Rev. Mat. Iberoam. (Online first)
DOI 10.4171/RMI/1422

On the sequence $n!$ mod p

Alexandr Grebennikov, Arsenii Sagdeev, Aliaksei Semchankau and Aliaksei Vasilevskii

Abstract. We prove that the sequence $1!, 2!, 3!, \ldots$ produces at least $(\sqrt{2}+o(1))\sqrt{p}$ distinct residues modulo prime p. Moreover, the factorials within an interval $\mathcal{I} \subseteq \{0, 1, \ldots, p-1\}$ of length $N > p^{7/8+\varepsilon}$ produce at least $(1+o(1))\sqrt{p}$ distinct residues modulo p. As a corollary, we prove that every non-zero residue class can be expressed as a product of seven factorials $n_1! \cdots n_7!$ modulo p, where $n_i = O(p^{6/7+\varepsilon})$ for all $i = 1, \ldots, 7$, which provides a polynomial improvement upon the preceding results.

1. Introduction

Wilson's theorem represents one of the most elegant results in elementary number theory. It states that if p is a prime number, then $(p-1)! = -1 \mod p$. As one of its simple corollaries, we note that $(p-2)! = 1! \mod p$, and thus not all the residues from

$$\mathcal{A}(p) := \{i! \mod p : i \in [p-1]\}$$

are distinct. Erdős conjectured, see [16], that this is not the only coincidence, i.e., that $|\mathcal{A}(p)| < p-2$. Surprisingly, despite the long history of this natural problem, Erdős' conjecture remains widely open though verified [18] for all primes $p < 10^9$.

At the same time, it is widely believed (see [2,6] and Section F11 in [12]) that the elements of $\mathcal{A}(p)$ may be considered as more or less 'independent uniform random variables' for large p. In particular, it is conjectured that

$$|\mathcal{A}(p)| = \Big(1 - \frac{1}{e} + o(1)\Big)p$$

as $p \to \infty$. However, the best lower bound up to now is due to García [10]:

Theorem (García).

$$|\mathcal{A}(p)| \geqslant \Big(\sqrt{\frac{41}{24}} + o(1)\Big)\sqrt{p}.$$

2020 Mathematics Subject Classification: Primary 11N56; Secondary 11L03, 11B65.
Keywords: Factorials, exponential sums, Lang–Weil bound.

The strategy in [10] was to prove that $\mathcal{A}(p)\mathcal{A}(p)$ contains residues with certain properties, which forces the estimate $|\mathcal{A}(p)\mathcal{A}(p)| \geqslant (41/48 + o(1))p$ to hold; combined with the observation

$$\binom{|\mathcal{A}(p)|+1}{2} \geqslant |\mathcal{A}(p)\mathcal{A}(p)|,$$

this yields the result. We improve it to the following.

Theorem 1.1.

$$|\mathcal{A}(p)\mathcal{A}(p)| \geqslant p + O(p^{13/14}(\log p)^{4/7}).$$

Corollary 1.2.

$$|\mathcal{A}(p)| \geqslant \left(\sqrt{2} + o(1)\right)\sqrt{p}.$$

One of the natural ways to generalize this problem is to consider it in a 'short interval' setting (see [8, 9, 13, 15]). Throughout this paper, we let p be a large enough prime, and L and N will be integers such that $0 < L + 1 < L + N < p$. Following Garaev and Hernández [8], we define a 'short interval' analogue of $\mathcal{A}(p)$ as follows:

$$\mathcal{A}(L, N) := \{n! \mod p : L + 1 \leqslant n \leqslant L + N\}.$$

As L will not play any role, we write $\mathcal{A}_N$ for short. To bound the cardinality of this set from below, it is usually fruitful to estimate the size of $\mathcal{A}_N/\mathcal{A}_N$, the set of pairwise fractions, since we trivially have $|\mathcal{A}_N|^2 \geqslant |\mathcal{A}_N/\mathcal{A}_N|$. The first lower bounds on the size of this set of fractions were linear on N (see [9, 13]), while Garaev and Hernández [8] found the following logarithmic improvement.

Theorem (Garaev–Hernández). *Let $p^{1/2+\varepsilon} < N < p/10$. Then, for some $c_0 = c_0(\varepsilon) > 0$,*

$$|\mathcal{A}_N/\mathcal{A}_N| \geqslant c_0 N \log\left(\frac{p}{N}\right).$$

The strategy in [8] was to observe that $\mathcal{A}_N/\mathcal{A}_N$ contains the sets $X_1, X_2, \ldots, X_M$ defined as $X_j = \{(x+1)(x+2)\cdots(x+j) : L + 1 \leqslant x \leqslant L + N - M\}$, and then prove that the X_j are 'large', but their intersections $X_k \cap X_j$ are 'small', which makes the inclusion-exclusion formula applicable:

$$|\mathcal{A}_N/\mathcal{A}_N| \geqslant |X_1 \cup X_2 \cup \cdots| \geqslant \sum_j |X_j| - \sum_{k<j} |X_k \cap X_j| \gg \sum_j |X_j|.$$

In the present paper, we give the following improvement of this result.

