Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Oleksiy KLURMAN et Marc MUNSCH

Distribution of factorials modulo *p*

Tome 29, nº 1 (2017), p. 169-177.

<http://jtnb.cedram.org/item?id=JTNB_2017__29_1_169_0>

Journal de Théorie des Nombres
de Bordeaux **29** (2017), 169–177

Distribution of factorials modulo p

par Oleksiy KLURMAN et Marc MUNSCH

Résumé. On s'intéresse à l'estimation du nombre de valeurs prises par la suite $n! \pmod p$. Principalement, on obtient en moyenne sur les nombres premiers $p \leq x$, une minoration du nombre de classes modulo p évitées par la suite $n! \pmod p$.

Abstract. We estimate the average number of residue classes missed by the sequence $n! \pmod p$ for $p \leq x$.

1. Introduction

Following [7], for each odd prime p let $V(H,N)$ denote the number of distinct residue classes modulo p that are taken by the sequence $\{n!, n = 2, 3 \dots, p-1\}$, $H \leq n \leq H+N$. Very little seems to be known about the behaviour of $V(H,N)$. P. Erdős conjectured that $2!, 3! \dots, (p-1)!$ cannot be all distinct modulo p, in other words $V(0,p-1) \neq p-2$. Although the conjecture is open, B. Rokowska and A. Schinzel [16] proved that this condition implies some restrictions on the values of p. This allows Trudgian to verify that the conjecture holds true for $p < 10^9$ (see [18]). More generally, the following asymptotic is conjectured in [9]:

$$V(0,p-1) \sim \left(1 - \frac{1}{e}\right) p.$$

In [4], C. Cobeli, M. Vâjâitu and A. Zaharescu provide a strong support towards this conjecture (see also [2]). They proved that for a random permutation σ of the set $\{1, \cdots, p-1\}$, the products

$$\left\{ \prod_{i=1}^{n} \sigma(i), n = 1, \cdots, p-1 \right\}$$

cover the expected number of residue classes. This implies in particular that in case the sequence $\{n!, n = 2, 3 \dots, p-1\}$ did not satisfy Guy's observation then it would not, in some sense, be a "standard" sequence amongst the set of all sequences of length p.

In a series of papers, [6], [7] and [8], M. Garaev, F. Luca and I. Shparlinski initiated an extensive study of the distribution properties of $n! (\bmod\ p)$. In

Manuscrit reçu le 27 mars 2015, révisé le 10 avril 2016, accepté le 13 avril 2016.
Mathematics Subject Classification. 11B50, 11B83, 11R09, 11R45.
Mots-clefs. Distribution of sequences mod p, polynomials, density results.

particular, in [7] the authors remark that the only known lower bound for $V(H,N)$ is a trivial one, namely

$$V(H,N) \geq \sqrt{N-1}.$$

Indeed, this immediately follows from the fact that the remainders $\frac{n!}{(n-1)!} = n$ are all distinct for $1 \leq n \leq p-1$.

Motivated by this question, V. Lev considered a similar problem in every finite abelian group G. He showed [14, Theorem 2] that there is a permutation $(g_1, \cdots, g_{|G|})$ of the elements of G such that the number of distinct sums of the form

$$g_1 + \cdots + g_j \, (1 \leq j \leq |G|)$$

is $O(\sqrt{|G|})$ and noticed that this is the smallest size possible. By fixing a primitive root g modulo p and passing to indices with respect to g, the question about the distribution of factorials reduces to considering the cyclic group of order $p-1$ and the permutation given by the indices. V. Lev observes that the conclusion one can draw concerning the sequence $n!$ is of a negative sort: in order to improve the lower bound on $V(H,N)$, combinatorics is not sufficient and one has to exploit the special properties of this particular sequence.

