Idempotents and Nilpotents Modulo n

Steven Finch

April 30, 2006

Abstract. We study asymptotic properties of periods and transient phases associated with modular power sequences. The latter are simple; the former are vaguely related to the reciprocal sum of square-free integer kernels.

Let $\mathbb{Z}_n$ denote the ring of integers modulo n. Define $S(x)$ to be the sequence $\{x^k\}_{k=0}^{\infty}$ for each $x \in \mathbb{Z}_n$. We wish to understand the periodicity properties of $S(x)$, that is, the statistics of

$$\sigma(x) = \begin{array}{l}\text{the } \textbf{period} \\ \text{of } S(x)\end{array} = \begin{array}{l}\text{the least } m \geq 1 \text{ for which } x^{k+m} = x^k \\ \text{for all sufficiently large } k,\end{array}$$

$$\tau(x) = \begin{array}{l}\text{the } \textbf{transient} \\ \textbf{phase} \text{ of } S(x)\end{array} = \begin{array}{l}\text{the least } \ell \geq 0 \text{ for which } x^{k+\sigma(x)} = x^k \\ \text{for all } k \geq \ell.\end{array}$$

For example, the unique x with $(\sigma, \tau) = (1, 0)$ is $x = 1$. If $(\sigma, \tau) = (2, 0)$, then x is a square root of unity; if $(\sigma, \tau) = (3, 0)$, then x is a cube root of unity [1]. If $\tau = 0$ (with no condition placed on σ), then x is relatively prime to n. Hence the number of such x is

$$\#\left\{x \in \mathbb{Z}_n : x^k = 1 \text{ for some } k \geq 1\right\} = \varphi(n)$$

where φ is the Euler totient function and, asymptotically [1, 2],

$$\sum_{n \leq N} \varphi(n) \sim \frac{3}{\pi^2} N^2 = (0.303963550927...) N^2$$

as $N \to \infty$. As another example, if $(\sigma, \tau) = (1, 1)$, then x is an **idempotent**. The number of such x, including 0 and 1, is

$$\#\left\{x \in \mathbb{Z}_n : x^2 = x\right\} = 2^{\omega(n)}$$

where $\omega(n)$ denotes the number of distinct prime factors of n and [1, 3]

$$\sum_{n \leq N} 2^{\omega(n)} \sim \frac{6}{\pi^2} N \cdot \ln N$$

as $N \to \infty$. More difficult examples appear in the following sections. As in [1], we make no claim of originality: Our purpose is only to gather relevant formulas in one place.

1. Generalized Idempotents

1.1. Bounded Transient Phase. If $\tau \leq 1$ (with no condition placed on σ), then the number of such x is [3]

$$a(n) = \#\left\{x \in \mathbb{Z}_n : x^{k+1} = x \text{ for some } k \geq 1\right\}.$$

This is a multiplicative function of n and

$$a(p^r) = \begin{cases} p & \text{if } r = 1, \\ p^r - p^{r-1} + 1 & \text{if } r \geq 2. \end{cases}$$

Let

$$\begin{aligned} F(s) &= \sum_{n=1}^{\infty} \frac{a(n)}{n^{s+1}} = \prod_p \left(1 + \sum_{r=1}^{\infty} \frac{p^r - p^{r-1} + 1}{p^{r(s+1)}}\right) \\ &= \prod_p \left(1 + \frac{p^{s+2} - 2p + 1}{p(p^{s+1} - 1)(p^s - 1)}\right) = G(s) \cdot \zeta(s). \end{aligned}$$

Hence, by the Selberg-Delange method [1, 4, 5, 6],

$$\sum_{n \leq N} a(n) \sim \frac{1}{2} G(1) \cdot N^2 = A \cdot N^2$$

as $N \to \infty$, where

$$A = \frac{1}{2} \prod_p \left(1 - \frac{1}{p^2(p+1)}\right) = 0.440756919862...$$

(the *quadratic class constant* described in [7], divided by two). Joshi [8] obtained this result via a different approach and found an alternative formula:

$$A = \frac{3}{\pi^2} \sum_{\ell=1}^{\infty} \left(\frac{1}{\ell^2} \cdot \prod_{p|\ell} \frac{p}{p+1}\right)$$

but did not numerically evaluate this expression.

