COPRIME MATCHINGS

Carl Pomerance
Mathematics Department, Dartmouth College, Hanover, New Hampshire
carlp@math.dartmouth.edu

Received: 11/12/21, Accepted: 12/13/21, Published: 1/7/22

Abstract
We prove that there is a (perfect) matching between two intervals of positive integers of the same even length, with corresponding pairs coprime, provided the intervals are in $[n]$ and their lengths are $> c(\log n)^2$, for a positive constant c. This improves on a recent result of Bohman and Peng. As in their paper, the result has an application to the lonely runner conjecture.

1. Introduction

Suppose one has two intervals I and J of positive integers, and both have the same length. Among the many possible bijections from I to J, it is interesting to wonder if at least one of them is a coprime matching. That is, in the bijection, corresponding numbers should be relatively prime. It is easy to see that sometimes this is not possible. For example, if $1 \notin I$ and J contains a number j divisible by the product of the members of I, then that number j cannot correspond to any member of I. Another easy way to block a coprime matching is if both intervals contain a strict majority of even numbers, as would be the case with $\{2, 3, 4\}$ and $\{8, 9, 10\}$, for example.

An easy way to bar the majority evens case is to insist that the common length be even, say $2m$. And an easy way to bar an element from one interval having a common nontrivial factor with each number of the other interval is to insist that the numbers are not too large in comparison to the length.

Here are some existing results about coprime matchings of intervals. If one of the intervals is $[n] = \{1, 2, \ldots, n\}$ and the other an arbitrary interval of length n, then there is a coprime matching, see [8]. Here we allow odd lengths and there is no prohibition of one of the intervals involving numbers much larger than the length, but these are compensated for by having the number 1 in one of the intervals.

Very recently, Bohman and Peng [1] showed that if I, J are contiguous intervals of any length $k \geq 4$ such that $k \in I$, then there is a coprime matching, so verifying a conjecture of Larsen, Lehmann, Park, and Robertson [7]. They also proved the following result.

Theorem A. *There is a positive constant $\mathcal{C}$ such that if n is sufficiently large, $m > \exp(\mathcal{C}(\log\log n)^2)$, and $I, J \subset [n]$ are intervals of length $2m$, then there is a coprime matching of I and J.*

In this note we improve on Theorem A.

Theorem 1. *There is a positive constant c such that if n is sufficiently large, $m > c(\log n)^2$, and $I, J \subset [n]$ are intervals of length $2m$, then there is a coprime matching of I and J.*

Note that the expression $c(\log n)^2$ cannot be improved to $\log n$. This follows from [2, Theorem I], where it is shown that there are infinitely many integers n for which there is an interval of $\geq \log n$ integers in $[n]$ each with a nontrivial common divisor with n. This can be improved a little using better estimates for the Jacobsthal function, see [3].

Adding to the interest of the Bohman–Peng paper is an application of Theorem A to the lonely runner conjecture. This conjecture asserts that if $v_1, v_2, \ldots, v_n$ are distinct positive integers, then there is a real number t such that no $v_i t$ is strictly within distance $1/(n+1)$ of an integer. This has been shown by Tao [10] when the v_i's are at most $1.2n$. In [1], the lonely runner conjecture is shown when the v_i's are at most $2n - \epsilon(n)$, where $\epsilon(n)$ is of the shape $\exp(\mathcal{C}'(\log\log n)^2)$, for a positive constant $\mathcal{C}'$. Theorem 1 (more precisely, Proposition 1 below) has the analogous application: by the same argument as in [1], if $v_1 < v_2 < \cdots < v_n \leq 2n - c'(\log n)^2$, the lonely runner conjecture holds. It remains a challenge to show it when $\{v_1, v_2, \ldots, v_n\} \subset [2n]$, much less the full conjecture.

2. The Set-up

Recall the König–Hall "marriage" theorem, see [4, 6]. One version asserts that if I, J are sets with $|I|$ finite, and G is a bipartite graph between I and J, then G contains a matching of I into J if and only if for each $S \subset I$, S has at least $|S|$ neighbors in J. The Bohman–Peng paper uses the following version of this theorem.

