Polynomial analogues of some results in number theory

Andreas Weingartner

Department of Mathematics
Southern Utah University

West Coast Number Theory, December 18, 2015

Correspondence between $\mathbb{Z}$ and $\mathbb{F}_q[T]$

$\mathbb{F}_q[T] :=$ set of polynomials over $\mathbb{F}_q$, the finite field with q elements.

Correspondence between $\mathbb{Z}$ and $\mathbb{F}_q[T]$

$\mathbb{F}_q[T] :=$ set of polynomials over $\mathbb{F}_q$, the finite field with q elements.

$\mathbb{Z}$	$\mathbb{F}_q[T]$
$\{\pm 1\}$	$\mathbb{F}_q^\times$
positive integers	monic polynomials
prime numbers	monic irreducible polynomials
absolute value	$\lvert f\rvert = q^{\deg f}$
integers of size $\asymp x$	monic polynomials of degree n where $x = q^n$

Prime number theorem

Hadamard, de la Vallée Poussin: The number of primes $p \leq x$ is asymptotic to $\frac{x}{\log x}$ as $x \to \infty$.

Prime number theorem

Hadamard, de la Vallée Poussin: The number of primes $p \leq x$ is asymptotic to $\frac{x}{\log x}$ as $x \to \infty$.

Gauss: The number of monic irreducible polynomials in $\mathbb{F}_q[T]$ of degree n is

$$\frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right).$$

Twin primes

Twin prime conjecture: There are infinitely many prime pairs $p, p+2$.

Twin primes

Twin prime conjecture: There are infinitely many prime pairs $p, p+2$.

Hall (2006): Let $q > 3$ and $C \in \mathbb{F}_q$ be constant. There are infinitely many twin prime pairs $P, P+C \in \mathbb{F}_q[T]$.

Twin primes

Twin prime conjecture: There are infinitely many prime pairs $p, p+2$.

Hall (2006): Let $q > 3$ and $C \in \mathbb{F}_q$ be constant. There are infinitely many twin prime pairs $P, P+C \in \mathbb{F}_q[T]$.

Pollack (2008) finds asymptotic result for the number of twin prime pairs $P, P+C \in \mathbb{F}_q[T]$, assuming $n^2/q \to 0$, where $n = \deg(P)$.

Rough integers: no small prime factors

Let $\Phi(x, y) = \#\{n \le x : p|n \Rightarrow p > y\}$.

Rough integers: no small prime factors

Let $\Phi(x,y) = \#\{n \le x : p|n \Rightarrow p > y\}$.

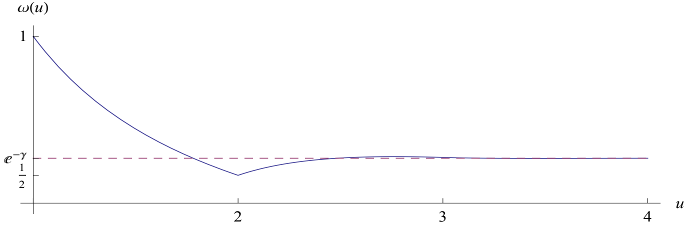
Tenenbaum: For $x \ge 2y \ge 5$,

$$\Phi(x,y) = e^{\gamma}(x\,\omega(u) - y)\prod_{p\le y}\left(1-\frac{1}{p}\right)\left\{1 + O\left(\frac{e^{-u/3}}{\log y}\right)\right\},$$

where $u = \frac{\log x}{\log y}$ and Buchstab's function ω is given by

$$\omega(u) = 1/u \quad (1 \le u \le 2),$$

$$(u\omega(u))' = \omega(u-1) \quad (u > 2).$$



Rough polynomials: no divisors of small degree

Let $r(n, m)$ be the proportion of polynomials of degree n over $\mathbb{F}_q$, all of whose non-constant divisors have degree $> m$.

Rough polynomials: no divisors of small degree

Let $r(n,m)$ be the proportion of polynomials of degree n over $\mathbb{F}_q$, all of whose non-constant divisors have degree $> m$.

W. (2015): Let $u = n/m$. For $n > m \geq 1$ we have

$$r(n,m) = e^{\gamma}\,\omega(u) \prod_{\deg(P)\leq m} \left(1 - \frac{1}{|P|}\right) \left\{1 + O\left(\frac{(u/e)^{-u}}{m}\right)\right\},$$

where P runs over monic irreducibles and $|P| = q^{\deg(P)}$.