If $\tau \leq 2$ (with no condition placed on σ), then the number of such x is [3]

$$b(n) = \#\left\{x \in \mathbb{Z}_n : x^{k+2} = x^2 \text{ for some } k \geq 1\right\}.$$

This is a multiplicative function of n and

$$b(p^r) = \begin{cases} p^r & \text{if } r \leq 2, \\ p^r - p^{r-1} + p^{(r-1)/2} & \text{if } r \geq 3 \text{ and } r \equiv 1 \bmod 2, \\ p^r - p^{r-1} + p^{r/2} & \text{if } r \geq 4 \text{ and } r \equiv 0 \bmod 2. \end{cases}$$

From

$$\sum_{n=1}^{\infty}\frac{b(n)}{n^{s+1}} = \prod_p\left(1+\sum_{\substack{r\geq 1,\\ r\equiv 1 \bmod 2}}\frac{p^r-p^{r-1}+p^{(r-1)/2}}{p^{r(s+1)}}+\sum_{\substack{r\geq 2,\\ r\equiv 0 \bmod 2}}\frac{p^r-p^{r-1}+p^{r/2}}{p^{r(s+1)}}\right)$$
$$= \prod_p\left(1+\frac{p^{3s+2}+p^{2s+2}-2p^{s+1}+p^s-2p+1}{p(p^{2s+1}-1)(p^{2s}-1)}\right),$$

we deduce that $\sum_{n\leq N} b(n)\sim B\cdot N^2$, where

$$B=\frac{1}{2}\prod_p\left(1-\frac{1}{p^2(p^2+p+1)}\right)=0.477176626987....$$

If $\tau\leq 3$ (with no condition placed on σ), then the number of such x is [3]

$$c(n)=\#\left\{x\in\mathbb{Z}_n : x^{k+3}=x^3 \text{ for some } k\geq 1\right\}.$$

This is a multiplicative function of n and

$$c(p^r)=\begin{cases} p^r & \text{if } r\leq 3,\\ p^r-p^{r-1}+p^{2(r-1)/3} & \text{if } r\geq 4 \text{ and } r\equiv 1 \bmod 3,\\ p^r-p^{r-1}+p^{(2r-1)/3} & \text{if } r\geq 5 \text{ and } r\equiv 2 \bmod 3,\\ p^r-p^{r-1}+p^{2r/3} & \text{if } r\geq 6 \text{ and } r\equiv 0 \bmod 3.\end{cases}$$

From

$$\sum_{n=1}^{\infty}\frac{c(n)}{n^{s+1}} = \prod_p\left(1+\sum_{\substack{r\geq 1,\\ r\equiv 1 \bmod 3}}\frac{p^r-p^{r-1}+p^{2(r-1)/3}}{p^{r(s+1)}}+\sum_{\substack{r\geq 2,\\ r\equiv 2 \bmod 3}}\frac{p^r-p^{r-1}+p^{(2r-1)/3}}{p^{r(s+1)}}\right.$$
$$\left.+\sum_{\substack{r\geq 3,\\ r\equiv 0 \bmod 3}}\frac{p^r-p^{r-1}+p^{2r/3}}{p^{r(s+1)}}\right)$$
$$= \prod_p\left(1+\frac{p^{5s+2}+p^{4s+2}+p^{3s+2}-2p^{2s+1}+p^{2s}-2p^{s+1}+p^s-2p+1}{p(p^{3s+1}-1)(p^{3s}-1)}\right),$$

we deduce that $\sum_{n\leq N} c(n)\sim C\cdot N^2$, where

$$C=\frac{1}{2}\prod_p\left(1-\frac{1}{p^2(p^3+p^2+p+1)}\right)=0.490145568004....$$

The pattern exhibited by A, B, C is clear and deserves proof for $\tau\leq T$, for arbitrary T. A different attempt [9] to determine the asymptotics of $\sum_{n\leq N} b(n)$ and of $\sum_{n\leq N} c(n)$ unfortunately turned out to be erroneous [10].

