JOINT DISTRIBUTION OF FACTORIAL UNITS AND VALUATIONS IN TRANSLATED INTERVALS

WILL HOWE, GRANT HUFFMAN, JENSEN KOHLMEYER, AND LIAM KRUER

Abstract. For every fixed finite set of primes, the corresponding prime valuations of factorials, reduced modulo arbitrary fixed integers, and the prime-free parts, reduced modulo arbitrary fixed prime powers, have a joint uniform distribution. We give a proof with a power-saving error on every interval of consecutive nonnegative integers, uniform in the interval's starting point. A fixed congruence on the index may be imposed independently. The resulting statement for the part of a factorial coprime to an arbitrary fixed modulus gives the densities and relative density asked for in Problems 2 and 3 of Hajdu and Papp. The proof uses a finite digit-window identity, a strict local character contraction, and a carry estimate followed by finite Fourier analysis.

hexagon:2611.00310v1

1. Statement and scope

Write $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ and $\mathrm{e}(x) = \exp(2\pi i x)$. For a prime p and $n \in \mathbb{N}_0$, put

$$E_p(n) = v_p(n!), \qquad U_p(n) = \frac{n!}{p^{E_p(n)}}.$$

Thus $E_p(0) = 0$, $U_p(0) = 1$, and $U_p(n)$ is a unit modulo every power of p. All parameters in the following theorems are fixed; only the length and starting point of the interval vary.

Theorem 1.1. *Let $\mathcal{P}$ be a nonempty finite set of distinct primes. For each $p \in \mathcal{P}$, fix integers $r_p, b_p \geq 1$. Fix also an integer $Q \geq 1$. There are constants $C > 0$ and $\delta > 0$, depending only on these parameters, such that the following holds. For all $A \in \mathbb{N}_0$, $N \geq 1$, all residues $a_p \pmod{r_p}$ and $c \pmod{Q}$, and all $z_p \in (\mathbb{Z}/p^{b_p}\mathbb{Z})^\times$,*

$$\#\{A \leq n < A + N : E_p(n) \equiv a_p \pmod{r_p},\ U_p(n) \equiv z_p \pmod{p^{b_p}}\ (p \in \mathcal{P}),\ n \equiv c \pmod{Q}\} \tag{1.1}$$
$$= \frac{N}{Q \prod_{p \in \mathcal{P}} r_p \varphi(p^{b_p})} + O(CN^{1-\delta}).$$

The implied absolute constant may be taken to be one by enlarging C. In particular, no coprimality assumption on Q is required.

For an integer $m > 1$, let

$$W_m(n) = \frac{n!}{\prod_{p \mid m} p^{E_p(n)}}.$$

This integer is coprime to m.

Theorem 1.2. *Fix $m > 1$, distinct primes $q_1, \ldots, q_t$, positive integers $r_1, \ldots, r_t$, and $Q \geq 1$, allowing $t = 0$. For every unit $z \pmod{m}$, residues $a_i \pmod{r_i}$, and $c \pmod{Q}$,*

$$\#\{A \leq n < A + N : W_m(n) \equiv z \pmod{m},\ E_{q_i}(n) \equiv a_i \pmod{r_i}\ (1 \leq i \leq t),\ n \equiv c \pmod{Q}\} \tag{1.2}$$
$$= \frac{N}{Q\varphi(m) \prod_{i=1}^{t} r_i} + O(N^{1-\delta}),$$

Date: November 7, 2026.

Prepared with AI assistance from OpenAI Codex in mathematical exploration, checking, and manuscript preparation.

where $\delta > 0$ and the implied constant depend only on the fixed parameters. The estimate is uniform for $A \in \mathbb{N}_0$, $N \geq 1$, and the displayed targets.

Taking $Q = 1$ and, respectively, $t = 0$ or arbitrary t gives the densities asked for in Problems 2 and 3 of Hajdu and Papp [2]. Their Theorems 2.1 and 2.2 establish the single-prime case with valuation modulus a power of that prime, including an explicit gap bound; their Theorems 2.3 and 2.4 give finer results in a particular case modulo 8. The distribution of the valuation coordinates alone was established by Berend and Kolesnik [1]. We include all ingredients needed for the joint unit and valuation statement here, without asserting priority for its special cases.