Theorem 1.3. *Let N be such that $c_5\sqrt{p}(\log p)^2 \leqslant N \leqslant p$. Let $K := p/N$ and let $Q := \frac{N}{\sqrt{p}(\log p)^2}$. Then*

$$|\mathcal{A}_N/\mathcal{A}_N| \geqslant \begin{cases} p + O(p^{13/14}(\log p)^{4/7}) & \text{if } N \geqslant c_1 p^{13/14}(\log p)^{4/7}, \\ p + O(p^{5/6}K^{4/3}(\log p)^{4/3}) & \text{if } c_1 p^{13/14}(\log p)^{4/7} \geqslant N \geqslant c_2 p^{7/8}\log p, \\ cNQ^{1/3}(\log Q)^{-2/3} & \text{if } c_2 p^{7/8}\log p \geqslant N \geqslant c_3 p^{4/5}(\log p)^{8/5}, \\ cNK^{1/2} & \text{if } c_3 p^{4/5}(\log p)^{8/5} \geqslant N \geqslant c_4 p^{4/5}(\log p)^{4/5}, \\ cNQ^{1/3} & \text{if } c_4 p^{4/5}(\log p)^{4/5} \geqslant N \geqslant c_5 p^{1/2}(\log p)^2. \end{cases}$$

where $c, c_1, c_2, c_3, c_4, c_5 > 0$ are some absolute constants, whose values can be extracted from the proof.

Corollary 1.4. *For $N \gg p^{7/8}\log p$,*

$$|\mathcal{A}_N| \geqslant (1+o(1))\sqrt{p}.$$

To derive Theorem 1.3, we continue the strategy from [8] as follows: using strong results from algebraic geometry, we prove 'best possible' bounds $|X_j| \geqslant (1+o(1))N$ and $|X_k \cap X_j| \leqslant (1+o(1))N^2/p$ for prime k, j. Then we observe that bounds on sets X_j and their intersections imply they behave like independent random variables, and therefore the size of their union is at least $p + o(p)$ (see Lemma 2.1), which implies that $\mathcal{A}_N/\mathcal{A}_N$ has size at least $p + o(p)$.

This strategy turns out to be helpful when proving Theorem 1.1 as well.

One of the nice applications of these results deals with the representation of residues as a product of several factorials. It is not hard to see that the classical Wilson theorem implies the following. Any given $a \in [p-1]$ can be represented[1] as a product of three factorials,

$$a \equiv n_1!n_2!n_3! \mod p$$

for some $n_1, n_2, n_3 \in [p-1]$. The aforementioned conjecture on the 'randomness' of $\mathcal{A}(p)$ implies that even two factorials are enough. However, if we add the additional constraint that all the n_i should be of magnitude $o(p)$ as $p \to \infty$, it becomes not so clear how many factorials are required. Garaev, Luca, and Shparlinski [9] coped with seven.

Theorem (Garaev, Luca and Shparlinski). *Fix any positive $\varepsilon < 1/12$. Then for all prime p, every residue class $a \not\equiv 0 \mod p$ can be represented as a product of seven factorials,*

$$a \equiv n_1! \cdots n_7! \pmod{p},$$

such that $n_0 := \max_{1 \le i \le 7} n_i = O(p^{11/12+\varepsilon})$ as $p \to \infty$.

During the last two decades, the number of factors in the last theorem was not reduced even to 6. However, there were certain improvements on the value of n_0. García [11] showed that the theorem above holds with $n_0 = O(p^{11/12}\log^{1/2} p)$, while Garaev and Hernández [8] relaxed it to $O(p^{11/12}\log^{-1/2} p)$. Since our Theorem 1.3 improves the bounds used in the latter proof, one can obtain a slight (again, *polynomial*) improvement on the value of n_0 by following the same proof.

Theorem 1.5. *Fix any positive $\varepsilon < 1/7$. Then for all prime p, every residue class $a \not\equiv 0$ $\bmod p$ can be represented as a product of seven factorials,*

$$a \equiv n_1! \cdots n_7! \pmod{p},$$

such that $n_0 := \max_{1 \le i \le 7} n_i = O(p^{6/7+\varepsilon})$ as $p \to \infty$.

The remainder of the text has the following structure. In Section 2 we introduce some notations and useful lemmas, in Section 3 we prove results on images of 'generic' polynomials, in Section 4 we apply these results to polynomials $P_j(x) = (x+1)\cdots(x+j)$, and, finally, in Sections 5 and 6 we prove Theorems 1.1 and 1.3.

---

[1] Indeed, one may easily verify that, depending on the 'parity' of the inverse residue $b \equiv a^{-1}$, we have either $a \equiv (b-1)!(p-1-b)!$, or $a \equiv -(b-1)!(p-1-b)! \equiv (b-1)!(p-1-b)!(p-1)!$ modulo p.

2. Conventions and preliminary results

Here and below, p denotes a large prime number.

