Refinements of Artin's primitive root conjecture

Paul Péringuey
University of British Columbia
Pacific Institute for the Mathematical Sciences
peringuey@math.ubc.ca

Joint work with Leo Goldmakher & Greg Martin

March 3, 2025
Lethbridge Number Theory and Combinatorics Seminar

Definition

An integer is a primitive root modulo n if it generates all the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$.

Proposition

The multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic iff $n = 2, 4, p^r$ or $2p^r$, where p is an odd prime and $r \geq 0$.

$\mathrm{ord}_p(a)$														
a \ p	2	3	5	7	11	13	17	19	23	29	31	37	41	43
2	/	2	4	3	10	12	8	18	11	28	5	36	20	14
3	1	/	4	6	5	3	16	18	11	28	30	18	8	42
4	/	1	2	3	5	6	4	9	11	14	5	18	10	7
5	1	2	/	6	5	4	16	9	22	14	3	36	20	42

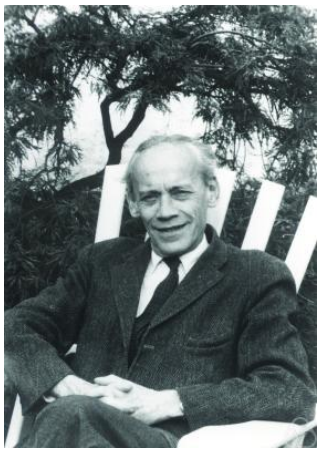
In red when $\mathrm{ord}_p(a) = p - 1$.

$$4^{\mathrm{ord}_p(2)} \equiv (2^{\mathrm{ord}_p(2)})^2 \equiv 1 \pmod{p},$$

hence $\mathrm{ord}_p(4) \mid \mathrm{ord}_p(2)$.
If $\mathrm{ord}_p(2) = p - 1$ then

$$4^{\frac{p-1}{2}} \equiv (2^{p-1}) \equiv 1 \pmod{p},$$

and therefore $\mathrm{ord}_p(4) < p - 1$, so 4 can't be a primitive root.



Conjecture (Artin 1927)

Let a be an integer which is neither $-1, 0, 1$ nor a square. Then a is a primitive root for an infinite number of primes. Moreover, by noting $\mathcal{N}_a(x)$ the number of primes $\leq x$ for which a is a primitive root:

$$\mathcal{N}_a(x) \sim \frac{x}{\log x} C(a),$$

with $C(a) \simeq 0.3739558$ if $a_0 \not\equiv 1 \pmod 4$ and a is not a perfect power, and $C(a) > 0$ otherwise. Where a_0 is the squarefree part of a.

Theorem (GRH, Hooley 1967)

$$\mathcal{N}_a(x) = \frac{x}{\log x} C(a) + \mathcal{O}\left(\frac{x \log\log x}{(\log x)^2}\right).$$

Theorem (Heath-Brown 1986)

At most two prime numbers are not primitive roots for an infinity of primes.

Let p and q two primes, a an integer coprime to p, not a perfect power. Then

$$q^\alpha \mid \frac{p-1}{\mathrm{ord}_p(a)} \Leftrightarrow \begin{cases} p \equiv 1 \mod q^\alpha \\ \text{and} \\ \exists b \mod p \text{ s.t. } a \equiv b^{q^\alpha} \mod p. \end{cases}$$

$$
\begin{aligned}
\mathcal{N}_a(x) &= \sum_{\substack{p\le x\\(a,p)=1}} \mathbb{1}\left(\frac{p-1}{\operatorname{ord}_p(a)}=1\right)\\
&= \sum_{\substack{p\le x\\(a,p)=1}} \prod_{qq\le x}\left(1-\mathbb{1}\left(q\mid\frac{(p-1)}{\operatorname{ord}_p(a)}\right)\right)\\
&= \sum_{\substack{p\le x\\(a,p)=1}} \prod_{qq\le x}\left(1-\mathbb{1}\left(p\equiv 1 \mod q,\ \begin{array}{l}a \text{ is a } q\text{-th}\\ \text{root} \mod p\end{array}\right)\right)\\
&= \sum_{\substack{\ell\\P^+(\ell)\le x}} \mu(\ell)\sum_{p\le x}\mathbb{1}\left((a,p)=1, p\equiv 1 \mod \ell,\ \begin{array}{l}a \text{ is an } \ell\text{-th}\\ \text{root} \mod p\end{array}\right.\\
&= \sum_{\substack{\ell\\P^+(\ell)\le x}} \mu(\ell)\#\left\{p\le x,(a,p)=1,\ \begin{array}{l}p \text{ splits completely}\\ \text{in } \mathbb{Q}(a^{1/\ell},\zeta_\ell)\end{array}\right\}
\end{aligned}
$$

What about primes for which a fails to be a primitive root by not much?

