Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
2023, Volume 29, Number 3, 564–570
DOI: 10.7546/nntdm.2023.29.3.564-570

The average value of a certain number-theoretic function over the primes

Louis Rubin

Department of Mathematics, Florida State University
Tallahassee, Florida, United States
e-mail: ljr22@fsu.edu

Received: 18 April 2023 **Revised:** 21 July 2023
Accepted: 26 July 2023 **Online First:** 2 August 2023

Abstract: We consider functions $F : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ for which there exists a positive integer n such that two conditions hold: $F(p)$ divides n for every prime p, and for each divisor d of n and every prime p, we have that d divides $F(p)$ iff d divides $F(p \bmod d)$. Following an approach of Khrennikov and Nilsson, we employ the prime number theorem for arithmetic progressions to derive an expression for the average value of such an F over all primes p, recovering a theorem of these authors as a special case. As an application, we compute the average number of r-periodic points of a multivariate power map defined on a product $Z_{f_1(p)} \times \cdots \times Z_{f_m(p)}$ of cyclic groups, where $f_i(t)$ is a polynomial.
Keywords: Average value, Prime number, Periodic points, Cyclic groups.
2020 Mathematics Subject Classification: 37C25, 11N37.

1 Introduction and Main result

The famous Prime Number Theorem for Arithmetic Progressions provides an asymptotic formula (as $M \to \infty$) for the number of primes less than or equal to M and congruent to a modulo n, where $n, a \in \mathbb{N}$ are relatively prime. To state the this result precisely, let us fix some notation.

Given integers n, a and $M > 0$, let

$$\pi(n, a, M) = |\{p \le M : p \text{ prime}, p \equiv a \pmod n\}|.$$

(We denote $\pi(1, 0, M)$, the number of primes less than or equal to M, simply by $\pi(M)$.) For each $k \in \mathbb{N}$, let $\varphi(k)$ equal the number of positive integers less than or equal to k and relatively prime to k. The result is as follows.

Theorem 1. *Let $n, a \in \mathbb{N}$ with $\gcd(n, a) = 1$. Then*

$$\pi(n, a, M) \sim \frac{\pi(M)}{\varphi(n)} \text{ as } M \to \infty.$$

According to Dirichlet's theorem on primes in arithmetic progressions, there are infinitely many primes of the form $a + nk$ when a, n are relatively prime. Intuitively, Theorem 1 says that the primes are evenly distributed among those congruence classes modulo n that accommodate infinitely many of them.

In [1], Khrennikov and Nilsson derive the following interesting formula as a consequence of Theorem 1. Below, $\tau(n)$ denotes the number of positive divisors of n.

Theorem 2. *For any positive integer n, we have*

$$\lim_{M\to\infty} \frac{1}{\pi(M)} \sum_{\substack{p \le M \\ p \text{ prime}}} \gcd(n, p-1) = \tau(n).$$

Khrennikov and Nilsson apply Theorem 2 to study the distribution (with respect to the parameter p) of periodic points of a single-variable power map $x \mapsto x^n$ defined on the p-adic numbers. In this note, we shall derive a vast generalization of the above formula. As an application, we mimic the approach in [1] to prove analogous results concerning periodic points of a multivariate power map $(x_1, \dots, x_m) \mapsto (x_1^{n_1}, \dots, x_m^{n_m})$ defined on defined on a product $Z_{f_1(p)} \times \dots \times Z_{f_m(p)}$ of cyclic groups, where $f_i(t)$ is a polynomial with integer coefficients.

For a discussion of the prime numbers' role in a variety of theoretical and practical applications, we suggest [2].

Our main result is as follows.

Theorem 3. *Let $F : \mathbb{Z}_{\ge 0} \to \mathbb{Z}_{\ge 0}$ for which there exists $n \in \mathbb{N}$ such that two conditions hold:*

1. *$F(p)|n$ for each prime p.*
2. *For each divisor d of n, we have that $d|F(p) \iff d|F(p \bmod d)$.*

Then

$$\lim_{M\to\infty} \frac{1}{\pi(M)} \sum_{\substack{p \le M \\ p \text{ prime}}} F(p) = \sum_{d|n} |\{0 \le y \le d-1 : d|F(y) \text{ and } \gcd(y, d) = 1\}|. \tag{1}$$

Before deriving Theorem 3, let us look at some particular instances of the function F.