1.2. Bounded Period. If $\sigma = 1$ (with no condition placed on τ), then the number of such x is [11]

$$u(n) = \#\left\{x \in \mathbb{Z}_n : x^{k+1} = x^k \text{ for some } k \geq 0\right\}.$$

This is a multiplicative function of n and

$$u(p^r) = \begin{cases} 2 & \text{if } r = 1, \\ p^{r-1} + 1 & \text{if } r \geq 2. \end{cases}$$

From

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{u(n)}{n^s} &= \prod_p \left(1 + \sum_{r=1}^{\infty} \frac{p^{r-1}+1}{p^{rs}}\right) \\ &= \prod_p \left(1 + \frac{2p^s - p - 1}{p(p^s-1)(p^{s-1}-1)}\right) \end{aligned}$$

we *would like* to deduce that $\sum_{n \leq N} u(n) \sim U \cdot f(N)$ for some simple expression $f(N)$. Unfortunately this is an unsolved problem. More details are found in section [2].

If $\sigma \leq 2$ (with no condition placed on τ), then the number of such x is [11]

$$v(n) = \#\left\{x \in \mathbb{Z}_n : x^{k+2} = x^k \text{ for some } k \geq 0\right\}.$$

This is a multiplicative function of n and

$$v(p^r) = \begin{cases} 2^r & \text{if } p = 2 \text{ and } r \leq 2, \\ 2^{r-1} + 4 & \text{if } p = 2 \text{ and } r \geq 3, \\ 3 & \text{if } p > 2 \text{ and } r = 1, \\ p^{r-1} + 2 & \text{if } p > 2 \text{ and } r \geq 2. \end{cases}$$

From

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{v(n)}{n^s} &= \left(1 + \frac{2}{2^s} + \frac{4}{2^{2s}} + \sum_{r=3}^{\infty} \frac{2^{r-1}+4}{2^{rs}}\right) \cdot \prod_{p>2} \left(1 + \sum_{r=1}^{\infty} \frac{p^{r-1}+2}{p^{rs}}\right) \\ &= \left(1 + \frac{2}{2^s} + \frac{4}{2^{2s}} + \frac{2^{s+2} - 6}{2^{2s}(2^s-1)(2^{s-1}-1)}\right) \cdot \prod_{p>2} \left(1 + \frac{3p^s - 2p - 1}{p(p^s-1)(p^{s-1}-1)}\right) \end{aligned}$$

we *would like* to deduce that $\sum_{n \leq N} v(n) \sim V \cdot f(N)$, where $f(N)$ is the same expression as for $\sigma = 1$.

If $\sigma \leq 3$ (with no condition placed on τ), then the number of such x is [11]

$$\#\left\{x \in \mathbb{Z}_n : x^{k+3} = x^k \text{ or } x^{k+2} = x^k \text{ for some } k \geq 0\right\} = w(n) - u(n) + v(n)$$

where

$$w(n) = \#\left\{x \in \mathbb{Z}_n : x^{k+3} = x^k \text{ for some } k \geq 0\right\}.$$

The latter is a multiplicative function of n and

$$w(p^r) = \begin{cases} 2 & \text{if } p = 3 \text{ and } r = 1, \\ 3^{r-1}+3 & \text{if } p = 3 \text{ and } r \geq 2, \\ 2 & \text{if } p \equiv 2 \bmod 3 \text{ and } r = 1, \\ 4 & \text{if } p \equiv 1 \bmod 3 \text{ and } r = 1, \\ p^{r-1}+1 & \text{if } p \equiv 2 \bmod 3 \text{ and } r \geq 2, \\ p^{r-1}+3 & \text{if } p \equiv 1 \bmod 3 \text{ and } r \geq 2. \end{cases}$$

From

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{w(n)}{n^s} &= \left(1 + \frac{2}{3^s} + \sum_{r=2}^{\infty} \frac{3^{r-1}+3}{3^{rs}}\right) \cdot \prod_{p \equiv 2 \bmod 3} \left(1 + \sum_{r=1}^{\infty} \frac{p^{r-1}+1}{p^{rs}}\right) \\ &\quad \cdot \prod_{p \equiv 1 \bmod 3} \left(1 + \sum_{r=1}^{\infty} \frac{p^{r-1}+3}{p^{rs}}\right) \\ &= \left(1 + \frac{2}{3^s} + \frac{2 \cdot 3^s - 4}{3^s(3^s-1)(3^{s-1}-1)}\right) \cdot \prod_{p \equiv 2 \bmod 3} \left(1 + \frac{2p^s - p - 1}{p(p^s-1)(p^{s-1}-1)}\right) \\ &\quad \cdot \prod_{p \equiv 1 \bmod 3} \left(1 + \frac{4p^s - 3p - 1}{p(p^s-1)(p^{s-1}-1)}\right) \end{aligned}$$

we *would like* to deduce that $\sum_{n \leq N} w(n) \sim W \cdot f(N)$, where $f(N)$ is the same expression as for $\sigma = 1$ and $\sigma \leq 2$.