Whenever A is a set, we identify it with its indicator function

$$A(x) = \begin{cases} 1, & x \in A, \\ 0, & x \notin A. \end{cases}$$

Throughout the paper, the standard notations $\ll$, $\gg$, and respectively O and Ω, are applied to positive quantities in the usual way. That is, $X \ll Y, Y \gg X, X = O(Y)$ and $Y = \Omega(X)$ all mean that $Y \geqslant cX$, for some absolute constant $c > 0$.

A polynomial $f \in \mathbb{F}_p[x]$ is *decomposable* if $f = g \circ h$ for some polynomials $g, h \in \mathbb{F}_p[x]$ of degrees at least 2. Otherwise, it is *indecomposable*.

We recall that for any integer $d > 0$ and $a \in \mathbb{F}_p$, the *Dickson polynomial* $D_{d,a} \in \mathbb{F}_p[x]$ is defined to be the unique polynomial such that $D_{d,a}(x + a/x) = x^d + (a/x)^d$. There is also an explicit formula for it:

$$D_{d,a}(x) = \sum_{i=0}^{\lfloor d/2 \rfloor} \frac{d}{d-i} \binom{d-i}{i} (-a)^i x^{d-2i}.$$

For a positive integer j, define the polynomial

$$P_j(x) = \prod_{i=1}^{j} (x+i).$$

Given a set A and a polynomial $P \in \mathbb{F}_p[x]$, denote by $P(A)$ the set $\{P(a) \pmod{p} : a \in A\}$.

A key lemma to estimate the union of sets is the following.

Lemma 2.1. *Let $A_1, A_2, \ldots, A_n$ be finite sets, and let $a \geqslant b$ be positive integers, such that the following properties hold*:

- $|A_i| \geqslant a$ *for all* i,
- $|A_i \cap A_j| \leqslant b$ *for all* $i \neq j$.

Let $A := A_1 \cup A_2 \cup \cdots \cup A_n$. Then

$$|A| \geqslant \frac{a^2}{b}\Big(1 - \frac{a}{nb}\Big).$$

Proof. Let $S = \sum_{i \leqslant n} \sum_{a \in A} A_i(a) \geqslant na$. Observe that

$$\begin{aligned} S^2 &= \Big(\sum_{a \in A} \Big(\sum_{i \leqslant n} A_i(a)\Big)\Big)^2 \leqslant |A| \sum_{a \in A} \Big(\sum_{i \leqslant n} A_i(a)\Big)^2 = |A| \sum_{a \in A} \sum_{i,j \leqslant n} A_i(a) A_j(a) \\ &= |A| \sum_{i,j \leqslant n} |A_i \cap A_j| \leqslant |A|\big(S + (n^2 - n)b\big), \end{aligned}$$

which implies

$$|A| \geqslant \frac{S^2}{S + (n^2-n)b} \geqslant \frac{(na)^2}{na + (n^2-n)b} \geqslant \frac{na^2}{a + nb} = \frac{a^2}{b} \frac{1}{1 + \frac{a}{bn}} \geqslant \frac{a^2}{b}\Big(1 - \frac{a}{bn}\Big). \qquad \blacksquare$$

3. On images of generic polynomials

The two following results seem to be well known, yet not explicitly written in the literature (see [4, 5] for more information on related questions); we prove them here for the sake of completeness.

Lemma 3.1. *Let $P \in \mathbb{F}_p[x]$ of degree d be such that $(P(x) - P(y))/(x - y)$ is absolutely irreducible over $\mathbb{F}_p$, and let $\mathcal{I}$ be an arithmetical progression in $\mathbb{F}_p$. Then*

$$|P(\mathcal{I})| = |\mathcal{I}| + O\big(|\mathcal{I}|^2 p^{-1} + d^2\sqrt{p}\,(\log p)^2\big).$$

Lemma 3.2. *Let $P, Q \in \mathbb{F}_p[x]$ of maximal degree d be such that $P(x) - Q(y)$ is absolutely irreducible over $\mathbb{F}_p$, and let $\mathcal{I}$ be an arithmetical progression in $\mathbb{F}_p$. Then*

$$|P(\mathcal{I}) \cap Q(\mathcal{I})| \leqslant |\mathcal{I}|^2 p^{-1} + O(d^2\sqrt{p}\,(\log p)^2).$$

We postpone their proofs until the end of the section, and formulate some helpful results, which are only to be used in this section.

Given $P, Q \in \mathbb{F}_p[x]$, let us define $\phi(P, Q) \in \mathbb{F}_p[x, y]$ as

$$\phi(P,Q)(x,y) := \begin{cases} P(x) - Q(y), & \text{if } P \neq Q, \\ \frac{P(x)-P(y)}{x-y}, & \text{if } P = Q. \end{cases}$$

Let us also define

$$J(P,Q) := \#\big\{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p : \phi(P,Q)(x,y) = 0\big\}.$$

Lemma 3.3. *Given $P, Q \in \mathbb{F}_p[x]$, suppose that $\phi(P, Q)$ is absolutely irreducible over $\mathbb{F}_p$. Then*

$$J(P,Q) = p + O(d^2\sqrt{p}),$$

where d is the degree of $\phi(P, Q)$.