Example 4. For any fixed $n \in \mathbb{N}$ and $f \in \mathbb{Z}[t]$, the function $F(x) = \gcd(n, f(x))$ satisfies the hypotheses of the theorem. Indeed, the range of this F consists of divisors of n, and the second condition is satisfied since polynomials preserve congruence. We get

$$\lim_{M\to\infty} \frac{1}{\pi(M)} \sum_{p\ \leq M} \gcd(n, f(p)) = \sum_{d|n} |\{0 \leq y \leq d-1 : d|f(y) \text{ and } \gcd(y, d) = 1\}|.$$

Setting $f(t) = t - 1$ yields Khrennikov and Nilsson's formula, as the right-hand side reduces to $\sum_{d|n} 1 = \tau(n)$ in this case.

Example 5. We may just as well take F to be the $\gcd$ of more than two quantities, e.g.,

$$F(x) = \gcd(n, f(x), g(x)),$$

for a fixed positive integer n and $f, g \in \mathbb{Z}[t]$. For instance, take $n = 6$, $f(t) = t^2 - 1$, and $g(t) = 3t^3 + 1$ to get

$$F(x) = \gcd(6, x^2 - 1, 3x^3 + 1).$$

In this case, the right-hand side of (1) evaluates to 2, so we have

$$\lim_{M\to\infty} \frac{1}{\pi(M)} \sum_{p\leq M} \gcd(6, p^2 - 1, 3p^3 + 1) = 2.$$

Now for the proof, which essentially reproduces the argument for Theorem 2 appearing in [1] at the appropriate level of abstraction.

Proof of Theorem 3. Let the assumptions on F hold. It is a basic fact that for each $N \in \mathbb{N}$,

$$N = \sum_{d|N} \varphi(d).$$

Therefore, for each prime p, we obtain

$$F(p) = \sum_{d|F(p)} \varphi(d).$$

Summing over all $p \leq M$ gives

$$\sum_{p\leq M} F(p) = \sum_{p\leq M} \sum_{d|F(p)} \varphi(d).$$

Recalling that each value $F(p)$ is a divisor of n, we may rearrange the right-hand side to get

$$\sum_{p\leq M} F(p) = \sum_{d|n} \varphi(d)\pi(d, M),$$

where $\pi(d, M) := |\{p \leq M : d|F(p)\}|$. For each $d|n$, let

$$C(d) := |\{0 \leq y \leq d-1 : d|F(y),\ \gcd(y, d) = 1\}|.$$

We have

$$\frac{1}{\pi(M)} \sum_{p\leq M} F(p) = \sum_{\substack{d|n \\ C(d)=0}} \frac{\pi(d, M)\varphi(d)}{\pi(M)} + \sum_{\substack{d|n \\ C(d)>0}} \frac{\pi(d, M)\varphi(d)}{\pi(M)}. \tag{2}$$

Suppose that $d|n$ with $C(d) = 0$. Let $p \leq M$ such that $d|F(p)$. Let $y = p \bmod d$. By assumption, $d|F(y)$, and it follows that $\gcd(y, d) > 1$. But $\gcd(y, d) = \gcd(p, d)$, so we get that $\gcd(y, d) = p$. In particular, $p|d$. Hence, $\pi(d, M)$ is bounded. Thus,

$$\lim_{M\to\infty} \frac{\pi(d, M)\varphi(d)}{\pi(M)} = 0,$$

so the first sum in (2) tends to zero as $M \to \infty$. Now suppose that $C(d) > 0$. Let

$$S(d) := \{0 \leq y \leq d - 1 : d|F(y)\}.$$

The hypotheses on F ensure that

$$\{p \leq M : d|F(p)\} = \{p \leq M : p \equiv y \pmod{d} \textit{ for some } y \in S(d)\}.$$

But the primes are equally distributed among the congruence classes (mod d) of those $y \in S(d)$ with $\gcd(y, d) = 1$, so we have

$$\pi(d, M) \sim C(d)\frac{\pi(M)}{\varphi(d)}$$

as $M \to \infty$. That is,

$$\lim_{M\to\infty} \frac{\pi(d, M)\varphi(d)}{C(d)\pi(M)} = 1.$$

Thus, from (2), we get

$$\lim_{M\to\infty} \frac{1}{\pi(M)} \sum_{p\leq M} F(p) = \lim_{M\to\infty} \sum_{\substack{d|n \\ C(d)>0}} \frac{\pi(d, M)\varphi(d)}{C(d)\pi(M)} C(d) = \sum_{d|n} C(d).$$

Therefore,

$$\lim_{M\to\infty} \frac{1}{\pi(M)} \sum_{\substack{p \leq M \\ p \text{ prime}}} F(p) = \sum_{d|n} |\{0 \leq y \leq d - 1 : d|F(y) \textit{ and } \gcd(y, d) = 1\}|.$$

Theorem 3 is obtained. □

We can modify the function from Example 4 as follows. Fix $n_1, \ldots, n_m \in \mathbb{N}$ and $f_1, \ldots, f_m \in \mathbb{Z}[t]$. The function $F(x) = \prod_{1\leq i\leq m} \gcd(n_i, f_i(x))$ satisfies the hypotheses of Theorem 3. (Take n to be the product of the n_i's.) Thus, we get the following corollary, which will be useful for our application.