Practical numbers

Srinivasan (1948): A positive integer n is called practical if all smaller positive integers can be represented as sums of distinct divisors of n.

Practical numbers

Srinivasan (1948): A positive integer n is called practical if all smaller positive integers can be represented as sums of distinct divisors of n.

Examples:

- 12 is practical: $5 = 3 + 2$, $7 = 4 + 3$, $8 = 6 + 2$, $9 = 6 + 3$, $10 = 6 + 4$, $11 = 6 + 3 + 2$.
- 10 is not practical: $9 > 5 + 2 + 1$.

Practical numbers

Srinivasan (1948): A positive integer n is called practical if all smaller positive integers can be represented as sums of distinct divisors of n.

Examples:

- 12 is practical: $5 = 3 + 2$, $7 = 4 + 3$, $8 = 6 + 2$, $9 = 6 + 3$, $10 = 6 + 4$, $11 = 6 + 3 + 2$.
- 10 is not practical: $9 > 5 + 2 + 1$.

The sequence of practical numbers:

$$1,\ 2,\ 4,\ 6,\ 8,\ 12,\ 16,\ 18,\ 20,\ 24,\ 28,\ 30,\ 32,\ 36,\ 40,\ldots$$

Practical numbers: Analogies with prime numbers

Practical numbers: 1, 2, 4, 6, 8, 12, 16, 18, 20, 24, 28, ...

Prime numbers: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...

Practical numbers: Analogies with prime numbers

Practical numbers: 1, 2, 4, 6, 8, 12, 16, 18, 20, 24, 28, ...

Prime numbers: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...

[Goldbach's Conjecture] (Melfi, 1996):
Every even positive integer is the sum of two practical numbers.

Practical numbers: Analogies with prime numbers

Practical numbers: 1, 2, 4, 6, 8, 12, 16, 18, 20, 24, 28, ...

Prime numbers: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...

[Goldbach's Conjecture] (Melfi, 1996):
Every even positive integer is the sum of two practical numbers.

[Legendre's Conjecture] (Hausman & Shaprio, 1984):
There is a practical number between x^2 and $(x+1)^2$ for every $x > 0$.

Practical numbers: Analogies with prime numbers

Practical numbers: 1, 2, 4, 6, 8, 12, 16, 18, 20, 24, 28, ...

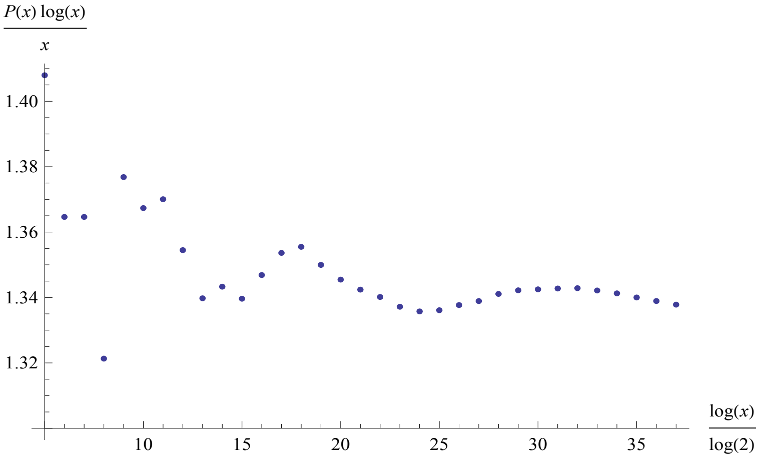
Prime numbers: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...

[Goldbach's Conjecture] (Melfi, 1996):
Every even positive integer is the sum of two practical numbers.

[Legendre's Conjecture] (Hausman & Shaprio, 1984):
There is a practical number between x^2 and $(x+1)^2$ for every $x > 0$.

[Prime Number Theorem] (Margenstern's Conjecture, 1991):
The number of practical numbers below x is asymptotic to $\dfrac{c\,x}{\log x}$.

