On the Value Set of $n!$ Modulo a Prime

William D. Banks
Department of Mathematics, University of Missouri
Columbia, MO 65211 USA
bbanks@math.missouri.edu

Florian Luca
Instituto de Matemáticas, UNAM
C.P. 58180, Morelia, Michoacán, México
fluca@matmor.unam.mx

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

Henning Stichtenoth
Fachbereich Mathematik, Universität Duisburg-Essen
45117 Essen, Germany
stichtenoth@uni-essen.de
and
Sabanci University, MDBF
34956 Orhanli, Tuzla, Istanbul, Turkey
henning@sabanciuniv.edu

Abstract

We show that for infinitely many prime numbers p there are at least $\log\log p/\log\log\log p$ distinct residue classes modulo p that are not congruent to $n!$ for any integer n.

1 Introduction

For any odd prime p, let $F(p)$ be the number of the distinct residue classes modulo p that are missed by the sequence $\{n! : n = 1, 2, \ldots\}$.

In **F11** of [5], it is conjectured that $F(p) \approx p/e$ as $p \to \infty$. This question appears to be quite difficult, and very little is known at the present time about the distribution of $n!$ modulo p. Some evidence for the conjecture is provided by [1], where it is shown that for a random permutation σ of the set $\{1, \ldots, p-1\}$, the products

$$\prod_{i=1}^{n} \sigma(i), \qquad n = 1, \ldots, p-1,$$

hit the expected number of $p(1 - 1/e)$ residue classes modulo p. It has been remarked in [3] that $F(p) \le p - (p-1)^{1/2}$ (which is based on the simple observation that $n = n!/(n-1)!$). Several other results about the distribution of $n!$ modulo p can be found in [2, 3, 4, 7, 10], but unfortunately these give very little insight into the behaviour of $F(p)$.

Here, we show that the *Chebotarev Density Theorem* implies that the relation $\limsup_{p\to\infty} F(p) = \infty$ holds. Below, we give a slightly more precise form of this statement using a result from [6].

The implied constants in the symbol 'O' are always absolute.

Acknowledgements. The authors wish to thank Francesco Pappalardi and Filip Saidak for useful discussions. During the preparation of this paper, W. B. was supported in part by NSF grant DMS-0070628, F. L. was supported in part by grants SEP-CONACYT 37259-E and 37260-E, and I. S. was supported in part by ARC grant DP0211459. The paper was written during a visit by F. L. and I. S. to the University of Missouri–Columbia and a visit by I. S. and H. S. to Sabanci University, Istanbul; the hospitality of these institutions is gratefully acknowledged.

2 Preparations

We use some standard notions of the theory of algebraic number fields which can be found in [8] and many other standard textbooks.

Given two number fields $\mathbb{K} \subset \mathbb{L}$ and a basis $\{\beta_1, \ldots, \beta_\ell\}$ for $\mathbb{L}$ over $\mathbb{K}$ (thus $\ell = [\mathbb{L} : \mathbb{K}]$), we denote by $D_{\mathbb{L}/\mathbb{K}}(\beta_1, \ldots, \beta_\ell)$ the discriminant of this basis. We also denote by $N_{\mathbb{L}/\mathbb{K}}(\beta) \in \mathbb{K}$ the relative norm of an element $\beta \in \mathbb{L}$.

We recall the following formula for discriminants in a tower of finite extensions $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ (see [8, Chapter 2, Exercise 23]). If $[\mathbb{L} : \mathbb{K}] = \ell$, $[\mathbb{M} : \mathbb{L}] = m$, and $\{\beta_1, \ldots, \beta_\ell\}$ and $\{\gamma_1, \ldots, \gamma_m\}$ are bases for $\mathbb{L}$ over $\mathbb{K}$ and $\mathbb{M}$ over $\mathbb{L}$, respectively, then the discriminant of the basis $\{\beta_1\gamma_1, \ldots, \beta_\ell\gamma_m\}$ of $\mathbb{M}$ over $\mathbb{K}$ is given by

$$D_{\mathbb{M}/\mathbb{K}}(\beta_1\gamma_1, \ldots, \beta_\ell\gamma_m) = D^m_{\mathbb{L}/\mathbb{K}}(\beta_1, \ldots, \beta_\ell) N_{\mathbb{L}/\mathbb{K}}\left(D_{\mathbb{M}/\mathbb{L}}(\gamma_1, \ldots, \gamma_m)\right). \quad (1)$$

We also recall that the discriminant $D_\mathbb{F}$ of an algebraic number field $\mathbb{F}$ over $\mathbb{Q}$ divides the discriminant $D_{\mathbb{F}/\mathbb{Q}}(\vartheta_1, \ldots, \vartheta_N)$ of any basis $\{\vartheta_1, \ldots, \vartheta_N\}$ of $\mathbb{F}$ over $\mathbb{Q}$, whenever $\vartheta_1, \ldots, \vartheta_N$ are algebraic integers (see [8, Chapter 2]).