Corollary 6. For any $n_1, \ldots, n_m \in \mathbb{N}$ and any $f_1, \ldots, f_m \in \mathbb{Z}[t]$,

$$\lim_{M\to\infty} \frac{1}{\pi(M)} \sum_{p\leq M} \prod_{1\leq i\leq m} \gcd(n_i, f_i(p))$$

$$= \sum_{d|n_1\cdots n_m} \Big|\{0 \leq y \leq d - 1 : d| \prod_{1\leq i\leq m} \gcd(n_i, f_i(y)) \textit{ and } \gcd(y, d) = 1\}\Big|.$$

2 Application: Periodic points of a multivariate power map

We now present an application of Corollary 6. Let p represent a prime number and let $\mathcal{F} = \{f_1, \ldots, f_m\}$ be a family of polynomials over $\mathbb{Z}$ taking positive values on the primes. For positive integers $n_1, \ldots, n_m$, define

$$f : Z_{f_1(p)} \times \cdots \times Z_{f_m(p)} \to Z_{f_1(p)} \times \cdots \times Z_{f_m(p)}$$

by

$$f(x_1, \ldots, x_m) = (x_1^{n_1}, \ldots, x_m^{n_m}), \tag{3}$$

where for each $k \in \mathbb{N}$, Z_k refers to the cyclic group of order k. A point $(x_1, \ldots, x_m)$ is called *periodic* if $f^r(x_1, \ldots, x_m) = (x_1, \ldots, x_m)$ for some positive integer r, where f^r, the *r-th iterate* of f, is the composition of f with itself r times. The *period* of such a point is the smallest positive integer r such that $f^r(x_1, \ldots, x_m) = (x_1, \ldots, x_m)$. We refer to a periodic point with period r as *r-periodic*.

By mimicking the approach in [1], we shall compute the average number of r-periodic points of f over the primes p. Specifically, if $N(r, p, n_1, \ldots, n_m, \mathcal{F})$ denotes the number of r-periodic points of the map (3), then our task is to evaluate

$$\lim_{M \to \infty} \frac{1}{\pi(M)} \sum_{p \leq M} N(r, p, n_1, \ldots, n_m, \mathcal{F})$$

in terms of the parameters $r, p, n_1, \ldots, n_m, \mathcal{F}$.

Following Khrennikov and Nilsson, let us begin by computing $N(r, p, n_1, \ldots, n_m, \mathcal{F})$ when p is fixed and $n_i \geq 2$, $1 \leq i \leq m$. As usual, μ will denote the Möbius function. It is a basic fact that if $g \in Z_k$ and the equation $x^n = g$ has a solution in Z_k, then there are exactly $\gcd(n, k)$ solutions. But $(x_1, \ldots, x_m) \in Z_{f_1(p)} \times \cdots \times Z_{f_m(p)}$ has period dividing r if and only if

$$x_i^{n_i^r} = x_i \iff x_i^{n_i^r - 1} = 1 \text{ for each } 1 \leq i \leq m.$$

The latter equation above has $\gcd(n_i^r - 1, f_i(p))$ solutions in $Z_{f_i(p)}$, so there are

$$\prod_{1 \leq i \leq m} \gcd(n_i^r - 1, f_i(p))$$

periodic points in $Z_{f_1(p)} \times \cdots \times Z_{f_m(p)}$ whose period divides r. That is,

$$\sum_{d \mid r} N(d, p, n_1, \ldots, n_m, \mathcal{F}) = \prod_{1 \leq i \leq m} \gcd(n_i^r - 1, f_i(p)).$$

By Möbius inversion, we obtain the following theorem.

Theorem 7. *For f as in (3) with $n_i \geq 2$ for each $1 \leq i \leq m$, the number $N(r, p, n_1, \ldots, n_m, \mathcal{F})$ of r-periodic points of f equals*

$$\sum_{d \mid r} \mu(d) \prod_{1 \leq i \leq m} \gcd(n_i^{\frac{r}{d}} - 1, f_i(p)).$$

Example 8. Consider the map $f : Z_3 \times Z_4$ given by $f(x_1, x_2) = (x_1^2, x_2^3)$. Here, we can take $p = 2$, $f_1 = x + 1$, $f_2 = x^2$, $n_1 = 2$, and $n_2 = 3$. For $r = 2$, the number of 2-periodic points is found to be 10.

