Research Article

Enumerating coprime permutations

Ashwin Sah  |  Mehtaab Sawhney

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts, USA

Correspondence
Mehtaab Sawhney, Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA.
Email: msawhney@mit.edu

Funding information
NSF, Grant/Award Number: DGE-1745302; PD Soros Fellowship

Abstract
Define a permutation \( \sigma \) to be coprime if \( \gcd(m, \sigma(m)) = 1 \) for \( m \in [n] \). In this note, proving a recent conjecture of Pomerance, we prove that the number of coprime permutations on \([n]\) is \( n! \cdot (c + o(1))^n \) where

\[
c = \prod_{p \text{ prime}} \frac{(p - 1)^{2(1-1/p)}}{p \cdot (p - 2)^{(1-2/p)}}.
\]

The techniques involve entropy maximization for the upper bound, and a mixture of number-theoretic bounds, permanent estimates, and the absorbing method for the lower bound.

MSC 2020
11B75 (primary)

1 | INTRODUCTION

Definition 1.1. Define a permutation \( \sigma : [n] \to [n] \) to be coprime if \( \gcd(m, \sigma(m)) = 1 \) for \( m \in [n] \). Let \( C(n) \) be the number of coprime permutations on \([n]\).

In recent work, Pomerance [11] provided nontrivial bounds on \( C(n) \) proving that \( n!/3.73^n < C(n) < n!/2.5^n \) for \( n \) sufficiently large. Pomerance then conjectured the existence of a constant \( c \) such that \( C(n) = n!(c + o(1))^n \) (see [11, Section 5]); our main objective is to provide such an asymptotic.
Theorem 1.2.

\[ C(n) = n! \left( \prod_{p \text{ prime}} \frac{(p-1)^{2(1-1/p)}}{p \cdot (p-2)^{(1-2/p)}} \pm \exp(-\Omega(\sqrt{\log n \log \log n})) \right)^n. \]

Remark. The \( p = 2 \) term is assumed to be 1/2. The same method demonstrates that for fixed \( W \), \( C_W(n) \), which counts permutations \( \sigma : [n] \to [n] \) with \( \gcd(\ell, \sigma(\ell), W!) = 1 \) (see [11, Section 5]), satisfies

\[ C_W(n) = n! \left( \prod_{p \leq W} \frac{(p-1)^{2(1-1/p)}}{p \cdot (p-2)^{(1-2/p)}} \right)^n \cdot \exp(O(\log n)), \]

though we forgo the details. McNew (private communication) has independently achieved similar results for fixed \( W \).

Theorem 1.2 is certainly not the only result regarding finding mappings between sets of integers such that the labels of the matched edges are coprime. One such example is work of Pomerance and Selfridge [13], answering a question of Newman, demonstrating that such a coprime matching exists between any set of \( n \) consecutive integers \( A \) and \([n]\). Another is work of Bohman and Peng [2], in connection with the lonely runner conjecture, proving that any two intervals \( A, B \) of length \( 2m \) in \([n]\) with \( m = 2^{O((\log \log n)^2)} \) have a coprime matching. This was strengthened in later work of Pomerance [12] to require only \( m = \Omega((\log n)^2) \). We also mention that enumerating \( C(n) \) was also considered by Jackson [7] and is listed as A005326 on the OEIS [15].

1.1 Proof techniques

For the upper bound, we study \( C(n) \) by looking at permutations where \( \gcd(j, \sigma(j)) \) has no prime divisor at most a growing function \( W \). Defining \( \tau = \prod_{p \leq W} p \) and examining the portion of integers \( j \) which are \( a \mod \tau \) and map to \( b \mod \tau \), we find that the problem essentially immediately reduces to an entropy maximization program. Using the concavity and subadditivity of entropy as well as the Chinese Remainder Theorem, we can obtain the upper bound, which is done in §2. Note that as written, this approach essentially necessarily requires \( W = O(\log n) \) as otherwise \( \tau > n \) and the integers \( \{1, \ldots, n\} \) are not equidistributed in residue classes \( \mod \tau \). In order to do better, we (a) restrict attention only to whether any prime \( p \leq W \) divides or does not divide an integer \( j \in [n] \), and (b) focus only on possible prime divisor patterns which produce large buckets (specifically, buckets which have at most \( k \approx (\log n)^{1/2} \) prime divisors), and treat the rest as an error term. Since \( \prod_{p \leq W} (1 - p^{-1}) = O(1/ \log W) \) is a negligible factor, the condition on \( W \) we obtain is roughly that \( W^k \leq n^{1/100} \), which allows for consideration of significantly more prime divisors via techniques similar to a combinatorial sieve.

For the proof of the lower bound in §3, the role of larger prime factors immediately becomes crucial. Let \( B_S \) be the set of integers in \([n]\) with \( S \) being the precise set of prime divisors at most \( W \). For the sake of this discussion \( W = \exp(c(\log n)^{1/2}(\log \log n)^{1/2}) \) and \( k = (\log n)^{1/2}(\log \log n)^{-1/2} \). Our proof is based on first taking a “template”, assigning the appropriate
“entropy-maximizing” fraction of $B_S$ to map to $B_{S'}$. Noting the size of $W$ it follows immediately that (say)

$$\sum_{\substack{p|n \\ p > W}} \frac{1}{p} \leq W^{-1/2}$$

as $n$ has at most $2 \log n/(\log \log n)$ distinct prime divisors. This suggests that the effect of “large primes” is minimal and therefore the upper bound proof should be reversible.

To make this argument rigorous, one chooses random subsets of $B_S$ to map to $B_{S'}$ in accordance with the entropy maximizing distribution. One then proves that with high probability the associated coprimality graph corresponding to $B_S, B_{S'}$, if $S$ and $S'$ have size at most $k$, has at most approximately a $W^{-1/2}$ fraction of edges missing at any vertex. This is done via the Chernoff bound and the prior estimate regarding large prime factors. Combined with estimates regarding the number of perfect matchings in a graph of high minimum degree due to Alon, Rödl, and Ruciński [1], one can (essentially) handle matching all integers with at most $k$ prime factors at most $W$.