In the preprint version of the present paper [11], we gave an elementary way to obtain nontrivial lower bound on $V(H,N)$ for all $N \gg p^{\frac{1}{4}+\varepsilon}$ proving

Theorem. *The set of* $n! \,(\mathrm{mod}\, p)$, $H \leq n \leq H+N$ *contains at least* $\sqrt{\frac{3}{2}N}$ *distinct values for all* $N \gg p^{\frac{1}{4}+\varepsilon}$.

This was subsequently improved by J. Hernandez and M. Garaev in [5]. In the other direction, it was proved in [1] that there exists infinitely many primes p such that $n!(\mathrm{mod}\ p)$ omits at least

$$p - V(0,p-1) \gg \frac{\log\log p}{\log\log\log p} \tag{1.1}$$

residue classes. Applying the method of [1] and replacing the unconditional bound for the least prime ideal by the one derived in [13] using the Generalized Riemann hypothesis (GRH) yields infinitely many primes such that

$$p - V(0,p-1) \gg \frac{\log p}{\log\log p}\cdot \tag{1.2}$$

We remark that in [1], due to the use of the bound on the least prime ideal from [12], one gets an extremely sparse set of primes satisfying (1.1) and (1.2). We are going to prove an average analog of this result in the following form.

Theorem. *We have*

$$\frac{1}{\pi(x)}\sum_{p\le x}(p-V(0,p-1))\gg\frac{\log\log x}{\log\log\log x}\cdot$$

Under GRH, we have the bound

$$\frac{1}{\pi(x)}\sum_{p\le x}(p-V(0,p-1))\gg\frac{x^{\frac{1}{4}}}{\log x}\cdot$$

Thus, under GRH, our result immediately implies the existence of infinitely many primes with

$$p-V(0,p-1)\gg\frac{p^{\frac{1}{4}}}{\log p}\cdot$$

2. Upper bound for $V(0,p-1)$ on average

As was mentioned in the introduction, it was proved in [1] that there exists infinitely many primes p such that $n!\,(\bmod p)$ omits at least

$$p-V(0,p-1)\gg\frac{\log\log p}{\log\log\log p}\tag{2.1}$$

residue classes. In this section, we show that the number of "missing" residue classes tends to infinity on average.

We fix a few notations. Let $L/\mathbb{Q}$ be a finite extension of degree n_L. For any ideal $\mathfrak{I}$ of the ring of integers $\mathcal{O}_L$, we denote the norm of an ideal by $N_{L/\mathbb{Q}}(\mathfrak{I})$ and write $N(\mathfrak{I})$. We also denote by $f\,(\mathfrak{p}/p)$ the inertial degree $|\,[\mathcal{O}_L/\mathfrak{p}:\mathbb{F}_p]\,|$ of the ideal $\mathfrak{p}$ above the rational prime p. The function $\pi_L(x)$ will count the number of prime ideals $\mathfrak{p}$ such that $N(\mathfrak{p})\le x$. Finally, denote by d_L the absolute discriminant of L.

Theorem 2.1. *We have*

$$\frac{1}{\pi(x)}\sum_{p\le x}(p-V(0,p-1))\gg\frac{\log\log x}{\log\log\log x}\cdot$$

Proof. Let N be a parameter which will be determined later. For $n\ge 1$ we consider the family of polynomials

$$f_n(t)=t(t+1)\dots(t+n-1)-1.$$

It is well-known (see [15, 9, part *viii*, chapter 2, section 3, Pb 121] that $f_n(t)$ is irreducible over $\mathbb{Q}$ for all $n\ge 1$. Let $\rho_n(p)$ denote the number of roots of $f_n(t)$ modulo p. We observe that $f_n(t_0)\equiv 0\,(\bmod p)$ implies

$$(t_0+n-1)!=(t_0-1)!\,(\bmod p).$$

Therefore, each distinct root of $f_n(t)$ modulo p increases the number of "missing" values by 1. We thus want to produce a lot of roots of f_n for many values of n.