Proof. We recall the modification of the classical Lang–Weil result [14], with an error term due to Aubry and Perret [1]:

Theorem (Lang–Weil). *Let $\mathbb{F}_q$ be a finite field. Let $X \subseteq \mathbb{A}^2_{\mathbb{F}_q}$ be a geometrically irreducible hypersurface of degree d. Then*

$$|X(\mathbb{F}_q) - q| \leqslant (d-1)(d-2)\sqrt{q} + d - 1.$$

Since $\phi(P, Q)(x, y)$ is absolutely irreducible over $\mathbb{F}_p$, its set of zeros is (by definition) a geometrically irreducible hypersurface, and therefore the Lang–Weil theorem is applicable. This proves the lemma. ∎

Given a subset $\mathcal{I} \subseteq \mathbb{F}_p$, let us define

$$J_{\mathcal{I}}(P,Q) := \#\{(x,y) \in \mathcal{I} \times \mathcal{I} : \phi(P,Q)(x,y) = 0\}.$$

We need the following lemma, whose proof is already contained in [8], but we write it down explicitly here in full generality.

Lemma 3.4. *Let $P, Q \in \mathbb{F}_p[x]$ be such that $\phi(P, Q)$ has no linear divisors. Let $\mathcal{I}$ be an arithmetical progression in $\mathbb{F}_p$. Then*

$$J_{\mathcal{I}}(P, Q) = \frac{|\mathcal{I}|^2}{p^2}\, J(P, Q) + O(d^2\sqrt{p}\,(\log p)^2),$$

where d is the degree of $\phi(P, Q)$.

Proof. We recall the statement of Lemma 1 in [8] (originated in [3]):

Theorem (Bombieri, Chalk-Smith). *Let $(b_1, b_2) \in \mathbb{F}_p \times \mathbb{F}_p$ be a nonzero vector, and let $f(x, y) \in \mathbb{F}_p[x, y]$ be a polynomial of degree $d \geqslant 1$ with the following property: there is no $c \in \mathbb{F}_p$ for which the polynomial $f(x, y)$ is divisible by $b_1 x + b_2 y + c$. Then*

$$\Big| \sum_{\substack{(x,y)\in\mathbb{F}_p\times\mathbb{F}_p:\\ f(x,y)=0}} e^{2\pi i(b_1x+b_2y)/p} \Big| \leqslant 2d^2 p^{1/2}.$$

In what follows, we will need a bit of discrete Fourier transform in $\mathbb{F}_p$. Given a function $f\colon \mathbb{F}_p \to \mathbb{C}$, we define its discrete Fourier transform $\hat{f}\colon \mathbb{F}_p \to \mathbb{C}$ by

$$\hat{f}(r) = \sum_{x\in\mathbb{F}_p} f(x)\, e^{-2\pi i\, rx/p}.$$

One can easily verify the inverse Fourier transform formula:

$$f(x) = \frac{1}{p}\sum_{r\in\mathbb{F}_p} \hat{f}(r)\, e^{2\pi i\, rx/p}.$$

We also need the following well-known result. Let $\mathcal{I}$ be a (finite) arithmetic progression in $\mathbb{F}_p$. Then

$$\sum_{r\in\mathbb{F}_p} |\hat{\mathcal{I}}(r)| \ll p\log p,$$

where $\mathcal{I}\colon \mathbb{F}_p \to \mathbb{C}$ is interpreted as the characteristic function of the set $\mathcal{I} \subseteq \mathbb{F}_p$.

Let us consider $\mathcal{I}$ as a characteristic function of a set. Then

$$\begin{aligned} J_{\mathcal{I}}(P, Q) &= \sum_{\substack{(x,y)\in\mathbb{F}_p\times\mathbb{F}_p:\\ \phi(P,Q)(x,y)=0}} \mathcal{I}(x)\,\mathcal{I}(y) = \sum_{\substack{(x,y)\in\mathbb{F}_p\times\mathbb{F}_p:\\ \phi(P,Q)(x,y)=0}} \frac{1}{p^2}\sum_{r_1,r_2\in\mathbb{F}_p} \hat{\mathcal{I}}(r_1)\,\hat{\mathcal{I}}(r_2)\, e^{2\pi\frac{(r_1x+r_2y)}{p}} \\ &= \frac{|\mathcal{I}|\,|\mathcal{I}|}{p^2} J(P, Q) + \frac{1}{p^2}\sum_{(r_1,r_2)\neq(0,0)} \hat{\mathcal{I}}(r_1)\,\hat{\mathcal{I}}(r_2) \sum_{\substack{(x,y)\in\mathbb{F}_p\times\mathbb{F}_p\\ \phi(P,Q)(x,y)=0}} e^{2\pi i\frac{(r_1x+r_2y)}{p}}. \end{aligned}$$

The last summand can be bounded as

$$\frac{1}{p^2}\sum_{r_1\in\mathbb{F}_p} |\hat{\mathcal{I}}(r_1)| \sum_{r_2\in\mathbb{F}_p} |\hat{\mathcal{I}}(r_2)| \max_{(r_1,r_2)\neq 0} \Big| \sum_{\substack{(x,y)\in\mathbb{F}_p\times\mathbb{F}_p:\\ \phi(P,Q)(x,y)=0}} e^{2\pi i\frac{r_1x+r_2y}{p}} \Big| \ll (\log p)^2\sqrt{p}d^2.$$

This completes the proof. ∎

Now, let us turn to the proof of Lemma 3.1.