For the remaining integers, we “absorb” this small subset into the set of integers divisible by no primes at most $W$, which is a very large set, namely of size $\Omega(n/\log W)$. On the other hand, the number of integers with at least $k$ prime factors less than $W$ is $n \exp(-Ω(k \log k))$. See [16] for a more extensive discussion of the absorbing method and its history. Our approach here can be thought of as analogous to a “robust absorption strategy”, which has appeared, for instance, in work of Montgomery [10], in which bipartite graphs with a “resilient matching” property are utilized. Finally, we note that we have omitted certain special considerations at the prime $p = 2$, which are handled via a reduction of Pomerance [11] (Lemma 3.1).

### 1.2 Further directions

We end by mentioning that we believe obtaining sharper asymptotics for $(C(n)/n!)^{1/n}$ is an interesting open problem; our methods are fundamentally limited to error terms that are of the form $n^{-o(1)}$ as we crucially rely on considering buckets whose shared prime divisors multiply to less than $n^{1/2}$ (say) in order to guarantee that the interval has the expected number of elements in such buckets. Thus either we cannot consider many primes, or cannot consider buckets with many prime divisors, either of which is a serious issue. Given this, error terms of the form $O(n^{-\Omega(1)})$ would require a substantial modification of our methods and even the truth of such a statement is not obvious. Additionally, obtaining an asymptotic expansion for $C(n)$ appears unlikely (as speculated by Jackson [7]).

We note that a reduction of Pomerance [11] shows it is enough to count coprime bijections $f : \{1, 3, ..., 2n-1\} \to [n]$. This is the number of matchings in a bipartite graph $i \in \{1, ..., 2n-1\}$ on the left and $j \in [n]$ on the right are connected if $\gcd(i, j) = 1$. Our proof can be interpreted as considering the nonedges that occur due to small primes and noting that the “remaining nonedges” are sparse. For sharper bounds, it may be possible to analyze an edge-removal process that targets the maximum entropy distribution described in Subsection 1.1 at each step, uniformly randomly choose an edge $(i, j)$ in the current graph with probability say proportional to some $g(i, j)$ and then delete $i$ from the left and $j$ from the right. Here we might take

$$g(i, j) = \prod_{2 < p \leq n} g_p(1_{p|i}, 1_{p|j})$$
with \(g_p(0,0) = (p - 2)/p, g_p(0,1) = g_p(1,0) = 1/p,\) and \(g_p(1,1) = 0.\) Depending on how long one can control this process, the remaining vertices can be handled by the absorbing method. Our proof can be thought of as very similar to analyzing such a process where we truncate the weights at \(p \leq W.\)

Techniques involving “weighted removal processes” or that target an “entropy-maximizing distribution” along with the absorbing method have been recently used to give sharp estimates on the \(n\)-queens problem [14], and may be applicable to further situations where one wishes to count objects with structured biases (such as number-theoretic considerations, as in the present work). This in turn builds on recent powerful techniques introduced for counting in quasirandom situations such as counting combinatorial designs [9], in which polynomially strong error terms are known. It remains interesting to see the limits of such techniques in number-theoretic settings.

**Notation**

Throughout this paper we will reserve \(p\) for variables which range over the primes. We will also implicitly assume \(n\) is sufficiently large for certain inequalities to hold. We write \(a = b \pm c\) to mean that \(a \in [b - c, b + c]\), and \(f = O(g)\) means \(|f| \leq Cg\) for some absolute constant \(C\) while \(f = \Omega(g)\) means \(f \geq C|g|\) for some absolute \(C\). We use \(\log^{(k)} n\) to denote the \(k\)-times iterated logarithm, for example, \(\log^{(5)} n = \log \log \log \log \log n\). We may sometimes omit floors and ceilings without comment if not essential to the situation. We say an event occurs whp (with high probability) if it occurs with probability tending to 1 as \(n \to \infty\). Given a set \(S\), we write \(\binom{S}{k}, \binom{S}{\leq k}, \binom{S}{< k}\) for the collection of subsets of \(S\) of size \(k\), size at most \(k\), and size less than \(k\), respectively. Finally, as above, we often refer to a bijective function or permutation as a matching between the domain and codomain, especially when dealing with extra constraints encoded via a graph.

## 2 | UPPER BOUND

### 2.1 | Setup

Fix \(W = \exp(2^{-10}(\log n \log \log n)^{1/2})\) and \(k = 2^{-5}(\log n / \log \log n)^{1/2}\). Let \(\alpha = \exp(-k \log k)\), which will roughly correspond to the error term we derive. Our upper bound on the number of coprime permutations \(\sigma: [n] \to [n]\) comes via enumerating permutations such that \(p \nmid \gcd(j, \sigma(j))\) for all \(p \leq W\). Let \(P_W = \{p: p \leq W\}\) be the primes which are at most \(W\).

We first define a series of sets with respect to the divisibility structure of \(P_W\). For each \(S \subseteq P_W\), let

\[
A_S = [n] \cap \bigcap_{p \in S} \{m: p|m\} \cap \bigcap_{p \in P_W \setminus S} \{m: p \nmid m\}
\]

and

\[
A_{>k} = [n] \setminus \left( \bigcup_{S \in \binom{P_W}{< k}} A_S \right).
\]

To start, we prove that \(A_S\) has the “predicted size” from an independent heuristic on small primes if \(|S| < k\), while \(A_{>k}\) is a vanishing small proportion of the set. This will allow us to
efficiently encode the divisibility structure of all primes at most $W$. Note that this is nontrivial as a more naïve bound based on the Chinese Remainder Theorem (CRT) would restrict us to having $W$ such that $\prod_{p \leq W} p \leq n^{1/2}$ (say) and hence $W \leq \log n$.

**Lemma 2.1.** For all $S \subseteq \mathcal{P}_W$ with $|S| < k$ we have

$$|A_S| = (1 \pm \alpha^2)n \prod_{p \in S} p^{-1} \prod_{p \in \mathcal{P}_W \setminus S} (1 - p^{-1}).$$

Furthermore,

$$|A_{\geq k}| \leq n\alpha^{1/2}.$$

**Remark.** A proposition of this form essentially follows techniques in the combinatorial sieve (see e.g. [6, Chapter 2]); for the sake of completeness we give a complete proof here.