- Fix k, look for p s.t. $\frac{p-1}{\mathrm{ord}_p(a)} = k$ (Moree 2013, GRH).
- Fix k, look for p s.t. $\frac{p-1}{\mathrm{ord}_p(a)}$ has k prime factors. (2025+ Goldmakher, Martin, P., GRH).

3 ways of counting prime factor:

- Without multiplicity: $\omega\left(\frac{p-1}{\mathrm{ord}_p(a)}\right)$.
- With multiplicity: $\Omega\left(\frac{p-1}{\mathrm{ord}_p(a)}\right)$.
- Comparing the square-free kernels: $\omega(p-1)-\omega(\mathrm{ord}_p(a))$.

$\mathrm{ord}_p(a)$														
a \ p	2	3	5	7	11	13	17	19	23	29	31	37	41	43
2	/	2	4	3	10	12	8	18	11	28	5	36	20	14
3	1	/	4	6	5	3	16	18	11	28	30	18	8	42
4	/	1	2	3	5	6	4	9	11	14	5	18	10	7
5	1	2	/	6	5	4	16	9	22	14	3	36	20	42

In red when $\mathrm{ord}_p(a) = p - 1$, i.e $\omega\left((p-1)/\mathrm{ord}_p(a)\right) = 0$.
In blue when $\omega\left((p-1)/\mathrm{ord}_p(a)\right) = 1$.

Theorem (Goldmakher, Martin, P., 2025+)

Let $a \in \mathbb{Z}\backslash\{-1,0,1\}$, $z \in \mathbb{C}$ with $|z| \leq 1$, then assuming GRH

$$\sum_{\substack{p\leq x\\ \nu_p(a)=0}} z^{\omega((p-1)/\mathrm{ord}_p(a))} = \mathrm{Li}(x)C_a^{\omega/}(z)\prod_p\left(1+\frac{z-1}{p(p-1)}\right)+E(x),$$

$$\sum_{\substack{p\leq x\\ \nu_p(a)=0}} z^{\Omega((p-1)/\mathrm{ord}_p(a))} = \mathrm{Li}(x)C_a^{\Omega}(z)\prod_p\left(1+\frac{(z-1)p}{(p-1)(p^2-z)}\right)+E(x),$$

$$\sum_{\substack{p\leq x\\ \nu_p(a)=0}} z^{\omega(p-1)-\omega(\mathrm{ord}_p(a))} = \mathrm{Li}(x)C_a^{\omega-}(z)\prod_p\left(1+\frac{z-1}{p^2-1}\right)+E(x).$$

with $E(x) = \mathcal{O}\left(\frac{x\log\log x}{\log^2 x}\right)$ and the C_a are rational functions.

Let $a \in \mathbb{Z}\backslash\{-1,0,1\}$ not a perfect power, $z \in \mathbb{C}$ with $|z| \leq 1$,

$$\begin{aligned} N_a(x) &= \sum_{\substack{p \leq x \\ \nu_p(a)=0}} z^{\omega((p-1)/\mathrm{ord}_p(a))} \\ &= \sum_{\substack{p \leq x \\ \nu_p(a)=0}} \sum_{\ell \mid (p-1)/\mathrm{ord}_p(a)} \mu^2(\ell)(z-1)^{\omega(\ell)} \\ &= \sum_{\substack{\ell \\ P^+(\ell) \leq x}} \mu^2(\ell)(z-1)^{\omega(\ell)} P_\ell(x) \end{aligned}$$

where $P_\ell(x) = \#\left\{ p \leq x, (a,p)=1, \begin{array}{l} p \text{ splits completely} \\ \text{in } \mathbb{Q}(a^{1/\ell}, \zeta_\ell) \end{array} \right\}$, and $P^+(\ell)$ is the largest prime factor of ℓ.

