PATTERNS FOR CYCLIC NUMBERS

Carl Pomerance

Mathematics Department, Dartmouth College, Hanover, NH, USA
carlp@math.dartmouth.edu

Received: , Revised: , Accepted: , Published:

For Mel Nathanson on his eightieth birthday

Abstract

A positive integer n is called cyclic if there is only one group of order n up to isomorphism, and of course this group must be cyclic. Every prime number is cyclic, but there are many more cyclic numbers. It is perhaps natural to wonder if various notorious conjectures about primes might be provable for cyclics. This thought was taken up in a remarkable paper of Cohen, where a number of conjectures about cyclic numbers were raised. In this note we address a few of these conjectures, including an analogue of the twin prime conjecture and an analogue of Goldbach's conjecture.

1. Introduction

A number n is said to be cyclic if all groups of order n are isomorphic to a cyclic group of order n. The well-known criterion for n to be cyclic is that $\gcd(n, \varphi(n)) = 1$, where φ is Euler's function; see the venerable history of this result in [7]. Consider the set

$$\mathcal{N} = \{n : n = p^2 \text{ or } n = pq \text{ with } p \equiv 1 \pmod{q}\},$$

where p, q denote prime numbers. Evidently no member of $\mathcal{N}$ is cyclic, and it is easy to see that every number that is not cyclic is divisible by some member of $\mathcal{N}$.

Let $C(x)$ denote the number of cyclic numbers in $[1, x]$ and let

$$w(x) = e^\gamma \log\log\log x$$

for $x \geq 20$, where γ is Euler's constant. (For completeness, we let $w(x) = 1$ for $x < 20$.) We know after Erdős [3] that

$$C(x) \sim x/w(x), \quad x \to \infty.$$

(This old result was recently sharpened by Pollack [8].) The idea behind the proof is that most numbers n not divisible by any prime below $\log\log n$ are cyclic and most

numbers divisible by a prime below $\log\log n$ are not cyclic. The quantity $\log\log n$ is crucial here. It is shown in [4] that on a set of asymptotic density 1, $\gcd(n, \varphi(n))$ is the largest divisor of n composed solely of primes below $\log\log n$.

A number of interesting conjectures about cyclic numbers are raised in the new paper of Cohen [1]. Here we prove some of them. We first prove an asymptotic result for the distribution of *twin cyclics*, defined as a pair $n, n+2$ with both numbers cyclic. (Note that the only even cyclic number is 2.) The proof is similar to the proof of [7, Theorem 2.1].

In addition, we leverage the ideas in the proof to give an asymptotic for the number of representations of an even number as a sum of two cyclic numbers that is very similar to the conjectured asymptotic related to Goldbach's conjecture.

We also discuss various finite patterns that admit or do not admit infinitely many cases with all numbers being cyclic.

2. Twin Cyclics

Let $C_2(x)$ denote the number of cyclic numbers $n \le x$ such that $n+2$ is also cyclic. And let c_2 denote the twin-prime constant

$$c_2 = \prod_{p>2} \Big(1 - \frac{1}{(p-1)^2}\Big).$$

It is conjectured by Hardy and Littlewood [5, Eq. 5.311] that $P_2(x)$, the number of twin-primes up to x, is $\sim 2c_2x/(\log x)^2$. Here we prove an asymptotic formula for $C_2(x)$.

Theorem 1. *We have $C_2(x) \sim 2c_2x/w(x)^2$ as $x \to \infty$.*

Proof. Let $y = \log\log x$, let $\epsilon = 1/\log\log y$, and let M denote the product of the odd primes up to $y^{1+\epsilon}$. For the lower bound implicit in the theorem, we first estimate

$$C_2'(x) = \sum_{\substack{n\le x \\ \gcd(n(n+2),2M)=1}} 1.$$

By a complete inclusion-exclusion argument, $C_2'(x)$ is equal to

$$\sum_{\substack{n\le x \\ \gcd(n(n+2),2M)=1}} 1 = \sum_{d\mid M} \mu(d) \sum_{\substack{n\le x \\ n \text{ odd} \\ d\mid n(n+2)}} 1 = \sum_{d_1d_2\mid M} \mu(d_1d_2) \sum_{\substack{n\le x \\ n \text{ odd} \\ d_1\mid n,\, d_2\mid n+2}} 1,$$