Define $P(x) := \#\{n \leq x : n \text{ is practical}\}$



Counting practical numbers

Let $P(x) = \#\{n \leq x : n \text{ practical}\}$

Counting practical numbers

Let $P(x) = \#\{n \leq x : n \text{ practical}\}$

Erdős and Loxton (1979): $P(x) = o(x)$

Counting practical numbers

Let $P(x) = \#\{n \leq x : n \text{ practical}\}$

Erdős and Loxton (1979): $P(x) = o(x)$

Hausman and Shapiro (1983): $P(x) \ll \frac{x}{(\log x)^\beta}, \quad \beta = 0.0979...$

Counting practical numbers

Let $P(x) = \#\{n \leq x : n \text{ practical}\}$

Erdős and Loxton (1979): $P(x) = o(x)$

Hausman and Shapiro (1983): $P(x) \ll \dfrac{x}{(\log x)^{\beta}}, \quad \beta = 0.0979\ldots$

Margenstern (1984): $P(x) \gg \dfrac{x}{\exp\left(\alpha(\log\log x)^2\right)}, \quad \alpha = 0.7213\ldots.$

Counting practical numbers

Let $P(x) = \#\{n \le x : n \text{ practical}\}$

Erdős and Loxton (1979): $P(x) = o(x)$

Hausman and Shapiro (1983): $P(x) \ll \dfrac{x}{(\log x)^\beta}, \quad \beta = 0.0979\ldots$

Margenstern (1984): $P(x) \gg \dfrac{x}{\exp\left(\alpha(\log\log x)^2\right)}, \quad \alpha = 0.7213\ldots.$

Tenenbaum (1986):

$$\frac{x}{\log x(\log_2 x)^{4.201}} \ll P(x) \ll \frac{x \log_2 x \log_3 x}{\log x}$$

Counting practical numbers

Let $P(x) = \#\{n \leq x : n \text{ practical}\}$

Erdős and Loxton (1979): $P(x) = o(x)$

Hausman and Shapiro (1983): $P(x) \ll \dfrac{x}{(\log x)^{\beta}}, \quad \beta = 0.0979\ldots$

Margenstern (1984): $P(x) \gg \dfrac{x}{\exp\left(\alpha(\log\log x)^2\right)}, \quad \alpha = 0.7213\ldots.$

Tenenbaum (1986):

$$\frac{x}{\log x(\log_2 x)^{4.201}} \ll P(x) \ll \frac{x \log_2 x \log_3 x}{\log x}$$

Saias (1997): $P(x) \asymp \dfrac{x}{\log x}$

Counting practical numbers

Let $P(x) = \#\{n \le x : n \text{ practical}\}$

Erdős and Loxton (1979): $P(x) = o(x)$

Hausman and Shapiro (1983): $P(x) \ll \dfrac{x}{(\log x)^{\beta}}, \quad \beta = 0.0979\ldots$

Margenstern (1984): $P(x) \gg \dfrac{x}{\exp\left(\alpha(\log\log x)^2\right)}, \quad \alpha = 0.7213\ldots.$

Tenenbaum (1986):

$$\frac{x}{\log x(\log_2 x)^{4.201}} \ll P(x) \ll \frac{x \log_2 x \log_3 x}{\log x}$$

Saias (1997): $P(x) \asymp \dfrac{x}{\log x}$

W. (2015): $P(x) = \dfrac{cx}{\log x}\left(1 + O\left(\dfrac{\log\log x}{\log x}\right)\right)$ for some $c > 0$.

Integers with dense divisors

$$D(x) := \# \{n \le x : [y, 2y) \text{ contains a divisor of } n \text{ for all } 1 \le y \le n.\}$$

Integers with dense divisors

$$D(x) := \#\{n \le x : [y, 2y) \text{ contains a divisor of } n \text{ for all } 1 \le y \le n.\}$$

Tenenbaum (1986): For $x \ge 2$,

$$\frac{x}{\log x\,(\log\log x)^{4.201}} \ll D(x) \ll \frac{x \log\log x}{\log x}.$$

Integers with dense divisors

$$D(x) := \#\{n \le x : [y, 2y) \text{ contains a divisor of } n \text{ for all } 1 \le y \le n.\}$$

Tenenbaum (1986): For $x \ge 2$,

$$\frac{x}{\log x\,(\log\log x)^{4.201}} \ll D(x) \ll \frac{x \log\log x}{\log x}.$$

Saias (1997): For $x \ge 2$, $\quad D(x) \asymp \dfrac{x}{\log x}$.