Write Q_η the least common multiple of all integers smaller than η, and

$$N_a(x,\eta) = \sum_{\substack{\ell \\ P^+(\ell)\leq \eta}} \mu^2(\ell)(z-1)^{\omega(\ell)} P_\ell(x) = \sum_{\substack{p\leq x \\ \nu_p(a)=0}} z^{\omega((Q_\eta,(p-1)/\mathrm{ord}_p(a)))}.$$

Let $\eta_1 < \eta_2$ such that there is only one prime q with $\eta_1 < q \leq \eta_2$, then

$$\begin{aligned} N_a(x,\eta_2) - N_a(x,\eta_1) &= \sum_{\substack{p\leq x \\ \nu_p(a)=0 \\ q|(p-1)/\mathrm{ord}_p(a)}} (z-1) z^{\omega((Q_{\eta_1},(p-1)/\mathrm{ord}_p(a)))} \\ &\ll \#\left\{ p \leq x, p \equiv 1 \mod q, \begin{array}{l} a \text{ is a } q\text{-th} \\ \text{root} \mod p \end{array} \right\} \\ &\ll P_q(x) \end{aligned}$$

Therefore

$$N_a(x) = N_a(x,\eta) + \mathcal{O}\left(\sum_{\eta<q\le x} P_q(x)\right).$$

- $\sum_{\sqrt{x}\log x<q\le x} P_q(x) \ll \frac{x}{\log^2 x}$ by some combinatorial argument.
- $\sum_{\sqrt{x}/\log^2 x<q\le\sqrt{x}\log x} P_q(x) \ll \frac{x\log\log x}{\log^2 x}$ by Brun-Titchmarsh theorem.
- $\sum_{\log x<q\le\sqrt{x}/\log^2 x} P_q(x) \ll \frac{x\log\log x}{\log^2 x}$ under GRH.

Under GRH, we have $\sum_{\log x<q\le x} P_q(x) \ll \frac{x\log\log x}{\log^2 x}$. Then

$$N_a(x) = \sum_{\substack{\ell \\ P^+(\ell)\le\log x}} \mu^2(\ell)(z-1)^{\omega(\ell)} P_\ell(x) + \mathcal{O}\left(\frac{x\log\log x}{\log^2 x}\right).$$

let $\mathcal{U} \subset \mathbb{N}$, for every prime power q^k, let $\mathcal{F}_{q^k}$ denote a subset of $\mathcal{U}$.
Suppose $\mathcal{F}_{q^k} \subseteq \mathcal{F}_{q^{k-1}}$ for all q^k.
Define $e(n)$ to be the unique number such that
$n \in \bigcap_{q^k | e(n)} \mathcal{F}_{q^k} \setminus \bigcup_{q^k \nmid e(n)} \mathcal{F}_{q^k}$.

Lemma (Goldmakher, Martin, P. 2025+)

Assume that the collection $\{\mathcal{F}_{q^k}\}$ is cumulative. Let $h(m)$ be a multiplicative function bounded in absolute value by 1 and g its Möbius inverse. Let $Q_y = \prod_{p^k \le y} p$. For any positive real numbers $\xi < y$,

$$\sum_{\substack{n \le x \\ n \in \mathcal{U}}} h(\gcd(e(n), Q_y)) = \sum_{\ell | Q_\xi} g(\ell) \#\{n \le x : n \in \bigcap_{q^k | \ell} \mathcal{F}_{q^k}\} + O\Bigg(\sum_{\xi < q^k \le y} \#\{n \le x : n \in \mathcal{F}_{q^k}\} \Bigg).$$

Theorem (GRH, Lang 1971)

Let K a number field, then under GRH:

$$\pi_K(x) = \mathrm{Li}(x) + \mathcal{O}\left(\sqrt{x}\log(x^{[K:\mathbb{Q}]}|\Delta_K|)\right).$$

Where $\pi_K(x)$ is the prime ideal counting function on K, Δ_K is the discriminant of K.

In our case $K = \mathbb{Q}(a^{1/\ell}, \zeta_\ell)$, we get $|\Delta_K| \leq \ell^{\mathbf{C}[K:\mathbb{Q}]}$.

Theorem (GRH, Hooley 1967)

Assume GRH. Let a an integer, ℓ a squarefree integer. Write $K = \mathbb{Q}\left(\zeta_\ell, \sqrt[\ell]{a}\right)$, then

$$P_\ell(x) = \frac{\mathrm{Li}(x)}{[K:\mathbb{Q}]} + \mathcal{O}\left(\sqrt{x}\log(x\ell)\right),$$

where the implied constant only depend on a.