We now establish a useful estimate for the discriminant of the splitting field of a polynomial over $\mathbb{Z}$ in terms of the differences between its roots. This result may be of independent interest.

Lemma 1. *Let $\alpha_1, \ldots, \alpha_t \in \mathbb{C}$ be the roots of a monic irreducible polynomial $f(X) \in \mathbb{Z}[X]$ of degree t. Then the discriminant $D_\mathbb{F}$ of the splitting field $\mathbb{F} = \mathbb{Q}(\alpha_1, \ldots, \alpha_t)$ satisfies the inequality*

$$|D_\mathbb{F}| \le \Delta^{t(t-1)t!/2},$$

where

$$\Delta = \max_{1\le i<j\le t} |\alpha_i - \alpha_j|.$$

Proof. We consider the tower of extensions $\mathbb{L}_0 = \mathbb{Q}$, $\mathbb{L}_i = \mathbb{L}_{i-1}(\alpha_i)$, and let $n_i = [\mathbb{L}_i : \mathbb{L}_{i-1}]$, $i = 1, \ldots, t$. In particular, $\mathbb{F} = \mathbb{L}_t$.

We observe that for $i = 1, \ldots, t$, the conjugates of α_i over $\mathbb{L}_{i-1}$ are among the roots of f. Therefore, for $i = 1, \ldots, t$, the n_i-tuple $\left(1, \alpha_i, \ldots, \alpha_i^{n_i-1}\right)$ is a basis of $\mathbb{L}_i$ over $\mathbb{L}_{i-1}$ whose discriminant is given by

$$D_{\mathbb{L}_i/\mathbb{L}_{i-1}}(1, \alpha_i, \ldots, \alpha_i^{n_i-1}) = (-1)^{n_i(n_i-1)/2} \prod_{\substack{r,s\in\mathcal{J}_i\\ r\ne s}} (\alpha_r - \alpha_s) \quad (2)$$

for some set $\mathcal{J}_i \subset \{1, \ldots, t\}$ of cardinality $\#\mathcal{J}_i = n_i$.

For every $i = 1, \ldots, t$, the $n_1 \cdot \ldots \cdot n_i$-tuple

$$\mathcal{A}_i = \left(\prod_{j=1}^{i} \alpha_j^{a_j}\right)_{0\le a_1\le n_1-1,\ldots,0\le a_i\le n_i-1}$$

is a basis of $\mathbb{L}_i$ over $\mathbb{Q}$. We claim that the absolute value of the discriminant of this basis $|D_{\mathbb{L}_i/\mathbb{Q}}(\mathcal{A}_i)|$ is a product of

$$N_i = n_1 \cdot \ldots \cdot n_i \cdot (n_1 + \ldots + n_i - i)$$

factors of the form $|\alpha_r - \alpha_s|$ for $1 \le r < s \le t$.

We prove this by induction on i. For $i = 1$, the assertion is trivial. We now assume that $|D_{\mathbb{L}_{i-1}/\mathbb{Q}}(\mathcal{A}_{i-1})|$ is a product of N_{i-1} such factors. Then, by (1) and (2), $|D_{\mathbb{L}_i/\mathbb{Q}}(\mathcal{A}_i)|$ is a product of

$$N_{i-1}n_i + n_1 \cdot \ldots \cdot n_i \cdot (n_i - 1) = n_1 \cdot \ldots \cdot n_i \cdot (n_1 + \ldots + n_i - i)$$

factors of the requested form. Taking into account that $n_i \le t - i + 1$ for $i = 1, \ldots, t$, we derive

$$N_t \le t! \left(\frac{t(t+1)}{2} - t \right) = \frac{t(t-1)t!}{2}.$$

Since, as we have mentioned, $D_{\mathbb{F}}$ divides $D_{\mathbb{F}/\mathbb{Q}}(\mathcal{A}_t)$, we obtain the inequality

$$|D_{\mathbb{F}}| \le |D_{\mathbb{F}/\mathbb{Q}}(\mathcal{A}_t)| \le \Delta^{N_t},$$

which concludes the proof. □

Let us consider the family of polynomials

$$f_t(X) = X(X+1)\ldots(X+t-1) - 1, \qquad t = 1, 2 \ldots. \tag{3}$$

Lemma 2. *For an integer $t \ge 5$, the roots of the polynomial f_t given by* (3) *are real and belong to interval* $[-t+1/2, 1/2]$.