Corollary 1.3. *Every set counted in Theorem 1.2 is infinite and relatively dense in $\mathbb{N}_0$: some integer $L \geq 1$, depending only on the fixed parameters, has the property that every interval $[A, A+L)$, $A \in \mathbb{N}_0$, contains a member of the set. Its natural density is $(Q\varphi(m)\prod_i r_i)^{-1}$.*

Proof. Set $d = (Q\varphi(m)\prod_i r_i)^{-1}$. Choose L so large that $CL^{1-\delta} < dL$. Then the count in every interval of length L is positive. Dividing (1.2) with $A = 0$ by N and letting N tend to infinity gives the density. □

Remark 1.4. The congruence $n \equiv c \pmod{Q}$ permits any fixed restriction on finitely many terminal digits, or any other fixed periodic restriction on the index, by taking a union of residue classes. No independence from unrestricted digit-sum conditions is asserted. The parameters do not grow with N. The results concern fixed local data and give no conclusion about isolated solutions of $n! + 1 = x^2$.

2. A digit-window formula

Fix a prime p and integers $r, b \geq 1$ throughout this section. All unit identities are in $(\mathbb{Z}/p^b\mathbb{Z})^\times$. Define

$$F(t) = \prod_{\substack{1 \leq j \leq t \\ p \nmid j}} j, \qquad G = F(p^b), \qquad w_i(n) = \left\lfloor \frac{n}{p^i} \right\rfloor \bmod p^b,$$

where $0 \leq w_i(n) < p^b$. Let $s_p(n)$ denote the sum of the base-p digits of n.

Lemma 2.1. *For $n \in \mathbb{N}_0$,*

$$U_p(n) = G^{E_p(n) - \sum_{j=1}^{b-1} \lfloor n/p^j \rfloor} \prod_{i \geq 0} F(w_i(n)). \tag{2.1}$$

For every character $\chi : (\mathbb{Z}/p^b\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ and $u \in \{0, \ldots, r-1\}$, one may write

$$\mathrm{e}(uE_p(n)/r)\chi(U_p(n)) = \mathrm{e}(\alpha n) f(n), \qquad f(n) = B(n)\mathrm{e}(\theta s_p(n)) \prod_{i \geq 0} \chi(F(w_i(n))), \tag{2.2}$$

where $|f(n)| = 1$, B has period p^{b-1}, and α, θ are real.

Proof. Separating the multiples of p from a factorial gives $U_p(n) = F(n)U_p(\lfloor n/p \rfloor)$ and hence $U_p(n) = \prod_{i \geq 0} F(\lfloor n/p^i \rfloor)$. The units in each block of length p^b have the same residues, so $F(t) = G^{\lfloor t/p^b \rfloor} F(t \bmod p^b)$. The resulting exponent of G is

$$\sum_{i \geq 0} \left\lfloor \frac{n}{p^{i+b}} \right\rfloor = E_p(n) - \sum_{j=1}^{b-1} \left\lfloor \frac{n}{p^j} \right\rfloor.$$

Here $E_p(n) = \sum_{j \geq 1} \lfloor n/p^j \rfloor$, since each factor of $n!$ is counted once for each power of p dividing it. If $n = \sum_j d_j p^j$, summing this formula over digits also gives $E_p(n) = (n - s_p(n))/(p-1)$.

Choose $\gamma \in \mathbb{R}$ with $\chi(G) = \mathrm{e}(\gamma)$, choosing $\gamma = 0$ when χ is trivial. Substitution in (2.1) gives

$$\theta = -\frac{u/r + \gamma}{p-1}, \qquad \alpha = -\theta - \gamma \sum_{j=1}^{b-1} p^{-j}, \qquad B(n) = \mathrm{e}\left(\gamma \sum_{j=1}^{b-1} \frac{n \bmod p^j}{p^j}\right).$$

These formulas prove (2.2) and the asserted periodicity. All infinite products and sums above have only finitely many nonidentity terms. Empty sums, including those when $b = 1$, are zero. □

Define the zero-padded window product

$$T(t) = \prod_{i \geq 0} F(w_i(p^{b-1}t)). \tag{2.3}$$

It includes every window of b consecutive digits meeting the digits of t, with zero digits on both sides.

