moree, "On primes in arithmetic progression having a prescribed primitive root. II," *Funct. Approx. Comment. Math.*, vol. 39, no. part 1, pp. 133–144, 2008.

[15] ——, "Artin's primitive root conjecture—a survey," *Integers*, vol. 12, no. 6, pp. 1305–1416, 2012. [Online]. Available: http://dx.doi.org/10.1515/integers-2012-0043

[16] M. R. Murty, *Problems in analytic number theory*, 2nd ed., ser. Graduate Texts in Mathematics. Springer, New York, 2008, vol. 206.

[17] P. Pollack, "Bounded gaps between primes with a given primitive root," *Algebra Number Theory*, vol. 8, no. 7, pp. 1769–1786, 2014. [Online]. Available: http://dx.doi.org/10.2140/ant.2014.8.1769

[18] J.-P. Serre, "Quelques applications du théorème de densité de Chebotarev," *Inst. Hautes Études Sci. Publ. Math.*, no. 54, pp. 323–401, 1981.

[19] C. Siegel, "Über die Classenzahl quadratischer Zahlkörper," *Acta Arith.*, vol. 1, no. 7, pp. 83–86, 1935.

[20] I. Vinogradov, "Representation of an odd number as a sum of three primes," *Dokl. Akad. Nauk. SSR*, vol. 15, pp. 291–294, 1937.

[21] A. Walfisz, "Zur additiven Zahlentheorie. II," *Math. Z.*, vol. 40, no. 1, pp. 592–607, 1936.

[22] Y. Zhang, "Bounded gaps between primes," *Ann. of Math. (2)*, vol. 179, no. 3, pp. 1121–1174, 2014. [Online]. Available: http://dx.doi.org/10.4007/annals.2014.179.3.7