TSUKUBA J. MATH.
Vol. 30 No. 2 (2006), 439–449

ON THE NUMBER OF POLYNOMIAL MAPS INTO $\mathbf{Z}_n$

By

Florian LUCA and Igor E. SHPARLINSKI

Abstract. In this paper, we study maximal, minimal, normal and average order of the function

$$f(n) = \prod_{k=0}^{n} n/\gcd(n, k!)$$

which is the cardinality of the set of polynomial maps from $\mathbf{Z}$ into $\mathbf{Z}_n$.

1 Introduction

For a positive integer n we let

$$f(n) = \prod_{k=0}^{n} \frac{n}{\gcd(n, k!)}.$$

It is known since the work of A. J. Kempner [9] that $f(n)$ gives the cardinality of the set of polynomial maps from $\mathbf{Z}$ into $\mathbf{Z}_n$. In a completely explicit form it is also given by M. Bhargava [1].

Here, we study some questions about the maximal, minimal, normal and average order of this function.

In fact, the question on the large order is trivial as clearly the inequality

$$f(n) \le n^n$$

holds for all positive integers n with equality if and only if n is prime. Thus, we concentrate on the remaining questions.

We remark that in what follows no attempt has been made to get sharp bounds on the error terms. Throughout the paper, the implied constants in symbols 'O', '$\ll$' and '$\gg$', may occasionally, where obvious, depend on the integer

Received August 17, 2005.

parameter ν, and are absolute otherwise (we recall that $U = O(V)$, $U \ll V$ and $V \gg U$ are both equivalent to the inequality $|U| \le cV$ with some constant $c > 0$).

We use the letters p and q, with subscripts or without, to denote prime numbers, and k, m and n to denote nonnegative integers.

If n is positive, we use $P(n)$, $\omega(n)$ and $\tau(n)$ for the largest prime factor of n, the number of distinct prime divisors of n and the total number of divisors of n, respectively (we also put $P(1) = 1$).

2 Minimal Order

THEOREM 1. *The inequality*

$$f(n) \ge \exp\left((1 + o(1))\frac{(\log n)^2}{2 \log\log n}\right)$$

holds as $n \to \infty$.

PROOF. We let k_n be such that $k_n! \le n$ and $(k_n + 1)! > n$. Since the inequality $\gcd(n, k!) \le \min\{n, k!\}$ holds for all $k = 0, \ldots,$ it follows that $\gcd(n, k!) \le k!$ for $k \le k_n$ and $\gcd(n, k!) \le n$ for all $k \ge k_n + 1$. Note that all equalities are achieved when n itself is a factorial. Thus,

$$f(n) \ge \prod_{k=0}^{k_n} \frac{n}{k!} = \exp\left((k_n + 1)\log n - \sum_{k=0}^{k_n} \log(k!)\right). \tag{1}$$

From the Stirling formula, we derive $\log k! = k \log k + O(k)$. Thus,

$$\sum_{k=0}^{k_n} \log(k!) = \sum_{k=0}^{k_n} k \log k + O(k_n^2) = \frac{1}{2} k_n^2 \log k_n + O(k_n^2).$$

Furthermore, since $k_n! \le n < (k_n + 1)!$, we get that

$$k_n \log k_n + O(k_n) = \log n,$$

which shows that

$$k_n = (1 + o(1))\frac{\log n}{\log\log n}.$$

Hence,

$$(k_n+1)\log n-\sum_{k=0}^{k_n}\log(k!)=k_n\log n-\frac{1}{2}k_n^2\log k_n+O\left(\left(\frac{\log n}{\log\log n}\right)^2\right)$$

$$=\frac{(\log n)^2}{2\log\log n}(1+o(1)),$$

which together with the estimate (1) completes the proof of the lower bound.