Lemma 1. *If I, J are finite sets with $|I| = |J|$ and G is a bipartite graph from I to J, then G contains a perfect matching if and only if for each $S \subset I$ and $T \subset J$ with $|S| + |T| > |I|$, there is some $s \in S$ and $t \in T$ with $(s, t) \in G$.*

Proof. Since $|I| = |J| < \infty$, any matching from I into J is a perfect matching. Say there is no perfect matching, so by the König–Hall theorem, there is some $S \subset I$ which has fewer than $|S|$ neighbors in J. Let S' be the set of neighbors of S and let $T = J \setminus S'$. Then there is no edge $(s, t) \in G$ with $s \in S, t \in T$, yet $|S| + |T| > |S'| + |T| = m$. Conversely, suppose some $S \subset I, T \subset J$ with $|S| + |T| > m$ has no edge (s,t) with $s \in S, t \in T$. The neighbors of S are contained in $J \setminus T$, a set of cardinality $m - |T| < |S|$, so there is no perfect matching by the König–Hall theorem. $\square$

We say two integers s, t are 2-coprime if no odd prime divides both s and t, that is, $\gcd(s,t)$ is a power of 2. As in the Bohman–Peng paper, the problem can be reduced to the following.

Proposition 1. *There is a positive constant c such that if n is sufficiently large, $m > c(\log n)^2$, and $I, J \subset [n]$ are arithmetic progressions of length m with common difference 1 or 2, the following holds. Whenever $S \subset I$ and $T \subset J$ are nonempty, with $|S| + |T| \geq m$, there is a 2-coprime pair s, t with $s \in S$, $t \in T$.*

Corollary 1. *There is a bijection of I and J with corresponding numbers being 2-coprime.*

Proof. This follows immediately from Proposition 1 and Lemma 1. $\square$

As pointed out in [1], to use Lemma 1 it suffices to consider the case when $|S| + |T| > m$. The weaker hypothesis $|S| + |T| \geq m$ in Proposition 1 is useful when considering the application to the lonely runner problem.

Corollary 2. *With c the constant in Proposition 1, if n is sufficiently large, $m > c(\log n)^2$, and $I, J \subset [n]$ are intervals, then there is a coprime matching of I and J if either*

1. *I, J have length $2m$ or*

2. *I, J have length $2m + 1$ and the least elements of I, J have opposite parity.*

Proof. First suppose that I, J have length $2m$. Let I_0, J_0 be the even elements of I, J, respectively, and let I_1, J_1 be the odd elements. We have $|I_0| = |J_1| = m$ and $|I_1| = |J_0| = m$. Applying Corollary 1, there is a matching of I_0 and J_1 with corresponding elements being 2-coprime. But as elements of I_0 are all even and elements of J_1 are all odd, being 2-coprime implies being coprime. So the matching is a coprime one, and similarly for I_1 and J_0. Thus, we have the result in the first case. So suppose I, J have length $2m+1$ with least elements of the opposite parity. Then again we have $|I_0| = |J_1|$ and $|I_1| = |J_0|$, and the same proof works. $\square$

In particular, Theorem 1 holds. We can also say something in the remaining cases of two intervals of the same length.

Corollary 3. *With c the constant in Proposition 1, if n is sufficiently large, $m > 4c(\log n)^2$ and $I, J \subset [n]$ are intervals of length $2m+1$ with odd least elements, then there is a coprime matching from I to J. Further, if $m > 7c(\log n)^2$ and $I, J \subset [n]$*

are intervals of length $2m+1$ *with even least elements, then there is a matching from* I *to* J *such that corresponding elements, except for one pair, are coprime, with the offending pair having* gcd 2.

Proof. We abbreviate an interval of integers $\{u, u+1, \ldots, u+k\}$ as $[u, u+k]$. Say $I = [i, i+2m]$ and $J = [j, j+2m]$, where i, j are odd. Let a be the first odd number $\geq 2m/3$ and let $I_1 = [2i, 2i+a]$. By Theorem 1 there is a coprime matching from I_1 to $[j+a, j+2a]$. Let $j+a_1$ correspond to $2i$ in the matching, so that a_1 is even. By Theorem 1 there is a coprime matching from $[i+1, i+a_1]$ to $[j, j+a_1-1]$ and also a coprime matching from $[i+a_1+1, i+2m]$ to $[j+a_1+1, j+2m]$. With the coprime pair $i, j+a_1$ this shows there is a coprime matching from I to J.