Integers with dense divisors

$$D(x) := \#\{n \le x : [y, 2y) \text{ contains a divisor of } n \text{ for all } 1 \le y \le n.\}$$

Tenenbaum (1986): For $x \ge 2$,

$$\frac{x}{\log x\,(\log\log x)^{4.201}} \ll D(x) \ll \frac{x\log\log x}{\log x}.$$

Saias (1997): For $x \ge 2$, $\quad D(x) \asymp \dfrac{x}{\log x}.$

W. (2015): For $x \ge 2$,

$$D(x) = \frac{c_2\, x}{\log x}\left\{1 + O\left(\frac{1}{\log x}\right)\right\},$$

for some $c_2 > 0$.

Polynomial Analogue: divisors of every degree

Ex.: $T(T^2+T+1)(T^4+T+1) \in \mathbb{F}_2[T]$ has divisors of deg $1, \ldots, 7$.

Polynomial Analogue: divisors of every degree

Ex.: $T(T^2+T+1)(T^4+T+1) \in \mathbb{F}_2[T]$ has divisors of deg $1, \ldots, 7$.

Ex.: $T(T^3+T+1)(T^3+T^2+1) \in \mathbb{F}_2[T]$ has no divisor of degree 2.

Polynomial Analogue: divisors of every degree

Ex.: $T(T^2+T+1)(T^4+T+1) \in \mathbb{F}_2[T]$ has divisors of deg $1,\ldots,7$.

Ex.: $T(T^3+T+1)(T^3+T^2+1) \in \mathbb{F}_2[T]$ has no divisor of degree 2.

W. (2015): The proportion of polynomials of degree n over $\mathbb{F}_q$, which have a divisor of every degree below n, is given by

$$\frac{c_q}{n}\left(1+O\left(\frac{1}{n}\right)\right).$$

Polynomial Analogue: divisors of every degree

Ex.: $T(T^2+T+1)(T^4+T+1) \in \mathbb{F}_2[T]$ has divisors of deg $1, \dots, 7$.

Ex.: $T(T^3+T+1)(T^3+T^2+1) \in \mathbb{F}_2[T]$ has no divisor of degree 2.

W. (2015): The proportion of polynomials of degree n over $\mathbb{F}_q$, which have a divisor of every degree below n, is given by

$$\frac{c_q}{n}\left(1+O\left(\frac{1}{n}\right)\right).$$

The factor c_q depends only on q and satisfies

$$0 < c_q = C + O\left(q^{-\beta}\right),$$

where $C = (1-e^{-\gamma})^{-1} = 2.280291...$, γ denotes Euler's constant and $\beta = 0.4109....$

Polynomial Analogue: divisors of every degree

Ex.: $T(T^2+T+1)(T^4+T+1) \in \mathbb{F}_2[T]$ has divisors of deg $1,\ldots,7$.

Ex.: $T(T^3+T+1)(T^3+T^2+1) \in \mathbb{F}_2[T]$ has no divisor of degree 2.

W. (2015): The proportion of polynomials of degree n over $\mathbb{F}_q$, which have a divisor of every degree below n, is given by

$$\frac{c_q}{n}\left(1+O\left(\frac{1}{n}\right)\right).$$

The factor c_q depends only on q and satisfies

$$0 < c_q = C + O\left(q^{-\beta}\right),$$

where $C = (1-e^{-\gamma})^{-1} = 2.280291...$, γ denotes Euler's constant and $\beta = 0.4109....$

Corollary: The proportion in question is $\dfrac{C}{n}\left(1+O\left(\dfrac{1}{n}+\dfrac{1}{q^{\beta}}\right)\right)$.

Functional Equation

Let $F = P_1 P_2 \cdots P_k$, $\deg(P_1) \leq \ldots \leq \deg(P_k)$. Then F has a divisor of every degree below n if and only if

$$\deg(P_j) \leq 1 + \sum_{1 \leq i < j} \deg(P_i) \qquad (1 \leq j \leq k).$$

Functional Equation

Let $F = P_1 P_2 \cdots P_k$, $\deg(P_1) \leq \ldots \leq \deg(P_k)$. Then F has a divisor of every degree below n if and only if

$$\deg(P_j) \leq 1 + \sum_{1 \leq i < j} \deg(P_i) \qquad (1 \leq j \leq k).$$

- Count all monic polynomials of degree n over $\mathbb{F}_q$ (there are q^n of them) according to their largest divisor which has itself a divisor of every degree:

$$q^n = \sum_{G \text{ has divisor of every degree}} r\big(n - \deg(G), \deg(G) + 1\big)$$