We also remark that if $n=m!$ then $k_n=m$ and the inequality (1) becomes an equality. □

3 Normal Order

It is clear that $f(n)\geq f(d)$ holds for all divisors d of n. In particular,

$$f(n)\geq f(P(n))=P(n)^{P(n)}. \tag{2}$$

We now show that for almost all n this bound is tight.

THEOREM 2. *For all but* $O(x(\log\log x)^2/\log x)$ *positive integers* $n\leq x$, *we have*

$$\log f(n)=\left(1+O\left(\frac{(\log\log x)^2}{\log x}\right)\right)P(n)\log P(n).$$

PROOF. We assume that x is a large positive real number and define

$$w=(\log x)^4,\quad y=\exp((\log\log x)^3),\quad z=\exp\left(\frac{\log x\log\log\log x}{3\log\log x}\right). \tag{3}$$

We now put

$$\mathscr{E}_1(x)=\{n\leq x: P(n)\leq z\}.$$

By known results on the distribution of smooth numbers (see, for example, Section III.5.4 in [11]), we have that

$$\#\mathscr{E}_1(x)=x\exp(-u\log u),$$

where

$$u=\frac{\log x}{\log z}=\frac{3\log\log x}{\log\log\log x}.$$

Hence,

$$\#\mathcal{E}_1(x) = x \exp(-(3+o(1))\log\log x) \ll \frac{x}{(\log x)^2}.$$

We let $\mathcal{E}_2(x)$ be the set of all positive integers $n \le x$ such that $a|n$ for some *squarefull* $a > w$. Recall that a number a is called squarefull if $p^2|a$ whenever p is a prime factor of a. It is known that if we write

$$\mathcal{V}(x) = \{a \le x : a \text{ squarefull}\},$$

then

$$\#\mathcal{V}(x) = c_0 x^{1/2} + O(x^{1/3}), \quad \text{where } c_0 = \frac{\zeta(3/2)}{\zeta(3)} \approx 2.1732 \tag{4}$$

(see Theorem 14.1 in [6]). Fix a squarefull $a > w$. The number of positive integers $n \le x$ which are multiples of a is $\le x/a$. Thus, using the estimate (4) and partial summation, we immediately get that

$$\mathcal{E}_2(x) \le \sum_{\substack{a>w \\ a\in\mathcal{V}(x)}} \frac{x}{a} \ll \frac{x}{w^{1/2}} \ll \frac{x}{(\log x)^2}.$$

We now let

$$\mathcal{E}_3(x) = \{n \le x : \omega(n) > 10 \log\log x\}.$$

If $n \in \mathcal{E}_3(x)$, then

$$\tau(n) \ge 2^{\omega(n)} > (\log x)^{10\log 2} > (\log x)^3.$$

Therefore,

$$\#\mathcal{E}_3(x) \le \frac{1}{(\log x)^3} \sum_{n\le x} \tau(n) \ll \frac{x}{(\log x)^2}$$

(see Theorem 2 of Chapter I.3.1 in [11]).

We now define $Q(n) = P(n/P(n))$ and let

$$\mathcal{E}_4(x) = \{n \le x : \min\{Q(n), z\} < P(n) < Q(n) \log x\}.$$

For each fixed $Q(n) = q$ and $P(n) = p$ the number of such $n \le x$ is at most $\lfloor x/pq \rfloor \le x/pq$. We also remark for $n \in \mathcal{E}_4(x)$ we have $Q(n) > z/\log x > \sqrt{z}$ provided that x is large enough. Thus, by the Mertens formula (see, for example, [10] for a very sharp error term), we derive

$$\#\mathscr{E}_4(x) \le x \sum_{z^{1/2}<q} \sum_{q<p<q\log x} \frac{1}{pq} = x \sum_{z^{1/2}<q} \frac{1}{q} \sum_{q<p<q\log x} \frac{1}{p}$$

$$= x \sum_{z^{1/2}<q} \frac{1}{q} \left(\log\log(q \log x) - \log\log q + O\left(\frac{1}{\log q}\right)\right)$$

$$= x \sum_{z^{1/2}<q} \frac{1}{q} \left(\log\left(1 + \frac{\log\log x}{\log q}\right) + O\left(\frac{1}{\log q}\right)\right)$$

$$\ll x \log\log x \sum_{z^{1/2}<q} \frac{1}{q \log q} \ll \frac{x \log\log x}{\log(z^{1/2})} \ll \frac{x(\log\log x)^2}{\log x}.$$