**Proof.** We first handle $A_{\geq k}$. Let $Y$ be a uniformly random positive integer in $[n]$ and $Y_p$ be the indicator of $p|Y$ for $1 \leq p \leq W$. Note that

$$\Pr[Y \in A_{\geq k}] \leq \sum_{1 \leq p_1 < \cdots < p_k \leq W} \Pr\left[ \bigcap_{1 \leq j \leq k} Y_{p_j} \right] = \sum_{1 \leq p_1 < \cdots < p_k \leq W} \Pr\left[ \bigwedge_{1 \leq j \leq k} (p_j | Y) \right]$$

$$\leq 2 \sum_{1 \leq p_1 < \cdots < p_k \leq W} \prod_{1 \leq j \leq k} \frac{1}{p_j} \leq 2 \cdot k! \left( \sum_{1 \leq p \leq W} \frac{1}{p} \right)^k \leq \exp(-k \log k/2) \tag{2.1}$$

where we have used that $W^k \leq n$ to derive the probability that $Y$ is divisible by $\prod_{1 \leq j \leq k} p_j$ and used that $\sum_{1 \leq p \leq W} 1/p = O(\log \log n)$. To derive the necessary bound on $A_S$, we proceed via the Principle of Inclusion-Exclusion (PIE), in particular with the use of Bonferroni’s inequalities [3]. In particular, we have

$$\Pr[Y \in A_S] = \mathbb{E}\left[ \prod_{p \in S} Y_p \prod_{p \in \mathcal{P}_W \setminus S} (1 - Y_p) \right]$$

$$= \sum_{0 \leq j \leq 4k} (-1)^j \sum_{T \subseteq \mathcal{P}_W \setminus S} \mathbb{E}\left[ \prod_{p \in S} Y_p \prod_{p \in T} Y_p \right] \pm \sum_{T \subseteq \mathcal{P}_W \setminus S} \mathbb{E}\left[ \prod_{p \in S} Y_p \prod_{p \in T} Y_p \right]$$

$$= \sum_{0 \leq j \leq 4k} (-1)^j \sum_{T \subseteq \mathcal{P}_W \setminus S} \prod_{p \in S \cup T} p^{-1} \pm \left( \prod_{p \in S} p^{-1} \right) \exp(-3k \log k) \pm \frac{(2W)^{4k}}{n}$$

$$= \prod_{p \in S} p^{-1} \prod_{p \in \mathcal{P}_W \setminus S} (1 - p^{-1}) \pm \left( \prod_{p \in S} p^{-1} \right) \exp(-3k \log k) \pm \frac{(2W)^{4k}}{n}$$

$$= (1 \pm \exp(-2k \log k)) \prod_{p \in S} p^{-1} \prod_{p \in \mathcal{P}_W \setminus S} (1 - p^{-1}).$$
The first error term in the third line comes from a bound similar to (2.1), while the second error term in the third line comes from the slight deviations in probability that a $Y$ is divisible by some product of primes at most $W^k \leq n$. The fourth line comes from bounding the tail terms of the product expansion of $\prod_{p \in S} p^{-1} \prod_{p \in P \setminus S} (1 - p^{-1})$ (e.g. by use of the Bonferroni inequalities once again) and the fifth line follows upon converting additive error to multiplicative error, using $W^k \leq n^{1/8}$ and $\prod_{p \in P \setminus S} (1 - p^{-1}) = \Omega(1/\log W)$. This completes the proof.

Given a coprime permutation $\sigma : [n] \to [n]$ and $S_1, S_2 \subseteq P_W$ we let

$$\beta_{S_1, S_2}(\sigma) = \#\{m \in [n] : m \in A_{S_1}, \sigma(m) \in A_{S_2}\}$$

and $\beta(\sigma)$ be the tuple of all such counts. Note there are at most $(2W)^k \leq \exp(k \log k) \leq n^{1/4}$ such sets $S$ with $|S| < k$ and that by Lemma 2.1, we have $|A_{S_k}| \leq n^{\alpha_1/2}$. This implies that there are at most

$$(n+1)^{\sqrt{n}} \cdot (2n^2)^{n^{\alpha_1/2}} \leq e^{n^{\alpha_1/3}}$$

possible choices for $\beta(\sigma)$: first, for every pair $S_1, S_2$ with $|S_1|, |S_2| < k$ we choose up to $n+1$ possibilities, and then we bound the ways to simultaneously choose all $\beta_{S,S'}(\sigma)$ for $S \subseteq P_W$ and $|S'| \geq k$ (and similar for $\beta_{S',S}(\sigma)$), which is a total of $t \leq n^2$ values which must sum to $|A_{S_k}|$.

Therefore we have that

$$C(n) \leq e^{n^{\alpha_1/3}} \cdot \sup_{\beta} |\{\sigma : [n] \to [n] \text{ coprime : } \beta(\sigma) = \beta\}| \tag{2.2}$$

Finally we define the following parameters:

$$\rho_{S_1, S_2} = \beta_{S_1, S_2}/n, \quad \beta_{S_1, \cdot} = \sum_{S_2} \beta_{S_1, S_2} = |A_{S_1}|, \quad \beta_{\cdot, S_2} = \sum_{S_1} \beta_{S_1, S_2} = |A_{S_2}|.$$  

### 2.2 Completing the upper bound

We now bound the number of choices of $\sigma$ given $\beta(\sigma)$. This will complete the proof of the upper bound due to (2.2). We bound the number of permutations $\sigma$ satisfying $\beta(\sigma) = \beta$ as follows:

- For each pair of subsets $S_1, S_2 \subseteq P_W$, choose which $\beta_{S_1, S_2}$ elements of $A_{S_1}$ which have image in $A_{S_2}$. Call the set of such elements $V_{S_1 \to S_2}$.
- For each pair of subsets $S_1, S_2 \subseteq P_W$, choose which $\beta_{S_1, S_2}$ elements of $A_{S_2}$ which have preimage in $A_{S_1}$. Call the set of such elements $V_{S_1 \leftarrow S_2}$.
- Determine a precise mapping between $V_{S_1 \to S_2}$ and $V_{S_1 \leftarrow S_2}$.