Note that $w - u + v$ is not multiplicative since $w(21) - u(21) + v(21) = 8 - 4 + 9 = 13$ while $w(3) - u(3) + v(3) = 2 - 2 + 3 = 3$ and $w(7) - u(7) + v(7) = 4 - 2 + 3 = 5$. It would easily follow that $\sum_{n \leq N}(w(n) - u(n) + v(n)) \sim (W - U + V) \cdot f(N)$, completing the case $\sigma \leq 3$, *if* the nature of $f(N)$ could be better ascertained.

1.3. Unbounded Period. Elements x of small period are apparently quite rare for large n. We will visit the other extreme. Consider, for example,

$$m(n) = \#\left\{x \in \mathbb{Z}_n : x^{k+\lceil \varphi(n)/2 \rceil} = x^k \text{ for some } k \geq 1\right\}$$

(the ceiling function is needed only for $1 \leq n \leq 2$, beyond which $\varphi(n)$ is always even). This is not a multiplicative function, but nevertheless can be simplified to

$$m(n) = \begin{cases} 3 & \text{if } n = 4, \\ \dfrac{p^{r-1}(p+1)}{2} & \text{if } n = p^r, \text{ where } p > 2 \text{ and } r \geq 1, \\ p^{r-1}(p+1) & \text{if } n = 2p^r, \text{ where } p > 2 \text{ and } r \geq 1, \\ n & \text{otherwise.} \end{cases}$$

From

$$\sum_{n=1}^{\infty} \frac{m(n)}{n^{s+1}} = \zeta(s) - \frac{1}{4^{s+1}} - \frac{2^s+1}{2^{s+1}} \sum_{p>2} \frac{p-1}{p(p^s-1)},$$

we deduce that $\sum_{n\le N} m(n) \sim (1/2)N^2$ since

$$0 < (s-1)\sum_p \frac{p-1}{p(p^s-1)} < (s-1)\sum_p \frac{1}{p^s} \sim -(s-1)\ln(s-1) \to 0^+$$

as $s \to 1^+$. The behavior of $\sum_{n\le N}(n-m(n))$ is more subtle. From

$$\sum_p \frac{p-1}{p(p^s-1)} \sim -\ln(s-1) \sim \sum_p \frac{1}{p^s}$$

and the fact that $\sum_{p\le N} p \sim N^2/(2\ln(N))$ via the Prime Number Theorem [12, 13], we deduce that

$$\sum_{n\le N}(n-m(n)) \sim \frac{3}{8}\frac{N^2}{\ln(N)}.$$

It would be interesting to replace $\lceil \varphi(n)/2 \rceil$ by more slowly-growing expressions and to see what asymptotic consequences arise.

2. NILPOTENTS

An element x of $\mathbb{Z}_n$ is **nilpotent** if its power sequence $S(x)$ is eventually zero. Define [14]

$$z(n) = \#\left\{x \in \mathbb{Z}_n : x^k = 0 \text{ for some } k \ge 1\right\}.$$

This is a multiplicative function of n and

$$z(p^r) = \begin{cases} 1 & \text{if } r = 1, \\ p^{r-1} & \text{if } r \ge 2. \end{cases}$$

Define also the **square-free kernel** $\kappa(n)$ to be the product of all distinct prime factors of n. Clearly $\kappa(p^r) = p$ for all $r \ge 1$ and hence $z(n) = n/\kappa(n)$ for all $n \ge 1$. From