Thus, for the set $\mathscr{E}(x) = \bigcup_{i=1}^{5} \mathscr{E}_i(x)$, we have

$$\#\mathscr{E}(x) \ll \frac{x(\log\log x)^2}{\log x}. \tag{5}$$

Now let $\mathscr{N}(x)$ be the set of all positive integers $n \le x$ which are not in $\mathscr{E}(x)$. Fix $n \in \mathscr{N}(x)$ and denote $d_k = \gcd(n, k!)$, $k = 0, 1, \ldots$. It is clear that $d_k | d_{k+1}$ for all $k \ge 0$.

We have

$$\prod_{k \le y} d_k \le y!^y < y^{y^2}.$$

Thus,

$$\log f(n) = n \log n - \sum_{y<k\le n} \log d_k + O(y^2 \log y). \tag{6}$$

Let $k_0 = \lfloor y \rfloor + 1$. If $\rho(n)$ is the largest powerful divisor of n, then $\rho(n) \mid d_{k_0}$. Indeed, let p be any prime factor of $\rho(n)$. Then $p < w$, and the exponent at which p appears in $\rho(n)$ is at most $(\log w)/(\log 2)$, because $n \notin \mathscr{E}_2(x)$. Indeed, this follows since the exponent at which p appears in $k_0!$ is at least

$$\lfloor k_0/p \rfloor \ge \lfloor y/w \rfloor > \frac{y}{2w} > \frac{\log w}{\log 2} > \rho(n),$$

provided that x is large enough. In particular, $m = n/d_{k_0}$ is squarefree. Let $k_0 < p_1 < \cdots < p_s = P(n)$ be all the prime factors of m. Since $P(n) > Q(n) \ge z/\log z > y$, we have $P(n)Q(n) \mid m$. It is then clear that

$$d_k = \begin{cases} d_{k_0}, & \text{if } k_0 \le k \le p_1 - 1, \\ d_{k_0} p_1 \cdots p_i, & \text{if } p_i \le k \le p_{i+1} - 1,\ i = 1, \ldots, s-1, \\ n, & \text{if } k \ge p_s. \end{cases}$$

Hence,

$$\begin{aligned} \sum_{y < k \le n} \log d_k &= (n - P(n)) \log n \\ &\quad + \sum_{i=1}^{s-1} (p_{i+1} - p_i) \log\left(\frac{n}{p_{i+1} \cdots p_s}\right) + (p_1 - k_0) \log d_{k_0} \\ &= (n - P(n)) \log n + P(n) \log\left(\frac{n}{P(n)}\right) - p_1 \log\left(\frac{n}{p_2 \cdots p_s}\right) \\ &\quad + \sum_{i=2}^{s-1} p_i \log p_{i+1} + (p_1 - k_0) \log d_{k_0} \\ &= n \log n - P(n) \log P(n) + O(\omega(n) Q(n) \log n)). \end{aligned}$$

In particular, from (6), we infer that

$$\log f(n) = P(n) \log P(n) + O(\omega(n) Q(n) \log n + y^2 \log y). \tag{7}$$

Since $n \notin \mathscr{E}_1(x) \cup \mathscr{E}_3(x) \cup \mathscr{E}_4(x)$, we have

$$\omega(n) \ll \log\log x, \quad \log P(n) \ge \log z \gg \frac{\log x}{\log\log x}, \quad P(n) \ge Q(n) \log x$$

for x large enough, which implies that

$$\omega(n) Q(n) \log n \ll P(n) \log P(n) \left(\frac{(\log\log x)^2}{\log x}\right).$$