Proof. Clearly, $|P(\mathcal{I})| \leqslant |\mathcal{I}|$. Let us obtain a lower bound. The Cauchy–Bunyakovsky–Schwarz inequality implies

$$\#\{(x,y) \in \mathcal{I} \times \mathcal{I} : P(x) = P(y)\}|P(\mathcal{I})| \geqslant |\mathcal{I}|^2,$$

Clearly,

$$\#\{(x,y) \in \mathcal{I} \times \mathcal{I} : P(x) = P(y)\} = |\mathcal{I}| + J_{\mathcal{I}}(P,P) \leqslant |\mathcal{I}| + |\mathcal{I}|^2 p^{-1} + O(d^2 \sqrt{p} \log^2 p),$$

where we applied Lemmas 3.4 and 3.3. Deriving the lower bound on $|P(\mathcal{I})|$ completes the proof. ∎

Now we prove Lemma 3.2.

Proof. By Lemmas 3.4 and 3.3,

$$\begin{aligned} |P(\mathcal{I}) \cap Q(\mathcal{I})| \leqslant J_{\mathcal{I}}(P,Q) &= \frac{|\mathcal{I}|^2}{p^2} J(P,Q) + O(d^2 \sqrt{p} \log^2 p) \\ &\leqslant \frac{|\mathcal{I}|^2}{p} + O(d^2 \sqrt{p} \log^2 p). \end{aligned}$$ ∎

4. Properties of the polynomials P_j

Let us start with the following simple lemma.

Lemma 4.1. *For a given integer j, $5 \leqslant j < p$, the polynomial $P_j(x) \in \mathbb{F}_p[x]$ is not equal to $\alpha D_{j,a}(x+b) + c$ for $\alpha, a, b, c \in \mathbb{F}_p$. Moreover, if j is prime, then $P_j(x)$ is indecomposable.*

Proof. The second assertion is clear since $\deg P_j = j$. The first assertion can be proved by a straightforward comparison of the first five leading coefficients of these two polynomials. ∎

For given k, j (possibly equal), we define the polynomial $Q_{kj}(x,y)$ as $P_k(x) - P_j(y)$ divided by all possible linear factors. If $k = j$, we denote this polynomial by $Q_j(x,y)$. One can show that, for $k, j < p-2$,

$$Q_{kj}(x,y) = \begin{cases} P_k(x) - P_j(y) & \text{if } j \neq k, \\ \frac{P_j(x)-P_j(y)}{x-y} & \text{if } k = j,\ j \text{ is odd}, \\ \frac{P_j(x)-P_j(y)}{(x-y)(x+y-j-1)} & \text{if } k = j,\ j \text{ is even}. \end{cases}$$

Lemma 4.2. *The polynomial $Q_{kj}(x,y)$ is absolutely irreducible over $\mathbb{F}_p$ for (possibly equal) primes $2 < j, k < p-2$.*

Proof. First, consider the case $j = k$. Recall the following theorem of Fried [7], later modified by Turnwald [19]. We adapt it for the field $\mathbb{F}_p$ and for polynomials f of degree less than p.

Theorem (Fried–Turnwald). *Let $f \in \mathbb{F}_p[x]$ be a polynomial of degree n, $4 < n < p$. Consider the polynomial*

$$\phi(x, y) := \frac{f(x) - f(y)}{x - y}.$$

If f is indecomposable, and it is not equal $\alpha D_{n,a}(x + b) + c$ for some $\alpha, a, b, c \in \mathbb{F}_p$, then $\phi(x, y)$ is absolutely irreducible.

The application of this result to the polynomial P_j (along with the Lemma 4.1), with the explicit check for $j = 3$, gives the result.

Next, consider the case $j \neq k$. Recall the statement of Theorem 1B in [17]:

Theorem (Schmidt). *Let*

$$f(x, y) = g_0 y^d + g_1(x) y^{d-1} + \cdots + g_d(x)$$

be a polynomial in $\mathbb{K}[x, y]$ for some field $\mathbb{K}$, where g_0 is a non-zero constant. Denote

$$\psi(f) = \max_{1 \leq i \leq d} \frac{\deg g_i}{i}$$

and suppose $\psi(f) = m/d$, where m is coprime to d. Then $f(x, y)$ is absolutely irreducible.