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{z(n)}{n^s} &= \prod_p \left(1 + \sum_{r=1}^{\infty} \frac{p^{r-1}}{p^{rs}}\right) \\ &= \prod_p \left(1 + \frac{1}{p(p^{s-1}-1)}\right) \end{aligned}$$

we *would like* to deduce that $\sum_{n\leq N} z(n) \sim Z \cdot f(N)$ for some simple expression $f(N)$. Unfortunately, as discussed in section [1.2], this is an unsolved problem. De Bruijn [15, 16, 17, 18] proved that

$$\ln\left(\sum_{n\leq N}\frac{1}{\kappa(n)}\right) \sim \left(\frac{8\ln N}{\ln\ln N}\right)^{1/2} \sim \ln\left(\frac{1}{N}\sum_{n\leq N}\frac{n}{\kappa(n)}\right)$$

and Schwarz [19] proved that

$$\sum_{n\leq N}\frac{1}{\kappa(n)} \sim 2^{-1/4}(4\pi)^{-1/2}\left(\frac{\ln\ln N}{\ln N}\right)^{1/4}\left(\min_{0<y<\infty} N^y \cdot \sum_{n=1}^{\infty}\frac{1}{\kappa(n)n^y}\right).$$

A more concrete rightmost factor would be good to see someday.

3. Primitive Roots

We have not mentioned the group $\mathbb{Z}_n^*$ (under multiplication) of integers relatively prime to n in this paper thus far. A well-known counting problem concerns the number [20, 21, 22, 23]

$$g(n) = \#\left\{x \in \mathbb{Z}_n^* : \sigma(x) = \varphi(n)\right\}$$

of **primitive** $\varphi(n)^{\text{th}}$ **roots modulo** n. Equivalently, $g(n)$ is the number of generators of $\mathbb{Z}_n^*$. Clearly $g(n) > 0$ if and only if $\mathbb{Z}_n^*$ is a cyclic group; further,

$$g(n) = \begin{cases} \varphi(\varphi(n)) & \text{if } n = 1, 2, 4,\ q^j \text{ or } 2q^j, \text{ where } q \text{ is an odd prime and } j \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

Also define the **reduced totient** or **Carmichael function** [24]

$$\psi(n) = \begin{cases} \varphi(n) & \text{if } n = 1, 2, 4 \text{ or } q^j, \text{ where } q \text{ is an odd prime and } j \geq 1, \\ \varphi(n)/2 & \text{if } n = 2^k, \text{ where } k \geq 3, \\ \operatorname{lcm}\left\{\psi(p_j^{e_j}) : 1 \leq j \leq \ell\right\} & \text{if } n = p_1^{e_1}p_2^{e_2}\cdots p_\ell^{e_\ell}, \text{ where } 2 \leq p_1 < p_2 < \ldots \text{ and } \ell \geq 2, \end{cases}$$

which is the size of the largest cyclic subgroup of $\mathbb{Z}_n^*$, and consider the number [20, 25, 26, 27]

$$h(n) = \#\left\{x \in \mathbb{Z}_n^* : \sigma(x) = \psi(n)\right\}$$

of **primitive** $\psi(n)^{\text{th}}$ **roots modulo** n. It is known that [28]

$$\sum_{n\leq N} g(n) \sim \tilde{A}\frac{N^2}{\ln N}$$

as $N \to \infty$, where

$$\tilde{A} = \frac{5}{8} \prod_p \left(1 - \frac{1}{p(p-1)}\right) = 0.233722383512...$$

(five-eighths of *Artin's constant* [7]). A corresponding result for $\sum_{n \le N} h(n)$ evidently remains open. The issue of the asymptotics of $\sum_{n \le N} g(n)$ and of $\sum_{n \le N} h(n)$ bears some resemblance to the periodicity problems discussed earlier.

4. Acknowledgements

I thank Gérald Tenenbaum for suggesting the relation to $\sum_{n \le N} 1/\kappa(n)$ and for informing me about [15, 19]. I also thank Pascal Sebah, my coauthor in [1]. After this paper was completed, I learned about [29], which uses sophisticated tools to examine mean periods over all $x \in \mathbb{Z}_n^*$ (a different and more successful approach than mine).

References

[1] S. Finch and P. Sebah, Squares and cubes modulo n, http://arxiv.org/abs/math.NT/0604465.

[2] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, 1976, pp. 55–62, 229; MR0434929 (55 #7892).

[3] N. J. A. Sloane, On-Line Encyclopedia of Integer Sequences, A034444, A055653, A117656, A117657.