where μ is the Möbius function. Since d_1d_2 is squarefree, the gcd of d_1, d_2 is 1, so the inner sum here is $\frac{1}{2}x/d_1d_2 + O(1)$ where the O-constant is uniform. Thus,

$$C_2'(x) = \frac{1}{2}x \sum_{d_1d_2\mid M} \frac{\mu(d_1d_2)}{d_1d_2} + O(3^{y^{1+\epsilon}}), \tag{1}$$

since the number of times we have the $O(1)$ to account for is the number of pairs d_1, d_2 with $d_1 d_2 \mid M$, which is $3^{\pi(y^{1+\epsilon})}$, with π the prime-counting function. (Each prime $p \mid M$ has 3 mutually exclusive choices: divide d_1, divide d_2, divide $M/d_1 d_2$.) By an elementary exercise, we have

$$\sum_{d_1 d_2 \mid M} \frac{\mu(d_1 d_2)}{d_1 d_2} = \sum_{d \mid M} \frac{\mu(d)}{d} \frac{\varphi(M/d)}{M/d} = \frac{\varphi(M)}{M} \sum_{d \mid M} \frac{\mu(d)}{\varphi(d)}$$
$$= \prod_{p \mid M} \Big(1 - \frac{1}{p}\Big)\Big(1 - \frac{1}{p-1}\Big) = \prod_{p \mid M} \Big(1 - \frac{1}{p}\Big)^2 \prod_{p \mid M} \Big(1 - \frac{1}{(p-1)^2}\Big).$$

The above display, Mertens' theorem, and the definition of c_2 imply that

$$\sum_{d_1 d_2 \mid M} \frac{\mu(d_1 d_2)}{d_1 d_2} \sim 4e^{-2\gamma} c_2/(\log y)^2 = 4c_2/w(x)^2, \quad x \to \infty.$$

Thus, from (1) we have $C_2'(x) \sim 2c_2 x/w(x)^2$ as $x \to \infty$.

For the lower bound it remains to show that very few such n do not have both n and $n+2$ cyclic; that is, that $C_2'(x) - C_2(x) = o(x/w(x)^2)$. Suppose the least prime factor of n exceeds $y^{1+\epsilon}$. If n is not cyclic, it must be divisible by some member of $\mathcal{N}$, so divisible by p^2 with $p > y^{1+\epsilon}$ or by some pq with $p \equiv 1 \pmod q$ and $q > y^{1+\epsilon}$. The number of $n \le x$ in the first category is at most

$$\sum_{p > y^{1+\epsilon}} \frac{x}{p^2} < \frac{x}{y^{1+\epsilon}} = o(x/w(x)^2).$$

For the second category we use the Brun–Titchmarsh inequality (see [6]) to sum $1/p$ over primes $p \equiv 1 \pmod q$, $2q < p \le x/q$, getting $\ll \log\log(x/q^2)/q < y/q$. Thus, the number of $n \le x$ in the second category is at most

$$\sum_{q > y^{1+\epsilon}} \sum_{\substack{p \equiv 1 \pmod q \\ 2q < p \le x/q}} \frac{x}{pq} \ll x \sum_{q > y^{1+\epsilon}} \frac{y}{q^2} < \frac{x}{y^\epsilon} = o(x/w(x)^2).$$

Thus, the number of $n \le x$ with $\gcd(n, 2M) = 1$ that are not cyclic is $o(x/w(x)^2)$. Similarly, the number of $n \le x$ with $\gcd(n+2, 2M) = 1$ that are not cyclic is $o(x/w(x)^2)$, so the number of $n \le x$ with $\gcd(n(n+2), 2M) = 1$ with either n or $n+2$ not cyclic is $o(x/w(x)^2)$. We thus conclude that

$$C_2(x) \ge (2c_2 + o(1))x/w(x))^2, \quad x \to \infty.$$

We now prove the upper bound implicit in the theorem. Let M' be the product of the odd primes $p \le y^{1-\epsilon}$. We will show that there are very few twin cyclics $n, n+2$ with $\gcd(n(n+2), 2M') > 1$ and by the arguments above, this will suffice.