Lemma 2.2. *One has $T(pt) = T(t)$ and*

$$T(t) = U_p(p^{b-1}t) G^{-E_p(t)}. \tag{2.4}$$

For $p \nmid t$,

$$\frac{T(t)}{T(t-1)} = R(t), \qquad R(t) = t \prod_{h=1}^{b-1} C_h(t), \qquad C_h(t) = \prod_{\substack{1 \leq a \leq p^h \\ p \nmid a}} (p^h(t-1) + a). \tag{2.5}$$

The function R permutes $(\mathbb{Z}/p^b\mathbb{Z})^\times$.

Proof. Shifting the digits one position in (2.3) adds the factor $F(0) = 1$, which proves $T(pt) = T(t)$. In (2.1) with $n = p^{b-1}t$, the exponent of G is $\sum_{j \geq b} \lfloor p^{b-1}t/p^j \rfloor = E_p(t)$, proving (2.4). Further,

$$U_p(p^{b-1}t) = U_p(t) \prod_{h=1}^{b-1} F(p^h t).$$

If $p \nmid t$, then $E_p(t) = E_p(t-1)$ and $U_p(t)/U_p(t-1) = t$. The quotient of the hth factors in the last product is $C_h(t)$, proving (2.5).

Each $C_h(t)$ is a unit and is constant modulo p. Thus R is a permutation modulo p. If $k \geq 1$, comparison of individual factors gives

$$C_h(t + ap^k) \equiv C_h(t) \pmod{p^{k+1}},$$

because $h \geq 1$. Consequently, for $0 \leq a < p$,

$$R(t + ap^k) \equiv R(t) + ap^k \prod_{h=1}^{b-1} C_h(t) \pmod{p^{k+1}}. \tag{2.6}$$

The coefficient of ap^k is a unit. Therefore the p lifts of a unit class modulo p^k map bijectively onto the p lifts of its image. Induction from $k = 1$ proves the assertion modulo p^b. For $b = 1$ this is simply the map $R(t) = t$. □

3. Contraction and Fourier decay in one base

Lemma 3.1. *Suppose (u, χ) is nontrivial, meaning $u \not\equiv 0 \pmod r$ or $\chi \neq 1$. With θ as in Lemma 2.1, let*

$$h_0 = b + 1, \qquad W(t) = \mathrm{e}(\theta s_p(t))\chi(T(t)).$$

There exists $\rho < 1$ such that, for every real λ,

$$\left| p^{-h_0} \sum_{0 \leq t < p^{h_0}} W(t)\mathrm{e}(\lambda t) \right| \leq \rho. \tag{3.1}$$

Proof. The left side is a continuous function of $\lambda \pmod 1$, with values at most one, and therefore has a maximum. Suppose that maximum were one. Equality in the triangle inequality for numbers of modulus one implies that all the summands agree. The summand at $t = 0$ is one, so

$$W(t)\mathrm{e}(\lambda t) = 1 \qquad (0 \le t < p^{h_0}). \tag{3.2}$$

Both $s_p(pt) = s_p(t)$ and $T(pt) = T(t)$. Comparing $t = 1$ and $t = p$ in (3.2) gives $(p-1)\lambda \in \mathbb{Z}$. Because $t \equiv s_p(t) \pmod{p-1}$,

$$\chi(T(t)) = \mathrm{e}(-(\lambda+\theta)s_p(t)) \qquad (0 \le t < p^{h_0}).$$

For every $1 \le t < p^b$ with $p \nmid t$, subtracting one changes just the last nonzero digit, and $s_p(t) - s_p(t-1) = 1$. Lemma 2.2 now gives

$$\chi(R(t)) = \mathrm{e}(-(\lambda+\theta)).$$

Since $R(t)$ runs through every unit modulo p^b, the character χ is constant on its entire group. It takes the value one at the identity, so $\chi = 1$. Hence $\gamma = 0$, and the equation at $t = 1$ gives $\lambda + \theta \in \mathbb{Z}$. Together with $(p-1)\lambda \in \mathbb{Z}$ this implies $u/r = -(p-1)\theta \in \mathbb{Z}$, contrary to nontriviality. Compactness gives the strict bound (3.1). □