Also

$$y^2 \log y \ll z \log z \left(\frac{(\log\log x)^2}{\log x}\right) \ll P(n) \log P(n) \left(\frac{(\log\log x)^2}{\log x}\right).$$

We now derive from estimate (7) that

$$\log f(n) = \left(1 + O\left(\frac{(\log\log x)^2}{\log x}\right)\right) P(n) \log P(n)$$

for $n \in \mathscr{N}(x)$, which together with (5) finishes the proof. □

4 Average Order

We start by obtaining an asymptotic formula for the sum

$$\sigma_\nu(x) = \sum_{n \le x} (P(n) \log P(n))^\nu.$$

Similar sums have been studied by J.-M. De Koninck, A. Ivić, C. Pomerance and other researchers [2, 3, 5, 7, 8]. In particular, an easy modification of the proof of Theorem 3 in [7] gives an asymptotic formula for $\sigma_\nu(x)$.

Let $\zeta(s)$ denote the Riemann-zeta function.

LEMMA 3. *Let $\nu > 0$. We then have the following asymptotic formula:*

$$\sigma_\nu(x) = \left(\frac{\zeta(\nu+1)}{\nu+1} + O\left(\frac{\log\log x}{\log x}\right)\right) x^{\nu+1} (\log x)^{\nu-1}.$$

PROOF. Let $r = \lfloor (\log x)^2 \rfloor$. The contribution to $\sigma_\nu(x)$ coming from $n \le x$ with $P(n) \le x/r$ is obviously at most $x^{1+\nu}(\log x)^{-\nu}$. We now have

$$\sum_{\substack{n \le x \\ P(n) > x/r}} (P(n) \log P(n))^\nu = \left(1 + O\left(\frac{\log\log x}{\log x}\right)\right) (\log x)^\nu \sum_{\substack{n \le x \\ P(n) > x/r}} P(n)^\nu$$

$$= \left(1 + O\left(\frac{\log\log x}{\log x}\right)\right) (\log x)^\nu \sum_{n \le x} P(n)^\nu.$$

For the last sum, the asymptotic formula

$$\sum_{n \le x} P(n)^\nu = \left(\frac{\zeta(\nu+1)}{\nu+1} + O\left(\frac{1}{\log x}\right)\right) \frac{x^{\nu+1}}{\log x}$$

is given in the proof of Theorem 3 in [7], and the result now follows. □

It is easy to see that the method of proof of Theorem 3 in [7] can be used to derive an asymptotic expansion for $\sigma_\nu(x)$.

For a positive constant ν we define

$$F_\nu(x) = \sum_{n \le x} (\log f(n))^\nu.$$

THEOREM 4. *Let $\nu > 0$. Then we have the following estimate:*

$$F_\nu(x) = \left(\frac{\zeta(\nu+1)}{\nu+1} + O\left(\frac{(\log\log x)^2}{\log x}\right)\right) x^{\nu+1} (\log x)^{\nu-1}.$$

Proof. By Lemma 3, it is enough to prove that

$$F_\nu(x) = \left(1 + O\left(\frac{(\log\log x)^2}{\log x}\right)\right)\sigma_\nu(x).$$

We consider the same sets $\mathscr{E}_1(x)$, $\mathscr{E}_2(x)$, $\mathscr{E}_3(x)$, $\mathscr{E}_4(x)$ and $\mathscr{N}(x)$ as in the proof of Theorem 2. Since $n \log n \geq \log f(n) \geq P(n) \log P(n)$, the contribution to both $F_\nu(x)$ and $\sigma_\nu(x)$ from $n \in \bigcup_{i=1}^4 \mathscr{E}_i(x)$ is at most

$$\sum_{n \in \bigcup_{i=1}^4 \mathscr{E}_i(x)} (P(n) \log P(n))^\nu \leq (x \log x)^\nu \sum_{i=1}^5 \#\mathscr{E}_i(x) \ll x^{\nu+1} (\log x)^{\nu-2}.$$