Let $K_n = \mathbb{Q}(\alpha)$ be the extension of $\mathbb{Q}$ obtained by adjoining a root of f_n. By C_k we denote the subset of all non ramified primes in K_n such that f_n has exactly k roots modulo p. Observe, that

$$\sum_{p\leq x}\rho_n(p) \geq \sum_{k=1}^{n}\sum_{\substack{p\leq x\\ p\in C_k}} k. \tag{2.2}$$

By Dedekind's theorem, up to finitely many exceptions, the primes p such that f_n has a root modulo p correspond to the primes p such that there exists a prime ideal $\mathfrak{p}$ in $\mathcal{O}_{K_n}$ above p with inertial degree $f\left(\mathfrak{p}/p\right) = 1$.

Instead of working in the splitting field of f_n and using Chebotarev's theorem as in [1], we will directly count prime ideals in K_n using prime ideal theorem. By the standard argument, the prime ideals of degree > 1 will give negligible contribution. More precisely, we remark that counting prime ideals in K_n of degree 1 is equivalent to counting the rational primes p with weight k when f_n has k roots modulo p. Thus, we have

$$\sum_{k=1}^{n}\sum_{\substack{p\leq x\\ p\in C_k}} k = \sum_{\substack{N(\mathfrak{p})\leq x\\ f(\mathfrak{p}/p)=1}} 1. \tag{2.3}$$

By the effective prime ideal theorem (see [10, Theorem 5.33])[1], there exists an absolute constant $c > 0$ such that for all $n \geq 1$

$$\sum_{\substack{N(\mathfrak{p})\leq x\\ f(\mathfrak{p}/p)=1}} 1 = \pi(x) + O\left(Li(x^{\beta_n}) + \frac{x}{\log x}\exp\left(-c\sqrt{\frac{\log x}{n^2}}\right)\right) \tag{2.4}$$

where β_n is the potential positive real zero of the Dedekind zeta function ζ_{K_n} and

$$0 < 1 - \beta_n \ll \frac{1}{\log d_{K_n}}\cdot$$

We now restrict ourselves to the family of polynomials $\{f_{2n+1}, 1 \leq n \leq N\}$. Recall that by the result of Stark [17, Lemma 8], we can control potential Siegel zeroes provided that the original extension does not contain any quadratic sub-extension. We do so here since $K_{2n+1} = \mathbb{Q}(\alpha)$ is of an odd degree. Latter yields the bound

$$\beta_{2n+1} \leq 1 - \frac{1}{4(2n+1)!\log|d_{K_{2n+1}}|}\cdot \tag{2.5}$$

[1] We could equally apply effective version of Chebotarev theorem [13] for the trivial extension K_n/K_n.

Using (2.2) together with (2.4), we derive

$$\begin{aligned} \frac{1}{\pi(x)}\sum_{p\leq x}(p-V(0,p-1)) &\geq \sum_{n=1}^{N}\frac{1}{\pi(x)}\sum_{p\leq x}\rho_{2n+1}(p) \\ &\geq \sum_{n=1}^{N}\frac{1}{\pi(x)}\sum_{k=1}^{2n+1}k\sum_{\substack{p\leq x\\ p\in C_k}}1 \qquad (2.6)\\ &\geq N+ET, \qquad (2.7)\end{aligned}$$

where

$$ET=O\left(\frac{1}{\pi(x)}\left\{\sum_{n=1}^{N}Li(x^{\beta_{2n+1}})+\frac{x}{\log x}\exp\left(-c\sqrt{\frac{\log x}{(2n+1)^2}}\right)\right\}\right)\cdot$$

Hence, we have to choose parameter N such that

$$N\gg\sum_{n=1}^{N}\frac{1}{\pi(x)}\left\{Li(x^{\beta_{2n+1}})+\frac{x}{\log x}\exp\left(-c\sqrt{\frac{\log x}{(2n+1)^2}}\right)\right\}. \tag{2.8}$$

The sum of the exponential terms in (2.8) satisfies this as long as

$$N\ll\log^{1/2}x.$$

Since K_{2n+1} is generated by the single root of f_{2n+1}, we can bound its discriminant by the discriminant of the polynomial f_{2n+1}. Hence, denoting by α_i the roots of f_{2n+1} we derive

$$d_{K_{2n+1}}\leq\prod_{\substack{i,j\\ i<j}}^{2n+1}|\alpha_i-\alpha_j|^2\ll n^{10n^2}, \tag{2.9}$$

where we used the bound $|\alpha_i-\alpha_j|\ll n$ which is proved in [1, Lemma 2].