An r*-cycle* for the map f in (3) is a set $\{x, f(x), \ldots, f^{r-1}(x)\}$, where $x \in Z_{f_1(p)} \times \cdots \times Z_{f_m(p)}$ is an r-periodic point. Letting $K(r, p, n_1, \ldots, n_m, \mathcal{F})$ denote the number of r-cycles associated with f, we see that

$$K(r, p, n_1, \ldots, n_m, \mathcal{F}) = \frac{N(r, p, n_1, \ldots, n_m, \mathcal{F})}{r},$$

since each r-cycle contains r periodic points of period r. In particular, we obtain the following interesting number-theoretic fact, which extends the result of Remark 3.3 in [1]: *For any prime* p*, any* $2 \leq n_1, \ldots, n_m \in \mathbb{N}$*, and any* $\mathcal{F} = \{f_1, \ldots, f_m\} \subseteq \mathbb{Z}[t]$ *such that* $f_i(p) > 0$*, the quantity* $\sum_{d|r} \mu(d) \prod_{1\leq i\leq m} \gcd(n_i^{\frac{r}{d}} - 1, f_i(p))$ *is divisible by* r*.*

The next theorem, which follows in light of Corollary 6 and Theorem 7, summarizes our findings.

Theorem 9. *Let* $n_1, \ldots, n_m \in \mathbb{N}$ *with each* $n_i \geq 2$*, and let* $\mathcal{F} = \{f_1, \ldots, f_m\}$ *be polynomials over* $\mathbb{Z}$ *taking positive values on the primes. For* p *prime, define* $f : Z_{f_1(p)} \times \cdots \times Z_{f_m(p)} \to Z_{f_1(p)} \times \cdots \times Z_{f_m(p)}$ *by*

$$f(x_1, \ldots, x_m) = (x_1^{n_1}, \ldots, x_m^{n_m}).$$

If $N(r, p, n_1, \ldots, n_m, \mathcal{F})$ *denotes the number of* r*-periodic points of* f *corresponding to the prime* p*, then*

$$\lim_{M\to\infty} \frac{1}{\pi(M)} \sum_{p\leq M} N(r, p, n_1, \ldots, n_m, \mathcal{F}) = \sum_{\substack{(d,\, e) \\ d|r \text{ and } e|(n_1^{\frac{r}{d}} - 1)\cdots(n_m^{\frac{r}{d}} - 1)}} \mu(d)C(d, e),$$

where

$$C(d, e) := \left|\{0 \leq y \leq e - 1 : e \textit{ divides } \prod_{1\leq i\leq m} \gcd(n_i^{\frac{r}{d}} - 1, f_i(y)) \textit{ and } \gcd(y, e) = 1\}\right|.$$

Example 10. Consider the map

$$f : Z_{p^2-1} \times Z_{3p^4+2p^2-1} \times Z_{p^7+p^3-1} \to Z_{p^2-1} \times Z_{3p^4+2p^2-1} \times Z_{p^7+p^3-1}$$

defined by $f(x_1, x_2, x_3) = (x_1^3, x_2^6, x_3^7)$. Here, $m = 3$, $f_1 = t^2 - 1$, $f_2 = 3t^4 + 2t^2 - 1$, $f_3 = t^7 + t^3 - 1$, and $(n_1, n_2, n_3) = (3, 6, 7)$. For $r = 2$, the average number of 2-periodic points is calculated to be 36.

Acknowledgements

I thank Greg Martin and math.stackexchange.com user 'reuns' for elucidating the distribution of primes satisfying certain congruences; I would not have formulated my results without their help.

Also, I thank an anonymous referee for suggesting the trick at the start of the proof of Theorem 3, which considerably simplified my argument for an earlier, more specialized version of this result, and inspired me to generalize further. Finally, I am grateful for the support and encouragement of my family and friends.

References

[1] Khrennikov, A., & Nilsson, M. (2001). On the number of cycles of p-adic dynamical systems. *Journal of Number Theory*, 90, 255–264.

[2] Oleschko, K., Khrennikov, A., Oleshko, B., & Parrot, J. (2017). The primes are everywhere, but nowhere... *New Trends and Advanced Methods in Interdisciplinary Mathematical Sciences*, Springer, 155–167.