Suppose that $q \mid n$ where $q \le y^{1-\epsilon}$. If $q \nmid \varphi(n)$, then n is not divisible by any prime $p \equiv 1 \pmod{q}$. Using item 2 on p. 4 of [7] we have that the number of such $n \le x$ is $\ll x/\exp(y/(q-1))$ where the implied constant is uniform. This expression is increasing in the variable q and so summing the inequality for $q \le y^{1-\epsilon}$ we arrive at the estimate $O(xy/e^{y^{\epsilon}})$ which is indeed small compared to $x/(w(x))^2$. Thus, we may assume that $\gcd(2M', n) = 1$ and by a parallel argument, we may assume that $\gcd(2M', n+2) = 1$. This completes the proof. □

3. A Goldbach Analogue

Theorem 1 proves that there are infinitely many twin cyclics, thus settling Conjecture 3 in Cohen [1]. Conjecture 2 in [1] asks for an analogue of Goldbach's conjecture, namely to show that every even natural number n is a sum of two cyclic numbers. We can at least prove that this holds if n is sufficiently large. Let $G(n)$ be the number of ordered pairs of cyclic numbers m_1, m_2 with $m_1 + m_2 = n$.

Theorem 2. *For n even,*

$$G(n) \sim \frac{2c_2 n}{w(n)^2} \prod_{\substack{p \mid n \\ 2<p<\log\log n}} \frac{p-1}{p-2}, \quad n \to \infty.$$

Proof. We sketch the proof since it is very similar to the proof of Theorem 1. With the notation from that proof, we first estimate the number of pairs m_1, m_2 of positive integers with $m_1 + m_2 = n$ and $m_1 m_2$ coprime to $2M$. Here, n is a given large even number. The count is exactly

$$\sum_{\substack{m<n \\ (m(n-m),2M)=1}} 1 = \sum_{\substack{d_0 \mid (M,n) \\ d_1 d_2 \mid M/(n,M)}} \mu(d_0)\mu(d_1)\mu(d_2) \sum_{\substack{m<n \text{ odd} \\ d_0 d_1 \mid m \\ d_2 \mid n-m}} 1.$$

The inner sum here is $n/(2d_0d_1d_2) + O(1)$, so the count is

$$\frac{n}{2} \sum_{\substack{d_0 \mid (M,n) \\ d_1 d_2 \mid M/(M,n)}} \frac{\mu(d_0)\mu(d_1)\mu(d_2)}{d_0 d_1 d_2} + O(2^{y^{1+\epsilon}} 3^{y^{1+\epsilon}}).$$

The sum over d_0 is $\varphi((M,n))/(M,n)$ and the sum over d_1, d_2 proceeds as in the proof of Theorem 1. Thus, the count is

$$\begin{aligned} &\frac{n}{2} \prod_{p \mid (M,n)} \Big(1 - \frac{1}{p}\Big) \prod_{p \mid M/(M,n)} \Big(1 - \frac{1}{p}\Big)^2 \Big(1 - \frac{1}{(p-1)^2}\Big) + O(6^{y^{1+\epsilon}}) \\ &= \frac{n}{2} \prod_{p \mid (M,n)} \frac{p-1}{p-2} \prod_{p \mid M} \Big(1 - \frac{1}{p}\Big)^2 \Big(1 - \frac{1}{(p-1)^2}\Big) + O(6^{y^{1+\epsilon}}). \end{aligned}$$

At this point it remains to count the numbers $m < n$ which satisfy the above conditions with not both $m, n-m$ cyclic. This is seen, as in the proof of Theorem 1, to be negligible in comparison. For the upper bound implicit in the theorem one again appeals to the argument in the proof of Theorem 1 to see that there are very few pairs of cyclics that sum to n and have a prime factor below $y^{1-\epsilon}$. Further, the count of pairs $m, n-m$ which are coprime to the primes up to $y^{1-\epsilon}$ is seen in analogy to the above argument to be asymptotic to the same expression as in the theorem statement. □

The product in the theorem is $\ll w(n)$ so that $n/w(n)^2 \ll G(n) \ll n/w(n)$ for n even.