$$\sum_{\substack{p\leq x\\ \nu_p(a)=0}} z^{\omega((p-1)/\mathrm{ord}_p(a))} = \mathrm{Li}(x)\sum_{\ell}\frac{\mu^2(\ell)(z-1)^{\omega(\ell)}}{[\mathbb{Q}\left(\zeta_\ell,\sqrt[\ell]{a}\right):\mathbb{Q}]}+\mathcal{O}\left(\frac{x\log\log x}{\log^2 x}\right),$$

$$\sum_{\substack{p\leq x\\ \nu_p(a)=0}} z^{\Omega((p-1)/\mathrm{ord}_p(a))} = \mathrm{Li}(x)\sum_{\ell}\frac{z^{\Omega(\ell)}(1-z^{-1})^{\omega(\ell)}}{[\mathbb{Q}\left(\zeta_\ell,\sqrt[\ell]{a}\right):\mathbb{Q}]}+\mathcal{O}\left(\frac{x\log\log x}{\log^2 x}\right),$$

$$\sum_{\substack{p\leq x\\ \nu_p(a)=0}} z^{\omega(p-1)-\omega(\mathrm{ord}_p(a))} = \sum_{\ell}(z-1)^{\omega(\ell)}\sum_{m|\ell}\mu(m)\frac{\mathrm{Li}(x)}{[\mathbb{Q}\left(\zeta_{m\ell},\sqrt[\ell]{a}\right):\mathbb{Q}]}$$
$$+\mathcal{O}\left(\frac{x\log\log x}{\log^2 x}\right).$$

a is not a perfect power.
We have

$$[\mathbb{Q}\left(\zeta_\ell, \sqrt[\ell]{a}\right) : \mathbb{Q}] = \frac{[\mathbb{Q}\left(\sqrt[\ell]{a}\right) : \mathbb{Q}][\mathbb{Q}\left(\zeta_\ell\right) : \mathbb{Q}]}{\varepsilon_a(\ell)},$$

where $\varepsilon_a(\ell)$ is the degree of the largest common subfield of $\mathbb{Q}\left(\sqrt[\ell]{a}\right)$ and $\mathbb{Q}\left(\zeta_\ell\right)$. However $Q\left(\zeta_\ell\right)$ is Galois, hence

$$\varepsilon_a(\ell) = \begin{cases} 2, & \text{if } \sqrt{a} \in \mathbb{Q}\left(\sqrt[\ell]{a}\right) \cap \mathbb{Q}\left(\zeta_\ell\right), \\ 1, & \text{otherwise.} \end{cases}$$

More precisely we have

$$\begin{aligned}[\mathbb{Q}\left(\zeta_{m\ell}, \sqrt[\ell]{a}\right) : \mathbb{Q}] &= [\mathbb{Q}\left(\zeta_{m\ell}\right) : \mathbb{Q}] \times [\mathbb{Q}\left(\sqrt[\ell]{a}, \zeta_{m\ell}\right) : \mathbb{Q}\left(\zeta_{m\ell}\right)] \\ &= \varphi(m\ell)[\mathbb{Q}\left(\sqrt[\ell]{a}, \zeta_{m\ell}\right) : \mathbb{Q}\left(\zeta_{m\ell}\right)]\end{aligned}$$

And $[\mathbb{Q}\left(\sqrt[\ell]{a}, \zeta_{m\ell}\right) : \mathbb{Q}\left(\zeta_{m\ell}\right)] = \min\left\{j \in \mathbb{N} \colon a^{j/\ell} \in \mathbb{Q}\left(\zeta_{m\ell}\right)\right\}$.
Therefore we are looking for the smallest n for which $a^n = \gamma^\ell$ for some $\gamma \in \mathbb{Q}\left(\zeta_{m\ell}\right)$.

Lemma (Goldmakher, Martin, P., 2025+)

Fix positive integers m and ℓ. A rational number β is of the form γ^ℓ for some $\gamma \in \mathbb{Q}(\zeta_{m\ell})$ if and only if one of the following sets of conditions is satisfied:

- $\ell \equiv 1 \mod 2$ *and* $\beta = c^\ell$ *for some* $c \in \mathbb{Q}$.
- $\ell \equiv 0 \mod 2$, $\beta > 0$, *and* $\beta = c^{\ell/2}$ *for some* $c \in \mathbb{Q}$ *such that* $\sqrt{c} \in \mathbb{Q}(\zeta_{m\ell})$.
- $\ell \equiv 0 \mod 2$, $\beta < 0$, $2 \mid m$, *and* $\beta = -c^{\ell/2}$ *for some* $c \in \mathbb{Q}$ *such that* $\sqrt{c} \in \mathbb{Q}(\zeta_{m\ell})$.
- $\ell \equiv 2 \mod 4$, $\beta < 0$, $2 \nmid m$, *and* $\beta = c^{\ell/2}$ *for some* $c \in \mathbb{Q}$ *such that* $\sqrt{c} \in \mathbb{Q}(\zeta_{m\ell})$.
- $\ell \equiv 4 \mod 8$, $\beta < 0$, $2 \nmid m$, *and* $\beta = -(2c)^{\ell/2}$ *for some* $c \in \mathbb{Q}$ *such that* $\sqrt{c} \in \mathbb{Q}(\zeta_{m\ell})$.