The argument when $|I| = |J| = 2m+1$ with even least elements is similar. Now we match i with $j+a_2$, an even element in the middle third of J such that $(j+a_2)/2$ is coprime to i, with the rest of the argument being the same. To see that such a $j+a_2$ exists, we use Theorem 1 on the first one-sixth of the interval I, and one-half of the even numbers in the middle third of J. $\square$

2.1. Sketch of the Proof

The argument in [1] uses a result of Erdős [2] on the Jacobsthal function that implies that a long string of consecutive members of an arithmetic progression of common difference 1 or 2 has at least one member 2-coprime to a given integer s. We use instead a sequel result of Iwaniec [5] that implies that each $s \in S$ is 2-coprime to many elements of J, in fact, so many elements that we are done unless T is small enough to miss all of them. But T small forces S to be somewhat large, namely at least of magnitude $m/(\log m)^2$. At that point, an averaging argument comes into play. In particular, it is first shown that such a large set S has most members with a not-too-large "m part" (namely the largest squarefree divisor composed of odd primes up to m). This, coupled with the first argument shows that we may assume that $|S|$ is even larger, at least of magnitude $m/(\log\log m)^2$. A finer averaging argument now shows that for most $s \in S$ the value of $\varphi(s)/s$ is mostly determined by the primes $\leq \log m$ dividing s. A final averaging argument shows that many elements of S have $\varphi(s)/s$ not too small. Returning to the first thought of getting many members of J to be 2-coprime to s, we no longer need the Iwaniec result and can do a complete inclusion-exclusion, which allows us to complete the proof. This last step has some overlap with the approaches in [1] and [8].

3. The Proof of Proposition 1

Let φ denote Euler's function, and let $\omega(n)$ denote the number of different prime numbers that divide n. For $n > 2$ we have $\omega(n) = O(\log n/\log\log n)$. It is convenient to have a weaker, but explicit inequality: if $n > 1$, then $\omega(n) \le 2\log n$ (since $\omega(n)$ is at most the base-2 logarithm of n). Further, for $\omega(n) > 1$ and n odd, $n/\varphi(n) \le 3\log\omega(n)$. This follows from considering those n that are the product of the first $k \ge 2$ odd primes, using (3.5) and (3.30) from [9], and checking the small cases. In the proof $c_1, c_2, \dots$ are absolute, positive constants and it is assumed that n (and so m) is sufficiently large.

Assume the hypotheses of Proposition 1 hold. Let $S \subset I$, $T \subset J$ be nonempty subsets with $|S| + |T| \ge m$. We may assume that $|S| + |T| = m$ and $|S| \le |T|$. For any integer $k > 0$, let k_m denote the largest odd, squarefree divisor of k supported on the primes $\le m$. Since primes $> m$ can divide at most one element of J, if S contains an element s such that $s_m = 1$, then the number of elements of J that are not 2-coprime to s is at most $\omega(s) \le 2\log n = O(m^{1/2})$. Since $|T| \ge m/2$ there must be an element in T that is 2-coprime to s. Similarly, if $s_m = q^b$ where q is an odd prime $\le m$ and $b > 0$, then the number of elements of J that are not 2-coprime to s_m is $\le m/q + 1$ and so the number of elements not 2-coprime to s is $\le m/3 + O(m^{1/2})$. So again T must have an element 2-coprime to s.

From now on, we assume that each element of S is divisible by at least two different odd prime numbers $\le m$. Let $s \in S$. From [5], it follows that there is a positive constant c_1 such that an interval of length $c_1(s_m/\varphi(s_m))\omega(s_m)^2\log\omega(s_m)$ has $\ge \omega(s_m)^2$ integers coprime to s_m. If J has common difference 1, we apply this result directly to sub-intervals of J. If J has common difference 2 and $J \subset 2\mathbb{Z}$, we apply it to $\frac{1}{2}J$, while if $J \subset 2\mathbb{Z}+1$, we apply it to $\frac{1}{2}(J+M)$, where M is the product of all of the odd primes $\le m$. In all cases we thus have that for each string of $2c_1(s_m/\varphi(s_m))\omega(s_m)^2\log\omega(s_m)$ consecutive members of J, there are at least $\omega(s_m)^2$ integers coprime to s_m.

Note that s_m satisfies $s_m/\varphi(s_m) \le 3\log\omega(s_m)$ as remarked above. Thus, a string of length $6c_1(\omega(s_m)\log\omega(s_m))^2$ of consecutive members of J has at least $\omega(s_m)^2$ numbers coprime to s_m. Further, since $\omega(s_m) = O(\log s_m/\log\log s_m)$, we have $\omega(s_m)\log\omega(s_m) \le c_2\log s_m \le c_2\log n$ for some constant $c_2 > 0$. We let c in the theorem be $6c_1c_2^2$, so that J has at least 1 string of length $6c_1(\omega(s_m)\log\omega(s_m))^2$ of consecutive members. In particular, breaking J (or $\frac{1}{2}J$ in the case that $J \subset 2\mathbb{Z}$, or $\frac{1}{2}(J+M)$ in the case $J \subset 2\mathbb{Z}+1$) into consecutive strings of length $6c_1(\omega(s_m)\log\omega(s_m))^2$, we see that J contains $> (1/7c_1)m/(\log\omega(s_m))^2$ integers coprime to s_m. As above, s is divisible by at most $2\log n$ primes larger than m, and each of these primes divides at most one member of J. So J contains at least $(1/6c_1)m/(\log\omega(s_m))^2 - 2\log n$ numbers 2-coprime to s. Since $m > c(\log n)^2$ and $\omega(s_m) < 2\log n$, we have that there is a positive constant c_3 such that for each $s \in S$,