Functional Equation

Let $F = P_1 P_2 \cdots P_k,\ \deg(P_1) \leq \ldots \leq \deg(P_k)$. Then F has a divisor of every degree below n if and only if

$$\deg(P_j) \leq 1 + \sum_{1 \leq i < j} \deg(P_i) \qquad (1 \leq j \leq k).$$

- Count all monic polynomials of degree n over $\mathbb{F}_q$ (there are q^n of them) according to their largest divisor which has itself a divisor of every degree:

$$q^n = \sum_{G \text{ has divisor of every degree}} r\big(n - \deg(G), \deg(G) + 1\big)$$

- Approximate $r(\cdot, \cdot)$ in terms of Buchstab's function $\omega(\cdot)$.

Functional Equation

Let $F = P_1 P_2 \cdots P_k$, $\deg(P_1) \leq \ldots \leq \deg(P_k)$. Then F has a divisor of every degree below n if and only if

$$\deg(P_j) \leq 1 + \sum_{1 \leq i < j} \deg(P_i) \qquad (1 \leq j \leq k).$$

- Count all monic polynomials of degree n over $\mathbb{F}_q$ (there are q^n of them) according to their largest divisor which has itself a divisor of every degree:

$$q^n = \sum_{G \text{ has divisor of every degree}} r\big(n - \deg(G), \deg(G) + 1\big)$$

- Approximate $r(\cdot, \cdot)$ in terms of Buchstab's function $\omega(\cdot)$.
- Abel Summation $\rightarrow$ Integral Equation $\rightarrow$ Laplace Transform $\rightarrow$ Inversion of Laplace Transform

Another analogy: integers and permutations

S_n =set of permutations of $\{1, 2, 3, \ldots, n\}$.

Another analogy: integers and permutations

S_n =set of permutations of $\{1, 2, 3, \ldots, n\}$.

integers $\asymp x$	S_n
prime factors	cycles
$P(m \asymp x \text{ is prime }) \sim \frac{1}{\log x}$	$P(\sigma \in S_n \text{ is a cycle }) = \frac{1}{n}$

Rough permutations: no cycles of small length

Let $p(n, m)$ be the proportion of $\sigma \in S_n$, all of whose cycles have length $> m$.

Rough permutations: no cycles of small length

Let $p(n,m)$ be the proportion of $\sigma \in S_n$, all of whose cycles have length $> m$.

Manstavičius, Petuchovas (2015); W. (2015):
Let $u = n/m$. For $n > m \geq 1$ we have

$$p(n,m) = e^{\gamma - H_m} \omega(u) \left(1 + O\left(\frac{(u/e)^{-u}}{m} \right) \right).$$

where H_m is the m-th harmonic number.

Permutations which fix sets of every size

Example: The permutation $(1)(23)(4567)$ fixes the sets $\{1\}, \{2,3\}, \{1,2,3\}, \{4,5,6,7\}, \{1,4,5,6,7\}, \{2,3,4,5,6,7\}, \{1,2,3,4,5,6,7\}$.

Permutations which fix sets of every size

Example: The permutation $(1)(23)(4567)$ fixes the sets $\{1\}, \{2,3\}, \{1,2,3\}, \{4,5,6,7\}, \{1,4,5,6,7\}, \{2,3,4,5,6,7\}, \{1,2,3,4,5,6,7\}$.

Example: The permutation $(1)(234)(567)$ does not fix any set with two elements.

Permutations which fix sets of every size

Example: The permutation $(1)(23)(4567)$ fixes the sets $\{1\}, \{2,3\}, \{1,2,3\}, \{4,5,6,7\}, \{1,4,5,6,7\}, \{2,3,4,5,6,7\}, \{1,2,3,4,5,6,7\}$.

Example: The permutation $(1)(234)(567)$ does not fix any set with two elements.