Proposition 3.2. *For a nontrivial pair (u, χ), the function f in (2.2) satisfies, for some $K > 0$, $\eta > 0$,*

$$\sup_{\xi \in \mathbb{R}} \left| p^{-k} \sum_{0 \le n < p^k} f(n)\mathrm{e}(\xi n) \right| \le K p^{-\eta k} \qquad (k \ge 0). \tag{3.3}$$

Proof. Regard the k digits of n as independent uniform digits. Fix the bottom $b-1$ digits, so that $B(n)$ is fixed. In the remaining positions choose

$$J = \max\left(0, \left\lfloor \frac{k-b+1}{h_0 + 2b - 2} \right\rfloor\right)$$

disjoint consecutive blocks, each consisting of $b-1$ lower buffer digits, h_0 free digits, and $b-1$ upper buffer digits. Fix all buffers and any unused digits. No window of length b meets two free blocks. Consequently the summand in (3.3), as a function of the free blocks, factors into one function for each block times a constant of modulus one. The digit-sum phase and the linear phase factor in the same way.

If both buffers adjoining one free block are zero, its window factors are exactly $\chi(T(t))$, where $0 \le t < p^{h_0}$ is that block's digit value. Its digit-sum phase is $\mathrm{e}(\theta s_p(t))$, and its linear phase is $\mathrm{e}(\lambda t)$ for some real λ. Its normalized sum is therefore at most ρ by Lemma 3.1. For other buffer values the triangle inequality gives the bound one. Windows lying entirely in fixed digits contribute only constants and do not affect these bounds.

Average now over the fixed digits. The $2(b-1)$ buffer digits for distinct blocks are disjoint, so the events that both buffers vanish are independent, each with probability $p^{-2(b-1)}$. The absolute normalized sum is at most

$$\left(1 - p^{-2(b-1)}(1-\rho)\right)^J.$$

This decays exponentially in k, which is (3.3) after an adjustment of K for small k. When $b = 1$ the buffers and initial fixed digits are empty, and every block gives the factor ρ; the same proof applies. □

4. Carries and distinct bases

For $L = p^k$ let $f_{[k]}$ be the periodic function of period L whose values on $0, \dots, L-1$ equal those of f.

Lemma 4.1. *Suppose $k \geq b-1$ and $1 \leq h < p^{k-b+1}$. Except for at most*

$$h\left(\frac{N}{p^{k-b+1}}+2\right)$$

integers $n \in [A, A+N)$, one has

$$f(n+h)\overline{f(n)} = f_{[k]}(n+h)\overline{f_{[k]}(n)}. \tag{4.1}$$

The bound is independent of $A \in \mathbb{N}_0$.

Proof. Put $D = p^{k-b+1}$. Exclude the h integers immediately preceding each multiple of D. There are at most $N/D+2$ relevant multiples for the given interval. At all other integers, $\lfloor (n+h)/D \rfloor = \lfloor n/D \rfloor$. Thus the digits in positions $k-b+1$ and above are unchanged in passing from n to $n+h$.

Truncation modulo p^k preserves the lower k digits. The omitted digits make equal contributions to the two digit sums, so cancel in the ratio. Every window that crosses or lies above the truncation position has its lowest position at least $k-b+1$ and is unchanged, so its factors also cancel. All remaining windows agree with those of the truncated integers. Finally B has period p^{b-1}, which divides p^k, so it agrees with its truncated values. These observations prove (4.1). □

We record the elementary analytic facts used to combine primes. If v is a function of period L with $|v| = 1$, put

$$\widehat{v}(\ell) = \frac{1}{L}\sum_{a=0}^{L-1} v(a)\mathrm{e}(-\ell a/L), \qquad c_v(h) = \frac{1}{L}\sum_{a=0}^{L-1} v(a+h)\overline{v(a)}.$$

Orthogonality of the Lth roots of unity gives

$$\sum_{\ell=0}^{L-1} |\widehat{v}(\ell)|^2 = 1, \qquad \sum_{h=0}^{L-1} |c_v(h)|^2 = L\sum_{\ell=0}^{L-1} |\widehat{v}(\ell)|^4. \tag{4.2}$$