$$\sum_{\substack{j\in J\\ j\text{ 2-coprime to } s}} 1 \ge \frac{c_3 m}{(\log\omega(s_m))^2}. \tag{1}$$

Hence we may assume that $|T| \le m - c_3 m/(\log \omega(s_m))^2$, so that

$$|S| \ge c_3 m/(\log \omega(s_m))^2. \tag{2}$$

Now $\log \omega(s_m) \le \log(3 \log n)$ and $m > c(\log n)^2$ so that $\log\log n = O(\log m)$. Thus (2) implies that there is a positive constant c_4 with

$$|S| \ge c_4 m/(\log m)^2. \tag{3}$$

Lemma 2. *The number of integers $i \in I$ with $i_m > \exp((\log m)^4)$ is $O(m/(\log m)^3)$.*

Proof. We have

$$\sum_{i \in I} \log i_m = \sum_{2 < p \le m} \log p \sum_{\substack{i \in I \\ p \mid i}} 1 \le 2m \sum_{p \le m} \frac{\log p}{p} = O(m \log m),$$

by an inequality of Chebyshev. Thus, the lemma follows. □

Using (3), Lemma 2 implies that there is a member s of S with $s_m \le e^{(\log m)^4}$. Thus, by (2), we now can assume that there is a positive constant c_5 with

$$|S| \ge c_5 \frac{m}{(\log\log m)^2}. \tag{4}$$

Lemma 3. *The number of integers $i \in I$ with*

$$f(i) := \sum_{\substack{p \mid i \\ \log m < p \le m}} \frac{1}{p} > \frac{(\log\log m)^2}{\log m}$$

is at most $O(m/(\log\log m)^3)$.

Proof. We have

$$\sum_{i \in I} f(i) = \sum_{\log m < p \le m} \frac{1}{p} \sum_{\substack{i \in I \\ p \mid i}} 1 \le 2m \sum_{\log m < p \le m} \frac{1}{p^2} = O\left(\frac{m}{\log m \log\log m}\right).$$

The lemma follows. □

With Lemmas 2 and 3, (4) implies that there is a positive constant c_6 such that there are at least $(1 - c_6/\log\log m)|S|$ members s of S with $s_m \le e^{(\log m)^4}$ and $f(s) \le (\log\log m)^2/\log m$. For a positive integer k, let

$$k_0 = k_{\log m} = \prod_{\substack{p \mid k \\ 2 < p \le \log m}} p.$$

For any s as above, the number of members of J coprime to s_0 is

$$\sum_{d \mid s_0} \mu(d) \sum_{\substack{j \in J \\ d \mid j}} 1 \geq \sum_{d \mid s_0} \left(\mu(d) \frac{m}{d} - 1 \right) = \frac{\varphi(s_0)}{s_0} m - 2^{\omega(s_0)}.$$

Now $\omega(s_0) < \pi(\log m) = o(\log m)$, so that $2^{\omega(s_0)} = m^{o(1)}$, and on the other hand, $m\varphi(s_0)/s_0 = \Omega(m/\log\log m)$. Thus, J contains at least $0.99m\varphi(s_0)/s_0$ integers coprime to s_0. The number of members of J coprime to s_0 but not coprime to s_m is at most

$$\sum_{\substack{p \mid s \\ \log m < p \leq m}} \left(\frac{m}{p} + 1 \right) \leq 2mf(s).$$

Since $f(s) \leq (\log\log m)^2/\log m$, J contains at least $0.98m\varphi(s_0)/s_0$ integers coprime to s_m, and thus, as above, at least $0.97m\varphi(s_0)/s_0$ integers 2-coprime to s. And, as we have seen, this holds for at least $(1 - c_6/\log\log m)|S|$ members s of S.

We use the next result (cf. [8, Prop. 3]) to show that it is unusual for an element $i \in I$ to have $i_0/\varphi(i_0)$ large.