To bound the contribution coming from the potential Siegel zeroes, we apply the result of Stark (2.5) together with the discriminant bound (2.9) to arrive at

$$\sum_{n=1}^{N}\frac{1}{\pi(x)}Li(x^{\beta_{2n+1}})\ll\sum_{n=1}^{N}x^{-\frac{1}{n!\log(n^{n^2})}}\ll Nx^{-\frac{1}{N^N N^2}}. \tag{2.10}$$

Using the previous bound (2.10) and standard computations, we deduce that inequality (2.8) is true as long as

$$N\ll\frac{\log\log x}{\log\log\log x}\cdot \tag{2.11}$$

We are left to note that the "bad" primes which do not satisfy Dedekind's theorem are exactly the primes dividing $[\mathcal{O}_{K_{2n+1}}:\mathbb{Z}[\alpha]]$. We have at most

$\omega(2n+1)) \ll \log n$ of such primes and, using (2.11), their total contribution is at most

$$\frac{1}{\pi(x)}\sum_{n\leq N}\sum_{\substack{p\leq x\\ \text{p 'bad' for } K_{2n+1}}}\rho_n(p) \ll \frac{1}{\pi(x)}\sum_{n\leq N} n\log n \ll \frac{N^2\log N}{\pi(x)} = o(N). \quad \square$$

Assuming the Generalized Riemann Hypothesis (GRH) the bound from Theorem 2.1 can be significantly improved.

Theorem 2.2. *Assume that GRH is true. Then,*

$$\frac{1}{\pi(x)}\sum_{p\leq x}(p - V(0,p-1)) \gg \frac{x^{1/4}}{\log x}\cdot$$

Proof. We consider as before the family of polynomials f_n and the associated family of extensions K_n of degree n. Here, we do not need to restrict to odd n because we use GRH instead of Stark's result.

Following the same lines as in the proof of Theorem 2.1 and replacing the error term in the prime ideal theorem by the conditional one, we obtain

$$\sum_{p\leq x}\rho_n(p) \geq \pi(x) + O\left(x^{\frac{1}{2}}(\log d_{K_n} + n\log x)\right). \tag{2.12}$$

Averaging over the family of polynomials $\{f_n(x), 1\leq n\leq N\}$ and performing the same computation as in (2.6), we arrive at

$$\frac{1}{\pi(x)}\sum_{p\leq x}(p - V(0,p-1)) \geq \sum_{n=1}^{N}\frac{1}{\pi(x)}\sum_{p\leq x}\rho_n(p) \gg N + ET.$$

Using the discriminant bound (2.9) we can bound error term by

$$ET \ll \sum_{n=1}^{N}\left\{x^{-\frac{1}{2}}\log x(\log(n^{n^2}) + n\log x)\right\} \ll \frac{\log^2 x}{\sqrt{x}}N^3.$$

Easy computation shows that the error term is negligible compared to N provided

$$N \ll \frac{x^{1/4}}{\log x},$$

and the result follows. As in the proof of Theorem 2.1, we can easily deal with the additional restriction $p \nmid [\mathcal{O}_{K_n} : \mathbb{Z}[\alpha]]$. We bound the contribution of "bad" primes in exactly the same way:

$$\frac{1}{\pi(x)}\sum_{n\leq N}\sum_{\substack{p\leq x\\ \text{p 'bad' for } K_n}}\rho_n(p) \ll \frac{1}{\pi(x)}\sum_{n\leq N} n\log n \ll \frac{N^2\log N}{\pi(x)} = o(N). \quad \square$$