We now consider the function $S(n) = \min\{k : n \mid k!\}$, which is usually referred to as the *Smarandache function*, although it has appeared explicitly long before, for example, in the paper of A. J. Kempner [9] which dates back to 1921. Clearly,

$$f(n) \leq n^{S(n)}.$$

We put $\mathscr{F}(x) = \{n : S(n) > P(n)\}$. K. Ford (see [4]), has shown that

$$\#\mathscr{F}(x) \leq x \exp(-(\sqrt{2} + o(1))\sqrt{\log x \log\log x}) \ll \frac{x}{(\log x)^2}.$$

Since for $n \in \mathscr{E}_4(x)$ we have $Q(n) > z/\log x > z^{1/2}$, (and therefore we also have $P(n) \leq n/Q(n) \leq x/z^{1/2}$), the contribution to $F_\nu(x)$ and to $\sigma_\nu(x)$ coming from $n \in \mathscr{E}_4(x)$ is at most

$$\sum_{n \in \mathscr{E}_4(x)} (\log f(n))^\nu \ll \#\mathscr{F}(x)(n \log n)^\nu + \sum_{n \in \mathscr{E}_3(x) \setminus \mathscr{F}(x)} (P(n) \log n)^\nu$$

$$\ll x^{\nu+1} (\log x)^\nu z^{-\nu/2} + x(xz^{-1/2} \log x)^\nu \ll x^{\nu+1} (\log x)^{\nu-2}.$$

Finally, by Theorem 2, we obtain

$$\begin{aligned} F_\nu(x) &= \sum_{n \in \mathscr{N}(x)} (\log f(n))^\nu + O(x^{\nu+1} (\log x)^{\nu-2}) \\ &= \left(1 + O\left(\frac{(\log\log x)^2}{\log x}\right)\right) \sum_{n \in \mathscr{N}(x)} (P(n) \log P(n))^\nu + O(x^{\nu+1} (\log x)^{\nu-2}) \\ &= \left(1 + O\left(\frac{(\log\log x)^2}{\log x}\right)\right)\sigma_\nu(x) + O(x^{\nu+1} (\log x)^{\nu-2}) \\ &= \left(1 + O\left(\frac{(\log\log x)^2}{\log x}\right)\right)\sigma_\nu(x), \end{aligned}$$

which concludes the proof. □

5 Distribution of Values

THEOREM 5. *The function $f(n)$ is bijective.*

PROOF. For a prime p, we use $\operatorname{ord}_p s$ to denote the p-adic order of the integer s. We also denote by $k_p(s)$ the largest k such that $\operatorname{ord}_p k! \le \operatorname{ord}_p s$.

If $m \neq n$, then there is a prime p such that $\operatorname{ord}_p m \neq \operatorname{ord}_p n$. Assume that

$$\operatorname{ord}_p m < \operatorname{ord}_p n.$$

Then it is clear that $k_p(m) \le k_p(n)$. Therefore

$$\operatorname{ord}_p f(m) = \sum_{k=1}^{k_p(m)} (\operatorname{ord}_p m - \operatorname{ord}_p k!) < \sum_{k=1}^{k_p(m)} (\operatorname{ord}_p n - \operatorname{ord}_p k!)$$

$$\le \sum_{k=1}^{k_p(n)} (\operatorname{ord}_p n - \operatorname{ord}_p k!) = \operatorname{ord}_p f(m),$$

which concludes the proof. □

Let $\mathscr{V}(x) = \{f(n) \le x\}$ be set of values of $f(n)$ in the interval $[1, x]$.