W. (2015): The proportion of permutations $\sigma \in S_n$, with the property that for every positive integer $m \leq n$ there exists a set $M \subseteq \{1,2,3,\ldots,n\}$ with cardinality m such that $\sigma(M) = M$, is given by

$$\frac{C}{n}\left(1 + O\left(\frac{1}{n}\right)\right),$$

where $C = (1 - e^{-\gamma})^{-1} = 2.280291\ldots$

Romanoff's Theorem

Romanoff (1934): Given an integer $a \geq 2$, a positive proportion of integers can be written in the form $p + a^k$, where p is prime.

Romanoff's Theorem

Romanoff (1934): Given an integer $a \geq 2$, a positive proportion of integers can be written in the form $p + a^k$, where p is prime.

Pintz (2006): If $a = 2$, this proportion is at least 0.09368.

Romanoff's Theorem

Romanoff (1934): Given an integer $a \geq 2$, a positive proportion of integers can be written in the form $p + a^k$, where p is prime.

Pintz (2006): If $a = 2$, this proportion is at least 0.09368.

For $g \in \mathbb{F}_q[x]$, let $R(n, g, q)$ be the proportion of monic polynomials f of degree n, which can be written as $f = h + g^k$, where h is a monic irreducible polynomial of degree n and k is a nonnegative integer.

Romanoff's Theorem

Romanoff (1934): Given an integer $a \geq 2$, a positive proportion of integers can be written in the form $p + a^k$, where p is prime.

Pintz (2006): If $a = 2$, this proportion is at least 0.09368.

For $g \in \mathbb{F}_q[x]$, let $R(n, g, q)$ be the proportion of monic polynomials f of degree n, which can be written as $f = h + g^k$, where h is a monic irreducible polynomial of degree n and k is a nonnegative integer.

Shparlinski, W. (2015): Let $\delta = \deg(g) \geq 1$. We have

$$R(n, g, q) = \frac{1}{\delta}\left(1 + O\left(\frac{\delta}{n} + \frac{\log 2\delta}{\delta}\right)\right),$$

Romanoff's Theorem

Romanoff (1934): Given an integer $a \geq 2$, a positive proportion of integers can be written in the form $p + a^k$, where p is prime.

Pintz (2006): If $a = 2$, this proportion is at least 0.09368.

For $g \in \mathbb{F}_q[x]$, let $R(n, g, q)$ be the proportion of monic polynomials f of degree n, which can be written as $f = h + g^k$, where h is a monic irreducible polynomial of degree n and k is a nonnegative integer.

Shparlinski, W. (2015): Let $\delta = \deg(g) \geq 1$. We have

$$R(n, g, q) = \frac{1}{\delta}\left(1 + O\left(\frac{\delta}{n} + \frac{\log 2\delta}{\delta}\right)\right),$$

and

$$\frac{0.01}{\delta} < r(n, g, q) \leq \frac{2}{\delta}.$$

Romanoff's Theorem: main ingredient

Romanoff (1934): Let $a \geq 2$. We have

$$\sum_{\substack{n \geq 1 \\ \gcd(n,a)=1}} \frac{\mu^2(n)}{n \operatorname{ord}_n(a)} \ll 1.$$

Romanoff's Theorem: main ingredient

Romanoff (1934): Let $a \geq 2$. We have

$$\sum_{\substack{n \geq 1 \\ \gcd(n,a)=1}} \frac{\mu^2(n)}{n \operatorname{ord}_n(a)} \ll 1.$$

Shparlinski, W. (2015): Let $\delta = \deg(g) \geq 1$. We have

$$\sum_{\gcd(f,g)=1} \frac{\mu^2(f)}{|f| \operatorname{ord}_f(g)} \leq 1 + e^{\gamma} \min\left\{5\sqrt{\delta/q},\ \frac{\log 6\delta}{\log q}\right\}.$$

Romanoff's Theorem: main ingredient

Romanoff (1934): Let $a \geq 2$. We have

$$\sum_{\substack{n \geq 1 \\ \gcd(n,a)=1}} \frac{\mu^2(n)}{n \operatorname{ord}_n(a)} \ll 1.$$

Shparlinski, W. (2015): Let $\delta = \deg(g) \geq 1$. We have

$$\sum_{\gcd(f,g)=1} \frac{\mu^2(f)}{|f| \operatorname{ord}_f(g)} \leq 1 + e^{\gamma} \min\left\{5\sqrt{\delta/q}, \frac{\log 6\delta}{\log q}\right\}.$$

Thank you!