Proof. It is enough to show that $f_t(X)$ alternates its sign at half integers $-k+1/2$ for $k = 0, \ldots, t$. We first remark that this property obviously holds for $g_t(X) = X(X+1)\ldots(X+t-1)$. Thus, it is now enough to show that $|g_t(-k+1/2)| > 1$ for $k = 0, \ldots, t$. But trivially,

$$|g_t(-k+1/2)| = \prod_{i=0}^{t-1} |i - k + 1/2| \ge \left(\frac{3}{2}\right)^{t-2} \left(\frac{1}{2}\right)^2 \ge \left(\frac{3}{2}\right)^4 \left(\frac{1}{2}\right)^2 > 1$$

for $t \ge 6$. For $t = 5$ this property can be verified directly. □

3 The Main Result

Theorem 3. *The following bound holds:*

$$\limsup_{p\to\infty} \frac{F(p)\log\log\log p}{\log\log p} \ge 1.$$

Proof. For a sufficiently large integer $t \ge 1$ we consider the polynomial f_t given by (3). It is well known (see [9, Part VIII, Chapter 2, Section 3, Problem 121]) that f_t is irreducible over $\mathbb{Z}$. We denote by $\mathbb{F}_t = \mathbb{Q}(\alpha_1, \ldots, \alpha_t)$ the algebraic number field generated by all the roots $\alpha_1, \ldots, \alpha_t$ of f_t, and let D_t be the discriminant of $\mathbb{F}_t$. Then, by [6, Theorem 1.1], there exists a prime number $p \le D_t^{O(1)}$ which splits into a product of distinct ideals of first degree in $\mathbb{F}_t$ over $\mathbb{Q}$. This is equivalent to the fact that f_t has t distinct zeros $0 < m_1 < \ldots < m_t \le p-1$ modulo p. In particular, $(m_i-1)! \equiv (m_i+t-1)! \pmod p$ for each $i = 1, \ldots, t$. It is clear that $m_t+t-1 \le p-1$, for otherwise $f(m_t) \equiv -1 \not\equiv 0 \pmod p$. Also, $m_2 - 1 > 1$. Therefore, the $t-1$ values $(m_i+t-1)! \pmod p$, $i = 2, \ldots, t$ all occur at least twice among the residues of $n! \pmod p$. Hence $F(p) \ge t-1$.

Combining Lemma 1 and Lemma 2, we derive that

$$|D_t| \le t^{t(t-1)t!/2},$$

thus $p \le \exp\left(O(t!\, t^2 \log t)\right) \le \exp(t^t)$, provided that t is large enough. Considering both possibilities $t > \log\log p$ and $t \le \log\log p$ we see that the inequality

$$t \ge \frac{\log\log p}{\log\log\log p}$$

holds, which finishes the proof. ☐

References

[1] C. Cobeli, M. Vâjâitu and A. Zaharescu, 'The sequence $n! \pmod p$', *J. Ramanujan Math. Soc.*, **15** (2000), 135–154.

[2] M. Z. Garaev and F. Luca, 'On a theorem of A. Sárközy and applications', *Preprint*, 2003.

[3] M. Z. Garaev, F. Luca and I. E. Shparlinski, 'Character sums and congruences with $n!$', *Trans. Amer. Math. Soc.*, (to appear).

[4] M. Z. Garaev, F. Luca and I. E. Shparlinski, 'Exponential sums and congruences with factorials', *J. Reine Angew. Math.*, (to appear).

[5] R. K. Guy, *Unsolved problems in number theory*, Springer-Verlag, New York, 1994.

[6] J. C. Lagarias, H. L. Montgomery and A. M. Odlyzko, 'A bound for the least prime ideal in the Chebotarev density theorem', *Invent. Math.*, **54** (1979), 271–296.

[7] F. Luca and P. Stănică, 'Products of factorials modulo p', *Colloq. Math.*, **96** (2003), 191–205.

[8] D. A. Marcus, *Number fields*, Springer-Verlag, 1977.

[9] G. Pólya and G. Szegö, *Problems and theorem in analysis, Vol.II*, Springer-Verlag, 1976.

[10] B. Rokowska and A. Schinzel, 'Sur une probléme de M. Erdős', *Elem. Math.*, **15** (1960), 84–85.