THEOREM 6. *The following bound holds*:

$$\exp\left(\frac{\sqrt{\log x}}{\log\log x}\right) \ll \#\mathscr{V}(x) \ll \exp\left(\frac{2\log x \log\log\log x}{\log\log x}\right).$$

PROOF. Let us put

$$y = \frac{3\log x}{2\log\log x} \quad \text{and} \quad z = \frac{\log x}{\log\log x}.$$

Clearly the prime divisors of n and $f(n)$ coincide, in particular $P(f(n)) = P(n)$. Now from (2) we conclude that $P(f(n)) \le y$, provided that x is large enough. Using the bound

$$\log \Psi(x, y) = Z\left(1 + O\left(\frac{1}{\log y} + \frac{1}{\log\log x}\right)\right),$$

where

$$Z = \frac{\log x}{\log y} \log\left(1 + \frac{y}{\log x}\right) + \frac{y}{\log y} \log\left(1 + \frac{\log x}{y}\right)$$

(see Theorem 2 of Chapter III.5.1 in [11]) on the number $\Psi(x, y)$ of integers $m \le x$ with $P(m) \le y$, and remarking that

$$Z = (1 + o(1)) \frac{3 \log x \log\log\log x}{2 \log\log x},$$

we obtain the upper bound.

On the other hand, note that if n is squarefree then $f(n) \le n^{P(n)}$ (because $n | k!$ for all $k \ge P(n)$). Furthermore, since in this case

$$n \left| \prod_{p \le P(n)} p = \exp((1 + o(1))P(n)), \right.$$

we also have that $\log n \le (1 + o(1))P(n)$. Hence, $\log f(n) \le (1 + o(1))P(n)^2$ as $n \to \infty$ through squarefree values. Thus, if we let x be large and

$$w = \frac{9}{10} \sqrt{\log x},$$

then $f(n) \le x$ for all squarefree positive integers n with $P(n) < w$, provided that x is large enough. Certainly, the number of such values of n is

$$2^{\pi(w)} = \exp\left((1 + o(1)) \frac{9 \log 2}{5} \frac{\sqrt{\log x}}{\log\log x} \right),$$

and the result now follows from Theorem 5 together with the inequality $(9 \log 2)/5 > 1$. □

References

[1] M. Bhargava, 'The factorial function and generalizations', Amer. Math. Monthly, **107** (2000), 783–799.

[2] J.-M. De Koninck and A. Ivić, 'The average prime divisor of an integer in short intervals', Arch. Math., **52** (1989), 440–448.

[3] J.-M. De Koninck and A. Ivić, 'On the average prime factor of an integer and some related problems', Ricerche Mat., **39** (1990), 131–140.

[4] K. Ford, 'The normal behavior of the Smarandache function', Smarandache Notions J., **10** (1999), 81–86.

[5] A. Ivić, 'On sums involving reciprocals of the largest prime factor of an integer, II', Acta Arith., **71** (1995), 229–251.

[6] A. Ivić, The Riemann Zeta-Function, Theory and Applications, Dover Publications, Mineola, New York, 2003.

[7] A. Ivić, 'On a problem of Erdős involving the largest prime factor of n', Monat. Math., **145** (2005), 35–46.

[8] A. Ivić, and C. Pomerance, 'Estimates for certain sums involving the largest prime factor of an integer', Topics in Analytic Number Theory, Colloquia Math. Soc. J. Bolyai, **34**, North-Holland, 1981, 769–789.

[9] A. J. Kempner, 'Polynomials and their residue systems', Trans. Amer. Math. Soc., **22** (1921), 240–266; (cont.) 267–288.

[10] A. I. Vinogradov, 'On the remainder in Mertens's formula', Dokl. Akad. Nauk SSSR, **148** (1963), 262–263 (in Russian).

[11] G. Tenenbaum, Introduction to analytic and probabilistic number theory, Cambridge U. Press, 1995.

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán, México
fluca@matmor.unam.mx

Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au