Note also that if $\rho_{S_1, S_2} \neq 0$ where $S_1 \cap S_2 \neq \emptyset$, then the expression within the supremum in (2.2) is actually 0. Thus we can restrict attention to values of $\rho$ where $\rho_{S_1, S_2} = 0$ when $S_1 \cap S_2 \neq \emptyset$. 


Given this procedure, we see that the number of $\sigma$ such that $\beta(\sigma) = \beta$ is bounded by

$$\prod_{S_1, S_2 \subseteq P_W} \beta_{S_1, S_2}! \prod_{S_1 \subseteq P_W} \beta_{S_1}! \prod_{S_2 \subseteq P_W} \beta_{S_2}! \prod_{S_1 \subseteq P_W} \beta_{S_1, S_2}!$$

$$= \prod_{S_1, S_2 \subseteq P_W} (\beta_{S_1, S_2})^{-1} \prod_{S_1 \subseteq P_W} \beta_{S_1, S_2}! \prod_{S_2 \subseteq P_W} \beta_{S_2}!$$

$$\leq |A_{\geq k}|^2 \prod_{|S_1|, |S_2| < k} (\beta_{S_1, S_2})^{-1} \prod_{|S_1| < k} \beta_{S_1, S_2}! \prod_{|S_2| < k} \beta_{S_2}!$$

$$\leq e^{n \alpha^{1/3}} \cdot \prod_{|S_1|, |S_2| < k} (\beta_{S_1, S_2})^{-1} \prod_{|S| < k} |A_S|!^2$$  \hspace{1cm} (2.3)

where we used that factorials are log-convex in the third line to combine the terms for $|S| \geq k$, and used Lemma 2.1 and Stirling’s approximation in the fourth.

We now bound each term in the above product. Write $n_S = n \prod_{p \in S} p^{-1} \prod_{p \in P_W \setminus S} (1 - p^{-1})$. Noting that $n! \leq 3(n + 1)(n/e)^n$ for all $n \geq 1$ and $(2W)^k \leq n^{1/4}$, and applying Lemma 2.1 we find that

$$\prod_{|S| \leq k} |A_S|! \leq e^{n \alpha^{1/3}} \cdot \prod_{|S| < k} ((1 + \alpha^2)n_S/e)^{(1 + \alpha^2)n_S}$$

$$\leq e^{2n \alpha^{1/3}} \cdot \prod_{S \subseteq P_W} \left(\frac{n}{e}\right)^{n} \prod_{p \in S} p^{-1} \prod_{p \in P_W \setminus S} (1 - p^{-1})$$

$$= e^{2n \alpha^{1/3}} \cdot \left(\frac{n}{e}\right)^{n} \prod_{p \in P_W} (1 - 1/p)^{n(1 - 1/p)}(1/p)^{n/p}$$

Next noting that $n! \geq (n/e)^n$ for all $n \geq 1$, we find that

$$\prod_{|S_1|, |S_2| < k} (\beta_{S_1, S_2})^{-1} \leq e^{n} \prod_{|S_1|, |S_2| < k} \beta_{S_1, S_2}^{-\beta_{S_1, S_2}} \leq e^{n \alpha^{1/3}} \cdot e^{n} \prod_{S_1, S_2 \subseteq P_W} \beta_{S_1, S_2}^{-\beta_{S_1, S_2}}$$

$$= e^{n \alpha^{1/3}} \cdot e^{n} \exp\left(-n \sum_{S_1, S_2} \rho_{S_1, S_2} \log \beta_{S_1, S_2}\right)$$

$$= e^{n \alpha^{1/3}} \cdot (e/n)^{n} \exp\left(-n \sum_{S_1, S_2} \rho_{S_1, S_2} \log \rho_{S_1, S_2}\right).$$

Let $Z$ be the random variable which takes on the value $(S_1, S_2)$ with probability $\rho_{S_1, S_2}$. Treating each set $S_i$ as a vector in $\{0, 1\}^{|P_W|}$, we may equivalently view $Z = ((1_p \in S_1, 1_p \in S_2))_{p \in P_W} \in \{0, 1\}^{2|P_W|}$. Let $Z_p$ be $(1_p \in S_1, 1_p \in S_2)$ when $(S_1, S_2)$ is drawn according to $Z$, and note that $Z$ is
determined upon knowing $Z_p$ for all $p \in \mathcal{P}_W$. By the subadditivity of entropy we therefore find that
\[
\exp \left( -n \sum_{S_1,S_2} \rho_{S_1,S_2} \log \rho_{S_1,S_2} \right) = \exp(nH(Z)) \leq \prod_{p \in \mathcal{P}_W} \exp(nH(Z_p)).
\]
Note that $Z_p$ is supported on $(0,0), (1,0), (0,1)$ due to the constraint $\rho_{S_1,S_2} = 0$ whenever we have $p \in S_1 \cap S_2$. Additionally, $\mathbb{P}[Z_p = (1,')] = \mathbb{P}[Z_p = (',1)] = |n/p|/n$ since $\sigma$ is a permutation and $|[p'] \cap [n]| = |n/p|$. These constraints determine the law of $Z_p$ and therefore $H(Z_p)$. In particular, it follows that $\mathbb{P}[Z_p = (1,0)] = \mathbb{P}[Z_p = (0,1)] = 1/p \pm 1/n$ and $\mathbb{P}[Z_p = (0,0)] = 1 - 2/p \pm 2/n$.

Putting everything together into (2.3), this gives an upper bound of
\[
e^{7n\alpha^{1/3}} \cdot (n/e)^n \left( \prod_{p \in \mathcal{P}_W} (1 - 1/p)^{n(1-1/p)}(1/p)^{1/p} \right)^2 \prod_{p \in \mathcal{P}_W} (1 - 2/p)^{-n(1-2/p)}(1/p)^{-2n/p}
\]
\[
= e^{7n\alpha^{1/3}} \cdot (n/e)^n \prod_{p \in \mathcal{P}_W} (p-1)^{2(1-1/p)n}(p-2)^{-n(1-2/p)p^{-n}}
\]
\[
\leq e^{7n\alpha^{1/3} + n/W} \cdot (n/e)^n \prod_{p} (p-1)^{2(1-1/p)n}(p-2)^{-n(1-2/p)p^{-n}}
\]
where we have used that $(p-1)^{2(1-1/p)}(p-2)^{-(1-2/p)p^{-1}} = 1 + O(1/p^2)$ which implies the inequality $\prod_{p > W}(p-1)^{2(1-1/p)}(p-2)^{-(1-2/p)p^{-1}} = 1 + O(1/W \log W) \leq \exp(1/W)$. The desired result follows immediately using our expressions for $\alpha,W$.