Theorem 2.2 directly implies:

Corollary 2.3. *Assume that GRH is true. There exists infinitely many primes p such that*

$$p - V(0, p-1) \gg \frac{p^{1/4}}{\log p}\cdot$$

Remark 2.4. Working in K_n instead of the splitting field of f_n allows us to get the bound on the discriminant exponentially smaller than the one used in [1]. The main improvement then comes from the fact that counting prime ideals of degree 1 in K_n corresponds to counting primes with the appropriate weight suitable for our problem.

3. Concluding remarks. Erdős conjecture on average

It might be possible to prove Erdős conjecture for almost all primes p. Indeed, if a prime p satisfies Erdős conjecture, then at least two of the $f_n(x) = x(x+1)\cdots(x+n-1) - 1,\ n = 1, \ldots, p-1$ have a root modulo p. Chebotarev's theorem tells us that the density of primes p such that $f_n(x)$ has no roots modulo p is equal to the proportion of elements in $Gal(Spl(f_n))$ without fixed points. The natural strategy would be to apply Chebotarev's theorem to the product $f := \prod_i f_{n_i}$ (where n_i is a suitable sequence of integers) to control the density of primes failing Erdős conjecture. This amounts to understanding the proportion of elements in the Galois group without fixed points. The following lemma helps us to do that:

Lemma 3.1. *Suppose that G is a subgroup of S_n acting on a set X of n elements. Then the proportion σ_n of elements of G that do not have any fixed point satisfies*

$$\sigma_n \leq 1 - 1/n. \tag{3.1}$$

Proof. We denote by X^σ the number of elements of X fixed by $\sigma \in G$ and $X\backslash G$ the number of orbits of the action of G on X. By Burnside's lemma, we have that

$$|X\backslash G| = \frac{1}{|G|}\sum_{\sigma\in G}|X^\sigma|.$$

Hence

$$1 \leq |\{\sigma,\ X^\sigma \neq \varnothing\}|\frac{n}{|G|}$$

and the result follows. □

Remark 3.2. Interesting lower bounds for σ_n can be found in [3].

If the splitting fields of $f_{n_i}(x)$ are disjoint we can apply Chebotarev's theorem to f and bound the number of permutations without fixed points in

$$Gal(Spl(f)) \cong \prod_i Gal(Spl(f_{n_i})).$$

Several computations provides support towards the following conjecture:

Conjecture 3.3. *Let $n_1 \neq n_2$ be positive integers. Then*

$$Spl(f_{n_1}) \cap Spl(f_{n_2}) = \mathbb{Q}.$$

This conjecture together with Lemma 3.1 imply the Erdős conjecture on average. Indeed, for each prime p failing to satisfy the aforementioned conjecture, each f_n has at most 1 root. Hence, the density of primes S failing Erdős conjecture is

$$S \leq \sum_{n=2}^{N} (1-\sigma_n) \prod_{j \neq n} \sigma_j \ll \log N \prod_{n=2}^{N} \left(1 - \frac{1}{n}\right) \xrightarrow[N \to \infty]{} 0.$$

where we used Lemma 3.1. The last inequality follows by optimizing the function $f(\sigma_1, \cdots, \sigma_N) = \sum_{n=2}^{N} (1-\sigma_n) \prod_{j \neq n} \sigma_j$ over the domain defined by the inequalities $0 \leq \sigma_n \leq 1 - 1/n$, $n = 2, \ldots, N$.

We notice that proving Conjecture 3.3 for a good proportion of n would suffice to obtain a zero density of primes failing Erdős conjecture.