Indeed, expansion and summation of the geometric series gives the first identity, while $c_v(h) = \sum_\ell |\widehat{v}(\ell)|^2 \mathrm{e}(\ell h/L)$ gives the second. In particular, if $\max_\ell |\widehat{v}(\ell)| \leq KL^{-\eta}$ and $H < L$, Cauchy–Schwarz gives

$$\frac{1}{H}\sum_{h=1}^{H} |c_v(h)| \leq K(L/H)^{1/2}L^{-\eta}. \tag{4.3}$$

We shall also use the following elementary form of van der Corput's inequality. For z_n supported on an interval of N integers, with $|z_n| \leq 1$, and $1 \leq H \leq N$,

$$\left|\frac{1}{N}\sum_n z_n\right|^2 \leq \left(1+\frac{H}{N}\right)\left(\frac{1}{H}+\frac{2}{H}\sum_{h=1}^{H-1}\left|\frac{1}{N}\sum_n z_{n+h}\overline{z_n}\right|\right). \tag{4.4}$$

To verify it, write $H\sum_n z_n = \sum_j \sum_{h=0}^{H-1} z_{j+h}$. At most $N+H-1$ inner sums are nonzero. Apply Cauchy–Schwarz, expand their squared moduli, and bound each off-diagonal correlation in absolute value. This gives (4.4).

Proposition 4.2. *For each $p \in \mathcal{P}$ choose a character pair (u_p, χ_p) as in Lemma 2.1. If at least one pair is nontrivial, then for some $\delta > 0$,*

$$\sum_{A \leq n < A+N} \mathrm{e}(\beta n) \prod_{p\in\mathcal{P}} \mathrm{e}(u_p E_p(n)/r_p)\chi_p(U_p(n)) \ll N^{1-\delta} \tag{4.5}$$

uniformly for $A \in \mathbb{N}_0$, $N \geq 1$, and $\beta \in \mathbb{R}$.

Proof. By (2.2), the summand has the form $g(n) = \mathrm{e}(\beta' n) \prod_p f_p(n)$ for a real β'. Choose a prime p_* with a nontrivial character pair, and take an exponent $0 < \eta \le 1/4$ for which Proposition 3.2 holds in this base. For a positive integer H, choose powers

$$L_p = p^{k_p} \asymp_p H^{1+\eta}, \qquad L = \prod_{p \in \mathcal{P}} L_p.$$

For sufficiently large H, we have $k_p \ge b_p - 1$ and $H < L_p / p^{b_p - 1}$ for every p.

For $1 \le h \le H$, apply Lemma 4.1 to each base. Replacing the ratios $f_p(n+h)\overline{f_p(n)}$ by their periodic versions changes their normalized average by

$$O\left(\sum_p h/L_p + h/N \right),$$

with constants allowed to depend on the fixed prime powers. The restriction that both $n, n+h$ lie in the original interval changes a full interval average by at most h/N. The product of the periodic ratios has period L. Its average over any interval of N integers differs from its complete period average by $O(L/N)$, independently of the starting point. The moduli L_p are pairwise coprime. The Chinese remainder theorem therefore makes that complete average equal to $\prod_p c_p(h)$, where

$$c_p(h) = \frac{1}{L_p} \sum_{a=0}^{L_p - 1} f_{p,[k_p]}(a+h) \overline{f_{p,[k_p]}(a)}.$$

The linear twist contributes only the factor $\mathrm{e}(\beta' h)$. Since $|c_p(h)| \le 1$, the normalized correlation of g, restricted to the interval, has absolute value at most

$$|c_{p_*}(h)| + O\left(\sum_p h/L_p + h/N + L/N \right). \tag{4.6}$$

Proposition 3.2 bounds every discrete Fourier coefficient of $f_{p_*,[k_{p_*}]}$ by $K L_{p_*}^{-\eta}$. Equations (4.2)–(4.3) thus imply

$$\begin{aligned} \frac{1}{H} \sum_{h=1}^{H} |c_{p_*}(h)| &\ll (L_{p_*}/H)^{1/2} L_{p_*}^{-\eta} \\ &\ll H^{-\eta/2 - \eta^2}. \end{aligned}$$

Write $s = |\mathcal{P}|$ and choose $H = \lfloor N^{1/(2s(1+\eta))} \rfloor$. Then $L \ll N^{1/2}$ and $H/L_p \ll H^{-\eta}$. Averaging (4.6) in (4.4) yields

$$\left| \frac{1}{N} \sum_{A \le n < A+N} g(n) \right|^2 \ll H^{-1} + H^{-\eta/2-\eta^2} + H^{-\eta} + H/N + N^{-1/2} \ll N^{-\eta/(4s(1+\eta))}.$$