3 | LOWER BOUND

3.1 | Setup and preliminaries

Recall that we have set $W = \exp(2^{-10}(\log n \log \log n)^{1/2})$ and $k = 2^{-5}(\log n / \log \log n)^{1/2}$, as well as $\alpha = \exp(-k \log k)$.

For the lower bound, note that any coprime permutation must map even numbers to odd numbers, which are sets of approximately the same size. In order to witness this phenomenon, we use the following reduction of Pomerance [11]. Define $[n]_o = \{1, 3, \ldots, 2n - 1\}$, the first $n$ odd positive integers.

Lemma 3.1 [11, Lemma 1]. Let $C_0(n)$ be the number of bijective functions $f : [n]_o \to [n]$ with $\gcd(j, f(j)) = 1$ for all $j \in \{1, 3, \ldots, 2n - 1\}$. Then $C(2n) = C_0(n)^2$ and $C(2n + 1) \geq 2C_0(n - 1)^2$.

We will require slightly modified sets in order to capture the divisibility structures of $[n]$ and $[n]_o$. Let $\mathcal{P}_W' = \mathcal{P}_W \setminus \{2\}$. For $S \subseteq \mathcal{P}_W'$ define
\[
B_S = [n] \cap \bigcap_{p \in S} \{m : p|m\} \cap \bigcap_{p \in \mathcal{P}_W' \setminus S} \{m : p \nmid m\}, B_{\geq k} = [n] \setminus \bigcup_{S \subseteq (\mathcal{P}_W')_k} B_S
\]
and the analogous

\[ C_S = [n]_0 \cap \bigcap_{p \in S} \{ m : p \mid m \} \cap \bigcap_{p \in P'_W \setminus S} \{ m : p \nmid m \}, \quad C_{\geq k} = [n]_0 \setminus \bigcup_{S \in (P'_W)^k} C_S. \]

Similar to Lemma 2.1, we have the following control on the set sizes \( B_S, C_S \).

**Lemma 3.2.** For all \( S \subseteq P'_W \) with \( |S| < k \) we have,

\[ |B_S|, |C_S| = (1 \pm \alpha^2)n \prod_{p \in S} p^{-1} \prod_{p \in P'_W \setminus S} (1 - p^{-1}). \]

Furthermore,

\[ |B_{\geq k}|, |C_{\geq k}| \leq \alpha^{1/2}n. \]

For the remainder of this section we focus on providing an asymptotic lower bound on \( C_0(n) \), which we treat as a matching problem between \([n]_0\) and \([n]\) with forbidden edges corresponding to noncoprime pairs. Now, heuristically, the lower bound should match the bounding scheme presented in §2 (ignoring the prime \( p = 2 \)). However, to actually ensure we avoid coprimality with respect to larger primes \( p \), we will require a number of estimates. The crucial point for our lower bound is noting that the divisibility structure of primes larger than \( W \) removes a sparse graph (of density bounded by say \( W^{-1/2} \)).

**Fact 3.3.** For \( \ell \in [2n] \) we have that

\[ \sum_{\substack{p \mid \ell \\text{ or } p > W}} \frac{1}{p} < W^{-1/2}. \]

**Proof.** This is immediate noting that at most \( 2 \log n / (\log \log n) \) distinct primes divide an integer \( \ell \in [2n] \).

We will also require that for a given “large class” only a small portion of numbers are divisible by a fixed \( p \).

**Lemma 3.4.** For \( W < p' \leq n^{1/3} \) and \( |S| < k \), we have that

\[ |B_S \cap \{ m : p' \mid m \}| \leq 2|A_S|/p', \quad |C_S \cap \{ m : p \mid m \}| \leq 2|B_S|/p'. \]

For \( p' > n^{1/3} \) we have that

\[ |B_S \cap \{ m : p' \mid m \}| \leq 2n^{2/3}, \quad |C_S \cap \{ m : p \mid m \}| \leq 2n^{2/3}. \]

**Proof.** The second claim follows immediately as \( |[2n] \cap \{ m : p' \mid m \}| \leq 2n^{2/3} \). For the first claim, we focus on \( B_S \) as the analogous claim for \( C_S \) follows similarly. Let \( Y \) and \( Y_p \) be as in the proof of
Lemma 2.1. Note that

\[ P[Y \in A \land Y' \in B] = E \left[ Y'_p \prod_{p \in S} Y_p \prod_{p \in P' \setminus S} (1 - Y_p) \right] \]

\[ = \sum_{0 \leq j \leq 4k} (-1)^j \sum_{T \subseteq (P'_j \setminus S)} E \left[ Y'_p \prod_{p \in S} Y_p \prod_{p \in T} Y_p \right] \pm \sum_{T \subseteq (P'_j \setminus S)} E \left[ Y'_p \prod_{p \in S} Y_p \prod_{p \in T} Y_p \right] \]

\[ = \sum_{0 \leq j \leq 4k} (-1)^j \sum_{T \subseteq (P'_j \setminus S)} (p')^{-1} \prod_{p \in S \cup T} p^{-1} \]

\[ \pm \left( (p')^{-1} \left( \prod_{p \in S} p^{-1} \right) \exp(-3k \log k) + (2W)^{4k/n} \right) \]

\[ = (1 \pm \alpha^2)(p')^{-1} \prod_{p \in S} p^{-1} \prod_{p \in P' \setminus S} (1 - p^{-1}) \]

where we have used that \( n^{1/3}(W)^{4k} \leq n^{1/4} \). The result follows immediately. \( \Box \)

We will also require that in any bipartite graph with balanced vertex parts and a very large minimum degree there are a large number of perfect matchings. The argument is identical to that of Alon, Rödl, and Ruciński [1, Theorem 1], but we reprove the result in order to quantify the dependencies.