Lemma (Goldmakher, Martin, P., 2025+)

Let $K = \mathbb{Q}\left(\sqrt[\ell]{a}, \xi_{m\ell}\right)$, *and* $\zeta_{m\ell}$ *a primitive* $m\ell$*-th root of unity. Let* $a = \eta a_0^h$ *with* $\eta = \pm 1$, h *a positive integer and* a_0 *positive not a power. Let* $\ell' = \ell/(\ell, h)$, $a_0 = b_0 c_0^2$, *with* $c_0 \in \mathbb{Q}$, b_0 *a square-free integer,*

$$\mathfrak{d}(a_0) = \begin{cases} b_0, & \text{if } b_0 \equiv 1 \mod 4, \\ 4b_0, & \text{otherwise.} \end{cases}.$$

Then we have:

$$\left[\mathbb{Q}\left(\zeta_{m\ell}, a^{1/\ell}\right) : \mathbb{Q}\right] = \frac{\ell' \varphi(m\ell)}{\varepsilon_a(m\ell, \ell)},$$

where $\varepsilon_a(m\ell, \ell)$ *is defined as follows:*

- *If* $a > 0$, *then* $\varepsilon_a(m\ell, \ell) = \begin{cases} 2, & \text{if } \ell' \equiv 0 \mod 2 \text{ and } \mathfrak{d}(a_0) \mid m\ell, \\ 1, & \text{otherwise.} \end{cases}$
- *If* $a < 0$ *and* ℓ *is odd then* $\varepsilon_a(m\ell, \ell) = 1$.
- *If* $a < 0$, ℓ *is even but* ℓ' *is odd then* $\varepsilon_a(m\ell, \ell) = \begin{cases} 1, & \text{if } 2 \mid m, \\ 1/2, & \text{otherwise.} \end{cases}$
- *If* $a < 0$, *and* $\ell' \equiv 2 \mod 4$ *then*

$$\varepsilon_a(m\ell, \ell) = \begin{cases} 2, & \text{if } 2 \mid m \text{ and } \mathfrak{d}(a_0) \mid m\ell \\ 2, & \text{if } \ell \equiv 2 \mod 4,\ m \equiv 1 \mod 2 \text{ and } \mathfrak{d}(-a_0) \mid m\ell, \\ 2, & \text{if } \ell \equiv 4 \mod 8,\ m \equiv 1 \mod 2 \text{ and } \mathfrak{d}(2a_0) \mid m\ell, \\ 1, & \text{otherwise.} \end{cases}$$

- *If* $a < 0$, *and* $4 \mid \ell'$ *then* $\varepsilon_a(m\ell, \ell) = \begin{cases} 2, & \text{if } \mathfrak{d}(a_0) \mid m\ell, \\ 1, & \text{otherwise.} \end{cases}$

Lemma (Hooley 1967)

Let $a \neq -1, 0, 1$ and not a perfect power, ℓ a squarefree integer.
Let $a = b_0 c_0^2$, with $c_0 \in \mathbb{Z}$, b_0 a square-free integer.
Then we have:

$$\left[\mathbb{Q}\left(\zeta_\ell, a^{1/\ell}\right) : \mathbb{Q}\right] = \frac{\ell\varphi(\ell)}{\varepsilon_a(\ell)},$$

where $\varepsilon_a(\ell)$ is defined as follows:

$$\varepsilon_a(\ell) = \begin{cases} 2, & \text{if } 2b_0 \mid \ell \text{ and } b_0 \equiv 1 \mod 4, \\ 1, & \text{otherwise.} \end{cases}$$

The case ℓ not squarefree was done by Wagstaff (1982).

$$\sum_{\ell} \frac{\mu^2(\ell)(z-1)^{\omega(\ell)}}{[\mathbb{Q}\left(\zeta_\ell, \sqrt[\ell]{a}\right):\mathbb{Q}]} = \sum_{\ell} \frac{\mu^2(\ell)(z-1)^{\omega(\ell)}}{\ell\varphi(\ell)} + \delta \sum_{\substack{\ell \\ 2b_0|\ell}} \frac{\mu^2(\ell)(z-1)^{\omega(\ell)}}{\ell\varphi(\ell)}.$$

$$\text{with } \delta = \begin{cases} 1 & \text{if } b_0 \equiv 1 \mod 4 \\ 0 & \text{otherwise.} \end{cases}$$

$$\sum_{\ell} \frac{\mu^2(\ell)(z-1)^{\omega(\ell)}}{\ell\varphi(\ell)} = \prod_{p} \left(1 + \frac{z-1}{p(p-1)}\right).$$

$$\begin{aligned} \sum_{\substack{\ell \\ 2b_0|\ell}} \frac{\mu^2(\ell)(z-1)^{\omega(\ell)}}{\ell\varphi(\ell)} &= \frac{(z-1)^{\omega(b_O)+1}}{2b_0\varphi(b_0)} \sum_{\substack{\ell \\ (2b_0,\ell)=1}} \frac{\mu^2(\ell)(z-1)^{\omega(\ell)}}{\ell\varphi(\ell)}, \\ &= \prod_{p|2b_0} \left(\frac{z-1}{p^2-p+z-1}\right) \prod_{p} \left(1 + \frac{z-1}{p(p-1)}\right). \end{aligned}$$