Lemma 4. *For m sufficiently large, we have*

$$\sum_{i \in I} \left(\frac{i_0}{\varphi(i_0)} - 1 \right) < \frac{3}{10} m.$$

Proof. We have

$$\frac{k}{\varphi(k)} = \sum_{d \mid k} \frac{\mu(d)^2}{\varphi(d)}.$$

Let P denote the product of the odd primes $p \leq \log m$. Thus,

$$\begin{aligned} \sum_{i \in I} \frac{i_0}{\varphi(i_0)} &= \sum_{i \in I} \sum_{d \mid i_0} \frac{\mu(d)^2}{\varphi(d)} = \sum_{d \mid P} \frac{1}{\varphi(d)} \sum_{\substack{i \in I \\ d \mid i}} 1 \\ &\leq \sum_{d \mid P} \frac{m/d + 1}{\varphi(d)} = m \sum_{d \mid P} \frac{1}{d\varphi(d)} + \sum_{d \mid P} \frac{1}{\varphi(d)} \\ &= m \prod_{p \mid P} \left(1 + \frac{1}{p(p-1)} \right) + \prod_{p \mid P} \frac{p}{p-1}. \end{aligned} \tag{5}$$

Note that

$$\prod_{p} \left(1 + \frac{1}{p(p-1)} \right) = \frac{\zeta(2)\zeta(3)}{\zeta(6)} < 1.944,$$

where ζ is the Riemann zeta-function. The first product in (5) is missing the prime 2, so it is $< (2/3)1.944 = 1.296$. Extending the second product in (5) over all integers in $[2, \log m]$, we see that it is $\leq \log m$. Thus,

$$\sum_{i \in I} \frac{i_0}{\varphi(i_0)} < 1.296m + \log m,$$

and the lemma follows for all sufficiently large m. $\square$

Corollary 4. *For all sufficiently large integers m and for any real number $t > 1$, the number of $i \in I$ with $i_0/\varphi(i_0) > t$ is at most $0.3m/(t-1)$.*

Proof. Let N denote the number of integers i in question. Lemma 4 implies that $N(t-1) < 3m/10$. $\square$

Let $r = m/|S|$, so that $r \geq 2$. We apply Corollary 4 with $t = 0.9r$, and we deduce that the number of $i \in I$ with $i_0/\varphi(i_0) > 0.9r$ is $\leq 0.3m/(0.9r-1) \leq 3m/(8r) = \frac{3}{8}|S|$. Thus, more than $\frac{5}{8}$ of the members s of S have $s_0/\varphi(s_0) \leq 0.9r$. Further, we have seen above that at least $(1 - c_6/\log\log m)|S|$ members s of S are 2-coprime to at least $0.97m\varphi(s_0)/s_0$ members of J. Thus, at least $(5/8 - c_6/\log\log m)|S|$ members s of S have this property and also $s_0/\varphi(s_0) \leq 0.9r$. Let s be one such element. There are at least $0.97m/(0.9r)$ elements j of J that are 2-coprime to s. Now $0.97m/(0.9r) > 1.07m/r = 1.07|S|$, and $|T| = m - |S|$. Thus some of these values of j must be in T, completing the proof of Proposition 1.

Acknowledgment. I am grateful to Tom Bohman and Mits Kobayashi for their comments.

References

[1] T. Bohman and F. Peng, Coprime mappings and lonely runners, arXiv:2109.09860 [math.NT], 26 pp.

[2] P. Erdős, On the integers relatively prime to n and on a number-theoretic function considered by Jacobsthal, *Math. Scand.* **10** (1962), 163–170.

[3] K. Ford. B. Green, S. Konyagin, J. Maynard, and T. Tao, Long gaps between primes, *J. Amer. Math. Soc.* **31** (2018), 65–105.

[4] P. Hall, On representatives of subsets, *J. London Math. Soc.* **10** (1935), 26–30.

[5] H. Iwaniec, On the problem of Jacobsthal, *Demonstratio Math.* **11** (1978), 225–231.

[6] D. König, Über Graphen und ihre Anwendung auf Determinantentheorie und Mengenlehre, *Math. Ann.* **77** (1916), 453–465.

[7] B. Larsen, H. Lehmann, A. Park, and L. Robertson, Coprime mappings on n-sets, *Integers* **17** (2017), A-51, 11 pp.

[8] C. Pomerance and J. L. Selfridge, Proof of D. J. Newman's coprime mapping conjecture, *Mathematika* **27** (1980), 69–83.

[9] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.* **6** (1962), 64–94.

[10] T. Tao, Some remarks on the lonely runner conjecture, *Contributions to Discrete Mathematics* **13** (2018), 1–31.