Acknowledgements

The authors would like to thank Andrew Granville and Igor Shparlinski for valuable comments. During the preparation of this manuscript, O.K. was supported by the ISM doctoral grant and J. Armand Bombardier Foundation excellence award. M.M. was supported by a postdoctoral grant in CRM of Montreal under the supervision of Andrew Granville and Dimitris Koukoulopoulos.

References

[1] W. D. Banks, F. Luca, I. E. Shparlinski & H. Stichtenoth, "On the value set of $n!$ modulo a prime", *Turkish J. Math.* **29** (2005), no. 2, p. 169-174.

[2] K. A. Broughan & A. R. Barnett, "On the missing values of $n! \bmod p$", *J. Ramanujan Math. Soc.* **24** (2009), no. 3, p. 277-284.

[3] P. J. Cameron & A. M. Cohen, "On the number of fixed point free elements in a permutation group", *Discrete Math.* **106/107** (1992), p. 135-138, A collection of contributions in honour of Jack van Lint.

[4] C. Cobeli, M. Vâjâitu & A. Zaharescu, "The sequence $n! \pmod p$", *J. Ramanujan Math. Soc.* **15** (2000), no. 2, p. 135-154.

[5] M. Z. Garaev & J. Hernández, "A note on $n!$ modulo p", To appear in Monatschefte für Mathematic, `http://arxiv.org/abs/1505.05912`.

[6] M. Z. Garaev & F. Luca, "Character sums and products of factorials modulo p", *J. Théor. Nombres Bordeaux* **17** (2005), no. 1, p. 151-160.

[7] M. Z. Garaev, F. Luca & I. E. Shparlinski, "Character sums and congruences with $n!$", *Trans. Amer. Math. Soc.* **356** (2004), no. 12, p. 5089-5102 (electronic).

[8] ———, "Exponential sums and congruences with factorials", *J. Reine Angew. Math.* **584** (2005), p. 29-44.

[9] R. K. Guy, *Unsolved problems in number theory*, Unsolved Problems in Intuitive Mathematics, vol. 1, Springer-Verlag, New York-Berlin, 1981, xviii+161 pages.

[10] H. IWANIEC & E. KOWALSKI, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, 2004, xi+615 pages.

[11] O. KLURMAN & M. MUNSCH, "Distribution of factorials modulo p", Preprint, `http://arxiv.org/abs/1505.01198`.

[12] J. C. LAGARIAS, H. L. MONTGOMERY & A. M. ODLYZKO, "A bound for the least prime ideal in the Chebotarev density theorem", *Invent. Math.* **54** (1979), no. 3, p. 271-296.

[13] J. C. LAGARIAS & A. M. ODLYZKO, "Effective versions of the Chebotarev density theorem", in *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, Academic Press, London, 1977, p. 409-464.

[14] V. F. LEV, "Permutations in abelian groups and the sequence $n!$ (mod p)", *European J. Combin.* **27** (2006), no. 5, p. 635-643.

[15] G. PÓLYA & G. SZEGŐ, *Problems and theorems in analysis. Vol. II: Theory of functions, zeros, polynomials, determinants, number theory, geometry*, Die Grundlehren der mathematischen Wissenschaften, vol. 216, Springer-Verlag, 1976, xi+391 pages.

[16] B. ROKOWSKA & A. SCHINZEL, "Sur un problème de M. Erdős", *Elem. Math.* **15** (1960), p. 84-85.

[17] H. M. STARK, "Some effective cases of the Brauer-Siegel theorem", *Invent. Math.* **23** (1974), p. 135-152.

[18] T. TRUDGIAN, "There are no socialist primes less than 10^9", *Integers* **14** (2014), p. Paper No. A63, 4.

Oleksiy KLURMAN
Départment de Mathématiques et de Statistique
Université de Montréal, CP 6128 succ. Centre-Ville
Montréal QC H3C 3J7, Canada
E-mail: `lklurman@gmail.com`

Marc MUNSCH
CRM, Université de Montréal
5357 Montréal, Québec, Canada
E-mail: `munsch@dms.umontreal.ca`