Theorem (Goldmakher, Martin, P., 2025+)

Assume GRH. Let $a \in \mathbb{Z}\backslash\{-1,0,1\}$ not a perfect power, $z \in \mathbb{C}$ with $|z| \leq 1$, then

$$\sum_{\substack{p \leq x \\ \nu_p(a)=0}} z^{\omega((p-1)/\mathrm{ord}_p(a))} = \mathrm{Li}(x) C_a^{\omega/}(z) \prod_p \left(1 + \frac{z-1}{p(p-1)}\right) + \mathcal{O}\left(\frac{x \log\log x}{(\log x)^2}\right)$$

where

$$C_a^{\omega/}(z) = \begin{cases} 1, & \text{if } b_0 \not\equiv 1 \mod 4, \\ 1 + f_a^{\omega/}(2b_0), & \text{if } b_0 \equiv 1 \mod 4, \end{cases}$$

and $f_a^{\omega/}(2b_0) = \prod_{p \mid 2b_0} \left(\frac{z-1}{p^2-p+z-1}\right)$.

If $a = 5$:

$$\sum_{\substack{p \le x \\ \nu_p(5)=0}} z^{\omega((p-1)/\mathrm{ord}_p(5))} = \mathrm{Li}(x) \frac{2z^2 + 18z + 20}{z^2 + 20z + 19} \prod_p \left(1 + \frac{z-1}{p(p-1)}\right) + E(x),$$

$$\sum_{\substack{p \le x \\ \nu_p(5)=0}} z^{\Omega((p-1)/\mathrm{ord}_p(5))} = \mathrm{Li}(x) \frac{11z^2 + 77z + 200}{z^2 + 97z + 190} \prod_p \left(1 + \frac{(z-1)p}{(p-1)(p^2-z)}\right) + E(x),$$

$$\sum_{\substack{p \le x \\ \nu_p(5)=0}} z^{\omega(p-1)-\omega(\mathrm{ord}_p(5))} = \mathrm{Li}(x) \frac{2z^2 + 25z + 47}{z^2 + 25z + 46} \prod_p \left(1 + \frac{z-1}{p^2-1}\right) + E(x),$$

where $E(x) = \mathcal{O}\left(\frac{x \log\log x}{(\log x)^2}\right)$.

$$\sum_{\substack{p\leq x\\ \nu_p(5)=0}} z^{\omega((p-1)/\mathrm{ord}_p(5))} = \mathrm{Li}(x)\frac{2z^2+18z+20}{z^2+20z+19}\prod_p\left(1+\frac{z-1}{p(p-1)}\right)+E(x),$$

$$\#\left\{p\leq x,\ \omega\left(\frac{(p-1)}{\mathrm{ord}_p(5)}\right)=1\right\} = \frac{1}{2i\pi}\int_{|z|=1/2}\frac{1}{z^2}\sum_{\substack{p\leq x\\ \nu_p(5)=0}} z^{\omega((p-1)/\mathrm{ord}_p(5))}dz$$

$$\begin{aligned} = &\ \mathrm{Li}(x)\prod_p\left(1-\frac{1}{p(p-1)}\right)\left(\frac{18\times 19-20^2}{19^2}+\frac{20}{19}\sum_p\frac{1}{p^2-p-1}\right)\\ &+\frac{1}{2\pi}\int_{|z|=1/2}\frac{1}{z^2}|E(x)|dz\\ \approx &\ 0.455527\,\mathrm{Li}(x)+\mathcal{O}\left(\frac{x\log\log x}{\log^2 x}\right)\end{aligned}$$