Noticing that $\psi(Q_{kj}) = k/j$ gives the result. ∎

Clearly, if $j > k$ are odd primes, Lemma 4.2 is applicable, and Lemmas 3.1 and 3.2 imply the following:

$$|P_j(\mathcal{J})| = |\mathcal{J}| + O\big(|\mathcal{J}|^2 p^{-1} + j^2 \sqrt{p} (\log p)^2\big), \tag{4.1}$$

$$|P_j(\mathcal{J}) \cap P_k(\mathcal{J})| \leqslant |\mathcal{J}|^2 p^{-1} + O(j^2 \sqrt{p} (\log p)^2), \tag{4.2}$$

where $\mathcal{J}$ is a finite arithmetic progression in $\mathbb{F}_p$.

5. On the inequality $|\mathcal{A}(p)\mathcal{A}(p)| \geqslant p + o(p)$

Now we prove Theorem 1.1.

Proof. Let $\varepsilon_1, \varepsilon_2 > 0$ be dependent on p, but separated from zero. Set

$$N := \lfloor p^{1-\varepsilon_1} \rfloor, \quad M := \lfloor p^{\varepsilon_2} \rfloor, \quad \kappa := \log\log p / \log p,$$
$$\delta := \min(\varepsilon_1, 1/2 - 2\varepsilon_1 - 2\varepsilon_2 - 2\kappa, \varepsilon_2 - \varepsilon_1 - \kappa) > 0.$$

Let $\mathcal{J}$ be the set of odd numbers not exceeding $2N - M$, and let $Y_j := P_j(\mathcal{J})$. Clearly, $|\mathcal{J}| = N + O(M)$. Set

$$\mathcal{A} := \{1!, 2!, \ldots, (2N)!\} \cup \{(p - 2N)!, \ldots, (p - 2)!, (p - 1)!\} \mod p.$$

Clearly, $\mathcal{A}\mathcal{A} \subseteq \mathcal{A}(p)\mathcal{A}(p)$, and from now on we work with $\mathcal{A}\mathcal{A}$.

From Wilson's theorem, it follows that $y!(p-1-y)! = (-1)^{y+1} \mod p$. Therefore, y being odd implies $1/(p-1-y)! = y! \mod p$. Let $j \leqslant M$. Then

$$\begin{aligned}\mathcal{A}\mathcal{A} &\supseteq \{(y+j)!(p-1-y)! \mid y+j < 2N, y \text{ is odd}\}\\ &= \{(y+j)!/y! \mid y+j < 2N, y \text{ is odd}\} = \{P_j(y) \mid y+j < 2N, y \text{ is odd}\}.\end{aligned}$$

This implies $Y_j \subseteq \mathcal{A}\mathcal{A}$ for all $j \leqslant M$.

By equations (4.1) and (4.2), implied by Lemmas 3.1 and 3.2, we obtain the following (note that $\delta \leqslant \varepsilon_1, 1/2 - 2\varepsilon_1 - 2\varepsilon_2 - 2\kappa$ now plays a role):

$$|Y_j| \geqslant N + O(Np^{-\delta}), \quad |Y_k \cap Y_j| \leqslant \frac{N^2}{p} + O(N^2 p^{-1-\delta}), \quad k \neq j \text{ odd primes below } M.$$

Set

$$A := \bigcup_j Y_j \quad \text{for primes } j \leqslant M.$$

We have reduced the problem to showing that $|A| \geqslant p + o(p)$.

Let us apply Lemma 2.1 with

$$a := N(1 + O(p^{-\delta})), \quad b := \frac{N^2}{p}(1 + O(p^{-\delta})), \quad n \gg M/\log M \gg p^{\varepsilon_2 - \kappa}.$$

Notice that by definition of δ, which includes $\delta \leqslant \varepsilon_2 - \varepsilon_1 - \kappa$, the inequality $a/bn \ll p^{-\delta}$ holds, and therefore

$$|A| \geqslant \frac{a^2}{b}\Big(1 - \frac{a}{bn}\Big) \geqslant p(1 + O(p^{-\delta})) = p + O(p^{1-\delta}).$$

Now our goal is to maximize δ subject to

$$\delta \leqslant \begin{cases} \varepsilon_1, \\ 1/2 - 2\varepsilon_1 - 2\varepsilon_2 - 2\kappa, \\ \varepsilon_2 - \varepsilon_1 - \kappa. \end{cases} \tag{5.1}$$

Solving this system, we obtain optimal parameters $\varepsilon_1 := 1/14 - 4\kappa/7$ and $\varepsilon_2 := 1/7 - \kappa/7$, giving $\delta = 1/14 - 4\kappa/7$. This completes the proof. ∎

6. On the inequality $|\mathcal{A}_N/\mathcal{A}_N| \geqslant p + o(p)$

We turn now to the proof of Theorem 1.3.

Proof. Let $\mathcal{J} := \{L+1, \dots, L+N-M\}$, and $X_j := P_j(\mathcal{J}), j \leqslant M$, with parameters N and M depending on the case.