[4] A. Selberg, Note on a paper by L. G. Sathe, *J. Indian Math. Soc.* 18 (1954) 83-87; MR0067143 (16,676a).

[5] H. Delange, Sur des formules de Atle Selberg, *Acta Arith.* 19 (1971) 105-146 (errata insert); MR0289432 (44 #6623).

[6] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge Univ. Press, 1995, pp. 180–197, 257; MR1342300 (97e:11005b).

[7] S. R. Finch, Artin's constant, *Mathematical Constants*, Cambridge Univ. Press, 2003, pp. 104–109; MR2003519 (2004i:00001).

[8] V. S. Joshi, Order-free integers (mod m), *Number Theory*, Proc. 1981 Mysore conf., ed. K. Alladi, Lect. Notes in Math. 938, Springer-Verlag, 1982, pp. 93–100; MR0665441 (83k:10085).

[9] J. K. Patel, Order free integers (mod m), *Indian J. Pure Appl. Math.* 24 (1993) 503–508; MR1241102 (94i:11076).

[10] J. K. Patel, Erratum to: "Order free integers (mod m)", *Indian J. Pure Appl. Math.* 25 (1994) 457–458; MR1272816 (95c:11115).

[11] Sloane, op. cit., A117658, A117659, A117660.

[12] A. M. Odlyzko, Asymptotic enumeration methods, *Handbook of Combinatorics*, v. I, ed. R. Graham, M. Grötschel, and L. Lovász, MIT Press, 1995, pp. 1063-1229; MR1373678 (97b:05012).

[13] E. Bach and J. Shallit, *Algorithmic Number Theory*, v. 1, *Efficient Algorithms*, MIT Press, 1996, pp. 27–29; MR1406794 (97e:11157).

[14] Sloane, op. cit., A003557, A007947.

[15] N. G. de Bruijn, On the number of integers $\leq x$ whose prime factors divide n, *Illinois J. Math.* 6 (1962) 137–141; MR0147461 (26 #4977).

[16] N. G. de Bruijn and J. H. van Lint, On the number of integers $\leq x$ whose prime factors divide n, *Acta Arith.* 8 (1963) 349–356; MR0159779 (28 #2995).

[17] N. G. de Bruijn and J. H. van Lint, On the asymptotic behaviour of some Dirichlet series with a complicated singularity, *Nieuw Arch. Wisk.* 11 (1963) 68–75; MR0158878 (28 #2100).

[18] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge Univ. Press, 1995, pp. 54, 116–117, 126; MR1342300 (97e:11005b).

[19] W. Schwarz, Einige Anwendungen Tauberscher Sätze in der Zahlentheorie. B, *J. Reine Angew. Math.* 219 (1965) 157–179; MR0184917 (32 #2388).

[20] Sloane, op. cit., A002322, A046144, A010554, A033948, A033949, A111725.

[21] T. Nagell, *Introduction to Number Theory*, 2nd ed., Chelsea, 1981, pp. 102–111, 300; MR0174513 (30 #4714).

[22] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, 1990, pp. 41–45; MR1070716 (92e:11001) .

[23] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, 1976, pp. 204–213; MR0434929 (55 #7892).

[24] P. Erdös, C. Pomerance and E. Schmutz, Carmichael's lambda function, *Acta Arith.* 58 (1991) 363–385; MR1121092 (92g:11093).

[25] S. Li, On the number of elements with maximal order in the multiplicative group modulo n, *Acta Arith.* 86 (1998) 113–132; MR1654458 (99k:11144).

[26] P. J. Cameron and D. A. Preece, Notes on primitive lambda roots, available online at http://www.maths.qmul.ac.uk/∼pjc/csg.html.

[27] T. W. Müller and J.-C. Schlage-Puchta, On the number of primitive λ-roots, *Acta Arith.* 115 (2004) 217–223; MR2100500 (2005g:11189).

[28] S. S. Pillai, On the sum function connected with primitive roots, *Proc. Indian Acad. Sci. Sect. A.* 13 (1941) 526–529; MR0004834 (3,68c).

[29] F. Luca and I. E. Shparlinski, Average multiplicative orders of elements modulo n, *Acta Arith.* 109 (2003) 387–411; MR2009051 (2004i:11113).

Steven Finch
Steven.Finch@inria.fr