If $a = 4$:

$$\sum_{\substack{p \le x \\ \nu_p(4)=0}} z^{\omega((p-1)/\mathrm{ord}_p(4))} = \mathrm{Li}(x) \frac{2z}{z+1} \prod_p \left(1 + \frac{z-1}{p(p-1)}\right) + E(x),$$

$$\sum_{\substack{p \le x \\ \nu_p(4)=0}} z^{\Omega((p-1)/\mathrm{ord}_p(4))} = \mathrm{Li}(x) \frac{z^3 - z^2 + 12z}{4z+8} \prod_p \left(1 + \frac{(z-1)p}{(p-1)(p^2-z)}\right) + E(x),$$

$$\sum_{\substack{p \le x \\ \nu_p(4)=0}} z^{\omega(p-1)-\omega(\mathrm{ord}_p(4))} = \mathrm{Li}(x) \frac{7z+5}{4(z+2)} \prod_p \left(1 + \frac{z-1}{p^2-1}\right) + E(x),$$

where $E(x) = \mathcal{O}\left(\frac{x \log\log x}{(\log x)^2}\right)$.

Let X a discrete random variable with $\mathbb{P}(X = n) = a_n$ and define the power serie

$$f(z) = \sum_n a_n z^n.$$

Then

$$f'(1) = \sum_n n a_n = \mathbb{E}(X).$$

$a = 3$			
k	$\Omega\left(\frac{p-1}{\mathrm{ord}_p(3)}\right) = k$	$\omega\left(\frac{p-1}{\mathrm{ord}_p(3)}\right) = k$	$\omega(p-1) - \omega(\mathrm{ord}_p(3)) = k$
0	0.373955	0.373955	0.511757
1	0.405700	0.489828	0.428079
2	0.138409	0.125687	0.056962
3	0.056421	0.010164	0.003112
4	0.018447	0.000356	0.000085
5	0.005215	0.000006	0.000001
$\mathbb{E}$	0.96337	0.77315	0.55169

$a = 5$			
k	$\Omega\left(\frac{p-1}{\mathrm{ord}_p(5)}\right) = k$	$\omega\left(\frac{p-1}{\mathrm{ord}_p(5)}\right) = k$	$\omega(p-1) - \omega(\mathrm{ord}_p(5)) = k$
0	0.393637	0.393637	0.542249
1	0.357959	0.455527	0.371163
2	0.169510	0.135494	0.079483
3	0.056907	0.014732	0.006858
4	0.016216	0.000596	0.000241
5	0.004294	0.000011	0.000004
$\mathbb{E}$	0.96337	0.77315	0.55169

$a = 4$			
k	$\Omega\left(\frac{p-1}{\mathrm{ord}_p(4)}\right) = k$	$\omega\left(\frac{p-1}{\mathrm{ord}_p(4)}\right) = k$	$\omega(p-1) - \omega(\mathrm{ord}_p(4)) = k$
0	0	0	0.331694
1	0.560933	0.747911	0.543517
2	0.253293	0.231746	0.116448
3	0.122297	0.019629	0.008083
4	0.045042	0.000700	0.000252
5	0.013501	0.000012	0.000004
$\mathbb{E}$	1.71337	1.27315	0.80169

Corollary

Assume GRH. For any $a \in \mathbb{Q} \setminus \{-1, 0, 1\}$*:*

(a) *Both* $D_a^{\omega/}(n) \leq n^{-(2-o(1))n}$ *and* $D_a^{\omega-}(n) \leq n^{-(2-o(1))n}$ *(with the implied constants depending on* a*), with each of these upper bounds being attained infinitely often.*

(b) $D_a^{\Omega}(n) = R_a 4^{-n} + O_a(9^{-n})$.

$$
\begin{aligned}
\mathcal{N}_a(x) &= \sum_{\substack{p\le x\\(a,p)=1}} \mathbb{1}\left(\frac{p-1}{\operatorname{ord}_p(a)}=1\right)\\
&= \sum_{\substack{p\le x\\(a,p)=1}} \prod_{q\le x q\le \xi}\left(1-\mathbb{1}\left(q\mid\frac{(p-1)}{\operatorname{ord}_p(a)}\right)\right)\\
&= \le \sum_{\substack{p\le x\\(a,p)=1}} \prod_{q\le x q\le \xi}\left(1-\mathbb{1}\left(p\equiv 1 \mod q,\ \begin{array}{l}a \text{ is a } q\text{-th}\\ \text{root} \mod p\end{array}\right)\right)\\
&= \le \sum_{\substack{\ell\\ P^+(\ell)\le x P^+(\ell)\le\xi}} \mu(\ell)\sum_{p\le x}\mathbb{1}\left((a,p)=1, p\equiv 1 \mod \ell,\ a \text{ is}\right.\\
&\quad \left.\text{root}\right.\\
&= \le \sum_{\substack{\ell\\ P^+(\ell)\le x P^+(\ell)\le\xi}} \mu(\ell)\#\left\{p\le x,(a,p)=1,\ \begin{array}{l}p \text{ splits complete}\\ \text{in } \mathbb{Q}(a^{1/\ell},\zeta_\ell)\end{array}\right.
\end{aligned}
$$