Case 1. $N \gg p^{13/14}(\log p)^{4/7}$.

For this case, one can apply the same argument as in the proof of Theorem 1.1 to obtain the desired bound.

Case 2. $p^{13/14}(\log p)^{4/7} \gg N \gg p^{7/8}\log p$.

As in the proof above, we write $N = p^{1-\varepsilon_1}$ and set $M = \lfloor p^{\varepsilon_2} \rfloor$ for $\varepsilon_2 > 0$. Observe that now ε_1 is fixed, but ε_2 is not.

Arguing as before, we obtain $|\mathcal{A}_N/\mathcal{A}_N| \geqslant p + O(p^{1-\delta})$, where

$$\delta \leqslant \begin{cases} \varepsilon_1, \\ 1/2 - 2\varepsilon_1 - 2\varepsilon_2 - 2\kappa, \\ \varepsilon_2 - \varepsilon_1 - \kappa. \end{cases} \tag{6.1}$$

Let us set $\varepsilon_2 := 1/6 - \varepsilon_1/3 - \kappa/3$. Observe that $\varepsilon_2 > 0$, since $\varepsilon_1 \leqslant 1/2 - \kappa$. From here we obtain that $\delta = \min(\varepsilon_1, 1/6 - 4\varepsilon_1/3 - 4\kappa/3) = 1/6 - 4\varepsilon_1/3 - 4\kappa/3$ works. Notice that $\delta > 0$ as long as $\varepsilon_1 < 1/8 - \kappa$.

This concludes the proof in the case $N \gg p^{7/8}\log p$.

Case 3. $p^{7/8}\log p \gg N \gg p^{4/5}(\log p)^{8/5}$.

Let R be a positive integer, to be chosen later. Let M be a number with exactly R odd primes below it. Clearly, $M \approx R\log R$.

Applying Lemma 3.1 to P_j for an odd prime j below M, we have

$$|X_j| \geqslant N + O(N^2p^{-1} + j^2\sqrt{p}(\log p)^2) \gg N \quad \text{if } M^2 \ll Q.$$

Therefore, summing $|X_k \cap X_j|$ and applying Lemma 3.2 to P_k, P_j for odd prime k below j, we obtain

$$\sum_{k<j} |X_k \cap X_j| \ll \frac{N^2}{p} R + RM^2\sqrt{p}(\log p)^2 \ll N \quad \text{if } R \ll K, R^3(\log R)^2 \ll Q.$$

Therefore, setting $R := Q^{1/3}(\log Q)^{-2/3}$, we obtain

$$|\mathcal{A}_N/\mathcal{A}_N| \geqslant \underbrace{|X_3 \cup X_5 \cup \cdots|}_{\text{first } R \text{ odd primes}} - \sum_{k<j,\text{odd primes}} |X_k \cap X_j| \gg \underbrace{|X_3| + |X_5| + \cdots}_{\text{first } R \text{ odd primes}} \gg NR,$$

which completes the proof in this case.

Case 4. $p^{4/5}(\log p)^{8/5} \gg N \gg p^{1/2}(\log p)^2$.

We follow the same line of argumentation as in [8], but with modified bounds on the sets X_j and their intersections.

From now on we work with all j, not just primes. Clearly, $J(j), J(k,j) \leqslant pj$, and therefore the estimates

$$J_N(j), J_N(k,j) \leqslant \frac{N^2}{p^2}pj + O(j^2\sqrt{p}(\log p)^2)$$

hold, as in [8].

As in the proof of Lemma 3.1, we apply the Cauchy–Bunyakovskii–Shwarz inequality:

$$\#\{(x,y) : P_j(x) = P_j(y), 1 \leqslant x, y \leqslant N - M\}|X_j| \geqslant (N-M)^2,$$

from where we obtain

$$|X_j| \geqslant \frac{N^2}{N + J_N(j)} \geqslant N + O\Big(\frac{N^2 j}{p} + j^2\sqrt{p}(\log p)^2\Big) \quad \forall j \leqslant M.$$

For $X_k \cap X_j$, we have the bound

$$|X_k \cap X_j| \leqslant J_N(k,j) \leqslant \frac{N^2}{p} j + O(j^2\sqrt{p}(\log p)^2) \quad \forall k < j \leqslant M,$$

as in [8].

Clearly, we have $|X_j| \gg N$ as long as $M \ll K, M^2 \ll Q$.

Clearly, we have $\sum_{k<j} |X_k \cap X_j| \ll N \ll |X_j|$ as long as $M^2 \ll K, M^3 \ll Q$.

Therefore, similarly to [8], we conclude that

$$|\mathcal{A}_N/\mathcal{A}_N| \geqslant \sum_{j\leqslant M}\Big(|X_j| - \sum_{k<j}|X_k \cap X_j|\Big) \gg \sum_{j\leqslant M}|X_j| \gg MN,$$

where we set $M := \min(\sqrt{K}, \sqrt[3]{Q})$, which gives the desired bound. ∎

Acknowledgements. A significant part of this project was done during the research workshop “Open problems in Combinatorics and Geometry III”, held in Adygea in October 2021. A. Sagdeev would like to thank the Young Russian Mathematics Contest sponsors and jury. A. Semchankau is very happy to thank the Institut de Mathématiques de Bordeaux for their hospitality and excellent working conditions.