Lemma 3.5. Let \( G = (A \cup B, E) \) be a bipartite graph such that \( |A| = |B| = n \) and \( \Delta = \Delta(K_{A, B} \setminus G) \), the maximum degree of the bipartite complement, satisfies \( \Delta \leq n/3 \). Then there are at least \( (n - 2\Delta)/e \) perfect matchings in \( G \).

Proof. By [1, Theorem 3], if for any \( X \subseteq A, Y \subseteq B, k(|X| + |Y|) + E(A \setminus X, B \setminus Y) \geq kn \) holds, then \( G \) has a \( k \)-factor (and therefore a subgraph of \( G \) which is \( k \)-regular). Let \( k = n - 2\Delta \) and note that for \( |X| + |Y| \geq n \) the above inequality is immediate. If \( |X| + |Y| \leq n \), suppose that \( |X| \geq |Y| \) (the other case being analogous) and note that \( E(A \setminus X, B \setminus Y) \geq (n - |X|)(n - |Y|) - (n - |X|)\Delta = (n - |X|)(n - |Y| - \Delta) \) and hence

\[ k(|X| + |Y|) + E(A \setminus X, B \setminus Y) \geq k(|X| + |Y|) + (n - |X|)(n - |Y| - \Delta). \]

Therefore it suffices to check that \( k(|X| + |Y|) + (n - |X|)(n - |Y| - \Delta) \geq kn \) which is equivalent to

\[ k(n - |X| - |Y|) \leq (n - |X|)(n - |Y| - \Delta). \]

Fix \( |X| + |Y| = t \) and imagine varying \( |X| \) with \( t \geq |X| \geq |Y| = t - |X| \). By concavity of the right side, it suffices to check when \( |X| = t, |Y| = 0 \) and \( |X| = |Y| = t/2 \). In the first case the inequality
follows as \( k \leq n - \Delta \) and in the second case the inequality is equivalent to
\[
k(n - t) \leq (n - t/2)(n - t/2 - \Delta).
\]
Viewing the difference of the right and left hand sides as functions of \( t \), the derivative is seen to be \( t/2 + k - n + \Delta/2 \) and thus the inequality is closest when \( t = 2n - 2k - \Delta = 3\Delta \). It becomes
\[
(n - 2\Delta)(n - 3\Delta) \leq (n - 3\Delta/2)(n - 5\Delta/2)
\]
which is trivially true as \( n \geq 3\Delta \).

Now let \( G' \) be the corresponding subgraph of \( G \) which is exactly \( k \)-regular. Then by the solution of the van der Waerden conjecture on permanents due to Egorychev [4] and Falikman [5] it follows that the number of perfect matchings in \( G' \) is at least \((k/n)^n n! \geq (k/e)^n\). \( \square \)

Finally we will repeatedly require the Chernoff bound (see, e.g., [8, Theorems 2.1 and 2.10]). Recall that the hypergeometric distribution with parameters \( (N, n_1, n_2) \) is the size of the intersection of two independent uniformly random subsets of \([N]\) of sizes \( n_1 \) and \( n_2 \).

**Lemma 3.6** (Chernoff bound). Let \( X \) be either:

- a sum of independent random variables, each of which takes values in \([0,1]\)
- hypergeometrically distributed (with any parameters).

Then for any \( \delta \geq 0 \) we have
\[
P[X \geq (1+\delta) \mathbb{E}X] \leq \exp(-\delta^2 \mathbb{E}X/(2 + \delta)).
\]

### 3.2 Proof of the lower bound

In order to complete the proof of Theorem 1.2, we devise a procedure that produces a triplet \((\sigma, R_B, R_C)\) where \( R_B \subseteq [n] \) and \( R_C \subseteq [n] \) with \( |R_B|, |R_C| \leq n \exp(n\alpha_c) \) and such that the permutation \( \sigma \) is coprime. The number of possible outcomes of such a procedure is bounded above by \( C(n) \exp(n\alpha_c/2) \) due to the size bounds on \( R_B, R_C \) and therefore it suffices to provide a lower bound on the number of distinct possible outcomes. (One can think of \( R_B, R_C \) as encoding the degree of “noninjectivity” for the procedure producing coprime permutations \( \sigma \), to ensure a controllable lower bound.)

Let \( \mathcal{M}_B \) denote the set of labels \( \bigcup_{S \subseteq P^W} \{ S \} \cup \{ * \} \) and let \( \mathcal{M}_C \) denote the set of labels \( \bigcup_{S \subseteq P^W} \{ S \} \cup \{ * \} \). We first construct (via a randomized procedure) a pair of maps \( \phi_1 : [n] \to \mathcal{M}_B \) and \( \phi_2 : [n] \to \mathcal{M}_C \) which will serve as a template for the procedure producing coprime \( \sigma \).

**Lemma 3.7.** There exist assignment functions \( \phi_1 : [n] \to \mathcal{M}_B \) and \( \phi_2 : [n] \to \mathcal{M}_C \) such that:

- \( \phi_1(m_1) = * \) for \( m_1 \in B_{3k} \) and \( \phi_2(m_2) = * \) for \( m_2 \in C_{3k} \).
- If \( S \cap T \neq \emptyset \) then \( x \in B_S \) implies \( \phi_1(x) \neq T \), and \( y \in C_T \) implies \( \phi_2(y) \neq S \).
- For \( |S_1|, |S_2| < k \), we have
\[
\beta_{S_1,S_2} := |\{ m_1 \in B_{S_1} : \phi_1(m_1) = S_2 \}| = |\{ m_2 \in C_{S_2} : \phi_2(m_2) = S_1 \}|.
\]
• For all $|S_1|, |S_2| < k$,
\[
\beta_{S_1,S_2} = (1 \pm \exp(-\Omega((\log n \log \log n)^{1/2}))) n \prod_{p \in S_1} p^{-1} \prod_{p \in S_2} p^{-1} \prod_{p \in \mathcal{P}_w \setminus (S_1 \cup S_2)} (1 - 2p^{-1})
\]

• $|\{m_1 : \phi_1(m_1) = \ast\}| \leq 2\alpha^{1/2}n$.
• $|\{m_2 : \phi_2(m_2) = \ast\}| \leq 2\alpha^{1/2}n$.