Define $\omega_\xi(n) = \#\{p \leq \xi,\ p \mid n\}$, then

$$\begin{aligned}
\#\left\{p \leq x : \omega\left(\frac{p-1}{\mathrm{ord}_p(a)}\right) = 0\right\} &\leq \#\left\{p \leq x : \omega_\xi\left(\frac{p-1}{\mathrm{ord}_p(a)}\right) = 0\right\} \\
\#\left\{p \leq x : \omega\left(\frac{p-1}{\mathrm{ord}_p(a)}\right) \leq k\right\} &\leq \#\left\{p \leq x : \omega_\xi\left(\frac{p-1}{\mathrm{ord}_p(a)}\right) \leq k\right\}.
\end{aligned}$$

$$N_{a,\xi}(x) = \sum_{\substack{p \leq x \\ \nu_p(a)=0}} z^{\omega_\xi((p-1)/\mathrm{ord}_p(a))}$$

And taking $\xi = \frac{1}{2}\log\log\log\log x$, we obtain the same asymptotic for $N_{a,\xi}(x)$ as we had for $N_a(x)$, but this time unconditionally!

Theorem (Goldmakher, Martin, P., 2025+)

Assume GRH. If $a \in \mathbb{Q}$ is not a perfect power, then for any $z \in \mathbb{C}$ with $|z| \le 1$,

$$\frac{1}{\pi(x)} \sum_{\substack{p \le x \\ \nu_p(a)=0}} z^{\omega((p-1)/\mathrm{ord}_p(a))} = F_a^{\omega/}(z) \prod_q \left(1 + \frac{z-1}{q(q-1)}\right) + \mathcal{O}\left(\frac{x \log\log x}{(\log x)^2}\right)$$

where

$$F_a^{\omega/}(z) = \begin{cases} 1, & \text{if } \mathfrak{d}(a) \not\equiv 1 \mod 4, \\ 1 + \displaystyle\prod_{q \mid 2\mathfrak{d}(a)} \frac{z-1}{z+q^2-q-1}, & \text{if } \mathfrak{d}(a) \equiv 1 \mod 4. \end{cases}$$

Theorem (Goldmakher, Martin, P., 2025+)

Assume GRH. If $a \in \mathbb{Q}$ is not a perfect power, then for any $z \in \mathbb{C}$ with $|z| \le 1$,

$$\sum_{\substack{p \le x \\ \nu_p(a)=0}} z^{\Omega((p-1)/\mathrm{ord}_p(a))} = \pi(x) F_a^{\Omega}(z) \prod_q \left(1 + \frac{(z-1)q}{(q-1)(q^2-z)}\right) + \mathcal{O}\left(\frac{x}{(}\right.$$

where

$$F_a^{\Omega}(z) = 1 + \delta(a)(z-1)^{\omega(2b_0)} \prod_{q \mid 2b_0} \left(\frac{q}{z+q^3-q^2-q}\right),$$

with

$$\delta(a) = \begin{cases} 1, & \text{if } \mathrm{sgn}(a) b_0 \equiv 1 \mod 4, \\ z/4, & \text{if } \mathrm{sgn}(a) b_0 \equiv 3 \mod 4, \\ z^2/16, & \text{if } b_0 \equiv 2 \mod 4. \end{cases}$$

Theorem (Goldmakher, Martin, P., 2025+)

Assume GRH. If $a \in \mathbb{Q}$ is not a perfect power, then for any $z \in \mathbb{C}$ with $|z| \leq 1$,

$$\sum_{\substack{p \leq x \\ \nu_p(a)=0}} z^{\omega(p-1)-\omega(\mathrm{ord}_p(a))} = \pi(x) F_a^{\omega-}(z) \prod_q \left(1 + \frac{z-1}{q^2-1}\right) + \mathcal{O}\left(\frac{x \log\log}{(\log x)^2}\right.$$

where

$$F_a^{\omega-}(z) = 1 + \delta(a)(z-1)^{\omega(2b_0)} \prod_{q \mid 2b_0} \left(\frac{1}{q^2+z-2}\right),$$

with

$$\delta(a) = \begin{cases} 1, & \text{if } \mathrm{sgn}(a) b_0 \equiv 1 \mod 4, \\ -1/2, & \text{if } \mathrm{sgn}(a) b_0 \equiv 3 \mod 4, \\ -1/8, & \text{if } b_0 \equiv 2 \mod 4. \end{cases}$$

Thank you for your attention !