Funding. A. Grebennikov is supported by Ministry of Science and Higher Education of the Russian Federation, agreement no. 075-15-2019-1619. A. Sagdeev is supported in part by ERC Advanced Grant ‘GeoScape’; he is also a winner of the Young Russian Mathematics Contest. A. Semchankau was partially supported by the Foundation for the Advancement of Theoretical Physics and Mathematics “BASIS”, the University of Bordeaux Pause Program, the ANR project JINVARIANT, and Journal de Théorie des Nombres de Bordeaux.

References

[1] Aubry, Y. and Perret, M.: A Weil theorem for singular curves. In *Arithmetic, geometry and coding theory (Luminy, 1993)*, pp. 1–7. De Gruyter Proceedings in Mathematics, Berlin, 1996.

[2] Broughan, K. A. and Barnett, A. R.: On the missing values of $n!$ mod p. *J. Ramanujan Math. Soc.* **24** (2009), no. 3, 277–284.

[3] Chalk, J. H. H. and Smith, R. A.: On Bombieri’s estimate for exponential sums. *Acta Arith.* **18** (1971), 191–212.

[4] Chang, M.-C.: Sparsity of the intersection of polynomial images of an interval. *Acta Arith.* **165** (2014), no. 3, 243–249.

[5] Cilleruelo, J., Garaev, M. Z., Ostafe, A. and Shparlinski, I. E.: On the concentration of points of polynomial maps and applications. *Math. Z.* **272** (2012), no. 3-4, 825–837.

[6] Cobeli, C., Vâjâitu, M. and Zaharescu, A.: The sequence $n! \pmod p$. *J. Ramanujan Math. Soc.* **15** (2000), no. 2, 135–154.

[7] Fried, M.: On a conjecture of Schur. *Michigan Math. J.* **17** (1970), no. 1, 41–55.

[8] Garaev, M. Z. and Hernández, J.: A note on $n!$ modulo p. *Monatsh. Math.* **182** (2017), no. 1, 23–31.

[9] Garaev, M. Z., Luca, F. and Shparlinski, I. E.: Character sums and congruences with $n!$. *Trans. Amer. Math. Soc.* **356** (2004), no. 12, 5089–5102.

[10] García, V. C.: On the value set of $n!m!$ modulo a large prime. *Bol. Soc. Mat. Mexicana (3)* **13** (2007), no. 1, 1–6.

[11] García, V. C.: Representations of residue classes by product of factorials, binomial coefficients and sum of harmonic sums modulo a prime. *Bol. Soc. Mat. Mexicana (3)* **14** (2008), no. 2, 165–175.

[12] Guy, R. K.: *Unsolved problems in number theory*. Second edition. Problem Books in Mathematics, Unsolved Problems in Intuitive Mathematics I, Springer-Verlag, New York, 1994.

[13] Klurman, O. and Munsch, M.: Distribution of factorials modulo p. *J. Théor. Nombres Bordeaux* **29** (2017), no. 1, 169–177.

[14] Lang, S. and Weil, A.: Number of points of varieties in finite fields. *Amer. J. Math.* **76** (1954), no. 4, 819–827.

[15] Lev, V. F.: Permutations in abelian groups and the sequence $n! \pmod p$. *European J. Combin.* **27** (2006), no. 5, 635–643.

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

[17] Schmidt, W. M.: Absolutely irreducible equations $f(x, y) = 0$. In *Equations over finite fields, an elementary approach*, pp. 92–133. Lecture Notes in Mathematics 536, Springer Verlag, Berlin, Heidelberg, 1976.

[18] Trudgian, T.: There are no socialist primes less than 10^9. *Integers* **14** (2014), article no. A63, 4 pp.

[19] Turnwald, G.: On Schur's conjecture. *J. Austral. Math. Soc. Ser. A* **58** (1995), no. 3, 312–357.

Received September 29, 2022; revised February 19, 2023. Published online April 6, 2023.

Alexandr Grebennikov
Saint-Petersburg State University, Universitetskaya Emb. 7/9, 199034 Saint Petersburg, Russia; and IMPA, Estr. da Vista Chinesa 110, 22460-320 Rio de Janeiro, Brazil;
sagresash@yandex.ru

Arsenii Sagdeev
Alfréd Rényi Institute of Mathematics, Reáltanoda utca 13-15, 1053 Budapest, Hungary;
sagdeevarsenii@gmail.com

Aliaksei Semchankau
Moscow State University, Leninskie Gory 1, 119991 Moscow; and Saint-Petersburg State University, Universitetskaya Emb. 7/9, 199034 Saint Petersburg, Russia;
aliaksei.semchankau@gmail.com

Aliaksei Vasilevskii
Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, USA;
avasileu@andrew.cmu.edu