Taking square roots proves (4.5), for example with $\delta = \eta/(8s(1+\eta))$. Values of N for which the choices above are too small are absorbed by increasing the implied constant. No bound depends on A or β. □

5. Fourier inversion and composite moduli

Proof of Theorem 1.1. For a finite abelian group H, its characters satisfy

$$\mathbf{1}_{x=y} = \frac{1}{|H|} \sum_{\psi \in \widehat{H}} \psi(x) \overline{\psi(y)}.$$

For completeness, decompose H into cyclic groups. On each cyclic factor this is the geometric-series identity; multiplication gives the displayed formula. Apply it to the group

$$(\mathbb{Z}/Q\mathbb{Z}) \times \prod_{p\in\mathcal{P}} (\mathbb{Z}/r_p\mathbb{Z}) \times (\mathbb{Z}/p^{b_p}\mathbb{Z})^\times.$$

The trivial character gives exactly the main term in (1.1). Every character with at least one nontrivial prime pair is bounded by Proposition 4.2, with $\beta = v/Q$ for some integer v. If all prime pairs are trivial but the index character is not, its sum is a geometric series of ratio $\mathrm{e}(v/Q) \neq 1$, bounded by a constant depending only on Q. The finite number of characters permits one to take the minimum of their positive exponents and the maximum of their constants. If there are no nontrivial characters, the formula is exact. This proves the theorem uniformly in every target. □

Proof of Theorem 1.2. Let $\mathcal{P}$ contain the prime divisors of m and the primes q_i. For $p \mid m$ write $p^{b_p} \parallel m$; take $b_p = 1$ for the other primes. Put $r_p = r_i$ if $p = q_i$ and $r_p = 1$ otherwise. Enlarge each valuation modulus to

$$R_q = \operatorname{lcm}\big(r_q,\ \{\varphi(p^{b_p}) : p \mid m,\ p \neq q\}\big),$$

interpreting the least common multiple of the empty additional list as r_q. For $p \mid m$ the identity of integers defining W_m gives, in $(\mathbb{Z}/p^{b_p}\mathbb{Z})^\times$,

$$W_m(n) = U_p(n) \prod_{\substack{q\mid m\\ q\neq p}} q^{-E_q(n)}. \tag{5.1}$$

The powers on the right are determined by $E_q(n) \pmod{R_q}$, since the order of a unit modulo p^{b_p} divides $\varphi(p^{b_p})$.

Fix an enlarged valuation vector satisfying the original congruences. Then multiplication by the known correction factor in (5.1) is a bijection of $(\mathbb{Z}/p^{b_p}\mathbb{Z})^\times$. For each $p \mid m$ it prescribes exactly one unit value corresponding to $z \pmod{p^{b_p}}$. The Chinese remainder theorem identifies these prescriptions with the one target $z \pmod m$. All other unit coordinates are unrestricted.

Theorem 1.1, with moduli R_q, assigns uniform weight to each enlarged valuation vector and unit vector, independently of $n \pmod Q$. There are $\prod_q (R_q/r_q)$ allowed enlarged valuation vectors. Summing over these and the unrestricted unit coordinates leaves the proportion

$$\frac{1}{Q\prod_{p\mid m}\varphi(p^{b_p})\prod_q r_q} = \frac{1}{Q\varphi(m)\prod_{i=1}^{t} r_i}.$$

Only a fixed finite number of error terms is summed, so the power saving and its uniformity in A remain valid. □

References

[1] D. Berend and G. Kolesnik, *Regularity of patterns in the factorization of n!*, J. Number Theory **124** (2007), no. 1, 181–192. doi:10.1016/j.jnt.2006.08.010.

[2] L. Hajdu and Á. Papp, *On asymptotic density properties of the sequence* $(n!)_{n=0}^{\infty}$, Acta Arith. **184** (2018), no. 4, 317–340. doi:10.4064/aa170410-21-8.

E-mail addresses: howew@purdue.edu, huffma97@purdue.edu, jenwin@purdue.edu, kruerl@purdue.edu