**Proof.** We construct initial random assignment functions which essentially only fail the third bullet point, and then “throw out” a small fraction of values by reassigning them to $\ast$ in order to balance the two sides. For $m_1 \in B_{\geq k}$ deterministically assign $\phi_1'(m_1) = \ast$ and for $m_2 \in C_{\geq k}$ deterministically assign $\phi_2'(m_2) = \ast$. Given $m_1 \in B_S$ with $|S| < k$, for each $|T| < k$ we assign $\phi_1'(m_1) = T$ with probability
\[
1_{S \cap T = \emptyset} \cdot \prod_{p \in T} (p^{-1} - 1) \prod_{p \in \mathcal{P}_w \setminus (S \cup T)} (1 - (p^{-1} - 1))
\]
and otherwise set $\phi_1'(m_1) = \ast$. Analogously, given $m_2 \in C_S$ with $|S| < k$, for $|T| < k$ we assign $\phi_2'(m_2) = T$ with probability
\[
1_{S \cap T = \emptyset} \cdot \prod_{p \in T} (p^{-1} - 1) \prod_{p \in \mathcal{P}_w \setminus (S \cup T)} (1 - (p^{-1} - 1))
\]
and else set $\phi_2'(m_2) = \ast$. Evidently the stated probabilities add to at most 1 when summing over $|T| < k$, so this is well-defined.

By Lemma 3.2 we have for $|S_1|, |S_2| < k$ which are disjoint that
\[
\mathbb{E}|\{m_1 \in B_{S_1} : \phi_1'(m_1) = S_2\}| = (1 \pm \alpha^2)n \prod_{p \in S_1} p^{-1} \prod_{p \in \mathcal{P}_w \setminus (S_1 \cup S_2)} (1 - (p^{-1} - 1))
\]
and analogously
\[
\mathbb{E}|\{m_2 \in C_{S_2} : \phi_2'(m_2) = S_1\}| = (1 \pm \alpha^2)n \prod_{p \in S_2} p^{-1} \prod_{p \in \mathcal{P}_w \setminus (S_1 \cup S_2)} (1 - 2p^{-1})
\]
and applying Chernoff (Lemma 3.6) it follows with probability at least $1/2$ that if for $|S_1|, |S_2| < k$ disjoint we set
\[
\beta_{S_1,S_2} = \min(|\{m_1 \in B_{S_1} : \phi_1'(m_1) = S_2\}|, |\{m_2 \in C_{S_2} : \phi_2'(m_2) = S_1\}|)
\]
then

$$\beta_{S_1, S_2} = (1 \pm 2\alpha^2) n \prod_{p \in S_1} p^{-1} \prod_{p \in S_2} p^{-1} \prod_{p \in \mathbb{P} \setminus (S_1 \cup S_2)} (1 - 2p^{-1}).$$

To construct $\phi_1$, for each pair of disjoint $|S_1|, |S_2|$ of size less than $k$ assign $\beta_{S_1, S_2}$ values of $S_1$ to map to the label $S_2$. Send all remaining values in $S_1$, if any, to * (and set $B_{\geq k} = *$ as before). For $\phi_2$, assign $\beta_{S_1, S_2}$ values of $S_2$ to map to the label $S_1$ and send all remaining values in $S_2$, if any, to *. This is well-defined since clearly

$$\sum_{|S_2| < k} \beta_{S_1, S_2} \leq \sum_{|S_2| < k} |\{m_1 \in B_{S_1} : \phi_1'(m_1) = S_2\}| \leq |B_{S_1}|$$

and similar for $\phi_2'$.

The first four properties follow immediately. The final two properties follow from noting that

$$\left|\{m_1 \in B_{S_1} : \phi_1'(m_1) = S_2\}\right| - \left|\{m_2 \in C_{S_2} : \phi_2'(m_2) = S_1\}\right| \leq 8\alpha^2 \beta_{S_1, S_2},$$

so the extra amount of values assigned the label * is not significant, and by citing the second part of Lemma 3.2. 

To construct $(\sigma, R_B, R_C)$, we define $\beta_{S_1, S_2}$ as in Lemma 3.7, $\beta^1_* = |\{m_1 : \phi_1(\sigma_1(m_1)) = \ast\}|$, and $\beta^2_* = |\{m_2 : \phi_2(\sigma_2(m_2)) = \ast\}|$. Next we consider the following procedure:

- Fix $\phi_1, \phi_2$ satisfying Lemma 3.7 with these values of $\beta$.
- Choose $\sigma_1$ uniformly randomly among all permutations of $[n]$ with $\sigma_1(B_S) = B_S$ for all $S$ and $\sigma_2$ uniformly randomly among all permutations of $[n]$ with $\sigma_2(C_S) = C_S$ for all $S$.
- Let $B_{S_1, S_2} = \{m_1 \in B_{S_1} : \phi_1(\sigma_1(m_1)) = S_2\}$ and $C_{S_1, S_2} = \{m_2 \in C_{S_2} : \phi_2(\sigma_2(m_2)) = S_1\}$ for $|S_1|, |S_2| < k$. Furthermore let $R_B = \{m_1 : \phi_1(\sigma_1(m_1)) = \ast\}$ and $R_C = \{m_2 : \phi_2(\sigma_2(m_2)) = \ast\}$.
- For disjoint $S_1, S_2$ of size at most $k$ with $(S_1, S_2) \neq (\emptyset, \emptyset)$, let $\sigma$ form a uniformly random matching between $B_{S_1, S_2}$ and $C_{S_1, S_2}$ not violating the coprimality condition.
- For $(S_1, S_2) = (\emptyset, \emptyset)$ let $\sigma$ be a uniformly random matching between $B_{\emptyset, \emptyset} \cup R_B$ and $C_{\emptyset, \emptyset} \cup R_C$.
- Output $(\sigma, R_B, R_C)$.

Note that this fully specifies $\sigma$ since if $S_1 \cap S_2 \neq \emptyset$ we have $x \in B_{S_1}$ implies $\phi_1(x) \neq S_2$ and similar for $\phi_2$. Furthermore, given the output $(\sigma, R_B, R_C)$ we can mostly reconstruct the procedure. In particular, for $|S_1|, |S_2| < k$, $B_{S_1, S_2}$ is the set of values in $B_{S_1}$ mapped to $C_{S_2}$ by $\sigma$ for all $(S_1, S_2) \neq (\emptyset, \emptyset)$, while $B_{\emptyset, \emptyset}$ is the set of values in $B_{\emptyset} \setminus R_B$ mapped to $C_{\emptyset} \cup R_C$. This determines $\sigma_1$ up to right-multiplication by some $\xi_1$ which preserves the sets $B_{S_1, S_2}$ for all $|S_1|, |S_2| < k$ as well as $R_B$, and similar for $\sigma_2$.

Therefore, if $X$ is the number of possible outputs $(\sigma, R_B, R_C)$ where $\sigma$ is coprime and $Y$ is the number of ways to run the above procedure where the output is coprime, we have

$$Y \leq X \cdot \beta^1_* \beta^2_* \prod_{|S_1|, |S_2| < k \neq \emptyset} \beta_{S_1, S_2} \leq C_0(n) \cdot n^{\beta^1_* + \beta^2_*} \prod_{|S_1|, |S_2| < k \neq \emptyset} \beta_{S_1, S_2}.$$ (3.1)

Now we provide a lower bound on $Y$. 
Note that by Lemma 3.4 and the Chernoff bound (Lemma 3.6), with probability at least $3/4$ we have that for all disjoint $|S_1|, |S_2| < k$ the coprimality bipartite graph between parts $B_{S_1,S_2}$ and $C_{S_1,S_2}$ for $(S_1, S_2) \neq (\emptyset, \emptyset)$ has at most $4W^{-1/2}\beta_{S_1,S_2}$ edges missing from each vertex. Furthermore with probability $3/4$ the noncoprimality bipartite graph between $B_{\emptyset,\emptyset} \cup R_B$ and $C_{\emptyset,\emptyset} \cup R_C$ has at most $4W^{-1/2}\beta_{\emptyset,\emptyset} + |R_B|$ edges missing from each vertex. Using that $|\beta_{\emptyset,\emptyset}| \geq n \exp(-2\log\log n)$ and $|R_B| = \beta_1 \leq 2\alpha^{1/2}n$, we see that the maximum degree of the complement bipartite graph is bounded by $(4W^{-1/2} + \alpha^{1/3})\beta_{\emptyset,\emptyset}$, say.

Therefore applying Lemma 3.5 shows that there are

$$Y \geq (3/4)^2 \beta_1^2 \prod_{|S| < k} |B_S|! \prod_{|S| < k} |C_S|! \cdot \prod_{|S_1|, |S_2| < k, S_1 \cap S_2 = \emptyset} (\beta_{S_1,S_2}/e)^{\beta_{S_1,S_2} e^{-4(4W^{-1/2} + \alpha^{1/3})\beta_{S_1,S_2}}}$$

possible valid ways to run the procedure. Now, given (3.1) and (3.2), a nearly identical calculation as in § 2 demonstrates

$$C_0(n) \geq \exp(-n\alpha^{1/4}) n! \left( \prod_{p > 2} \frac{(p - 1)2^{(1-1/p)}}{p \cdot (p - 2)^{(1-2/p)}} \right)^n.$$

Finally, using Lemma 3.1 implies the result.

Acknowledgements

We thank Carl Pomerance for comments motivating our proof of Lemma 2.1 and for communicating the results of McNew (private communication) regarding $C_k(n)$. We also thank the referee for a number of useful comments. Sah and Sawhney were supported by NSF Graduate Research Fellowship Program DGE-1745302. Sah was supported by the PD Soros Fellowship.

Journal Information

Mathematika is owned by University College London and published by the London Mathematical Society. All surplus income from the publication of Mathematika is returned to mathematicians and mathematics research via the Society’s research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

References

1. N. Alon, V. Rödl, and A. Ruciński, Perfect matchings in $\epsilon$-regular graphs, Electron. J. Combin. 5 (1998), 13.
2. T. Bohman and F. Peng, Coprime mappings and lonely runners, Preprint, arXiv:2109.09860, 2021.
3. C. Bonferroni, Teoria statistica delle classi e calcolo delle probabilità, Pubblicazioni del R Istituto Superiore di Scienze Economiche e Commerciali di Firenze 8 (1936), 3–62.
4. G. P. Egorychev, The solution of the van der Waerden problem for permanents, Dokl. Akad. Nauk SSSR 258 (1981), no. 5, 1041–1044.
5. D. I. Falikman, Proof of the van der Waerden conjecture on the permanent of a doubly stochastic matrix, Mat. Zametki 29 (1981), no. 6, 931–938, 957.
6. H. Halberstam and H.-E. Richert, Lond. Math. Soc. Monographs, No. 4, Academic Press [Harcourt Brace Jovanovich, Publishers], London–New York, 1974.
7. D. M. Jackson, The combinatorial interpretation of the Jacobi identity from Lie algebras, J. Combinatorial Theory Ser. A 23 (1977), no. 3, 233–256.
8. S. Janson, T. Łuczak, and A. Rucinski, Wiley-interscience series in discrete mathematics and optimization, Wiley-Interscience, New York, N.Y., 2000.
9. P. Keevash, *Counting designs*, J. Eur. Math. Soc. (JEMS) **20** (2018), no. 4, 903–927.
10. R. Montgomery, *Spanning trees in random graphs*, Adv. Math. **356** (2019), 106793, 92.
11. C. Pomerance, *Coprime permutations*, Preprint, arXiv:2203.03085, 2022.
12. C. Pomerance, *Coprime matchings*, Integers **22** (2022), A2.
13. C. Pomerance and J. L. Selfridge, *Proof of D. J. Newman’s coprime mapping conjecture*, Mathematika **27** (1980), no. 1, 69–83.
14. M. Simkin, *The number of n-queens configurations*, Preprint, arXiv:2107.13460, 2021.
15. N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences (OEIS)*.
16. E. Szemerédi, *Is laziness paying off? (“Absorbing” method)*, Colloquium De Giorgi 2010–2012, Colloquia, vol. 4, Ed. Norm., Pisa, 2013, pp. 17–34.