4. *k*-tuples

The proof of Theorem 1 can be easily further generalized to count cyclic integers n with $n+j$ also cyclic, where j is an arbitrary even number. If $C_j(x)$ is the number of such $n \le x$, then we have, for $j \neq 0$, j even and fixed,

$$C_j(x) \sim \frac{2c_2 x}{w(x)^2} \prod_{\substack{p \mid j \\ 2<p<\log\log x}} \frac{p-1}{p-2}, \quad x \to \infty,$$

a formula which might be compared with [5, Conjecture B], which deals with prime pairs p, $p+j$. In fact, the later discussion in [5] deals with prime k-tuplets, where it is asked for $n+a_1, \ldots, n+a_k$ to be simultaneously prime infinitely often when $\{a_1, \ldots, a_k\}$ is an *admissible* set, meaning it does not contain a complete residue system modulo any prime. The analogue for cyclic numbers has us replace powers of $\log x$ with like powers of $w(x)$ and the singular series only involves primes to $\log\log x$. With cyclic numbers these are theorems, not just conjectures.

For example, the above ideas can show that the number of $n \le x$ with $n, n+2, n+6$ all cyclic is

$$\sim \frac{9c_3 x}{2w(x)^3}, \quad x \to \infty, \qquad \text{where } \; c_3 = \prod_{p>3} \Big(1 - \frac{3p-1}{(p-1)^3}\Big).$$

Precisely the same asymptotics hold for $n, n+4, n+6$.

Also note that if $a_1 < \cdots < a_k$ form an admissible set, then there are infinitely many n such that not only is each $n+a_i$ cyclic, but the k cyclic numbers are consecutive in the sequence of cyclic numbers. This can be proved by subtracting the various cases where there are intervening cyclic numbers, which have counts that are small compared with the initial count where being consecutive is not considered.

These thoughts go through for other linear patterns, such as the "Sophie Germain" pattern $n, 2n+1$. There are infinitely many cyclic numbers n with $2n+1$

also cyclic (this is Cohen's Conjecture 36, see [1]), in fact the number of such $n \le x$ is $\sim cx/w(x)^2$ for an appropriate positive constant c.

It is interesting that in all of the cases discussed so far, one can insist that the cyclic numbers in the patterns are composite cyclics. With k linear functions, the counting function for all of them being simultaneously cyclic (assuming admissibility) is a constant times $x/w(x)^k$, while if we insist one of them is prime, we have an upper bound of $O(x/w(x)^{k-1}\log x)$, which is asymptotically negligible in comparison.

While being admissible is essential when dealing with primes, this is not so with cyclics. For example, one can prove there are infinitely many cyclic triples $n, n+2, n+4$ (Cohen's Conjecture 4), even though $\{0,2,4\}$ is not admissible (it is a complete residue system modulo 3). However, the count for $n \le x$ is not of order $x/w(x)^3$ but the much smaller expression $x/w(x)^{5/2}(\log x)^{1/2}$. An asymptotic constant can be worked out using the above ideas plus the work in [2]. This particular pattern is based on the fact that the number of cyclic numbers up to x divisible by 3 is a constant times $x/(w(x)\log x)^{1/2}$, since we not only sieve by the primes up to $\log\log x$ but also by all primes up to x congruent to 1 (mod 3).

These thoughts are relevant to another conjecture in [1]. For $j = 1, 2, 3$, let $G_j(x)$ denote the number of cyclic numbers $n \le x$ with $n \equiv j \pmod 3$ and $2n+1$ also a cyclic number. If $n \equiv 2 \pmod 3$, then $2n+1 \equiv 2 \pmod 3$, so $G_2(x)$ is asymptotically a constant times $x/w(x)^2$. But the other two cases for j have one of $n, 2n+1$ divisible by 3, so $G_j(x)$ in these cases is a constant times $x/w(x)^{3/2}(\log x)^{1/2}$, and in fact the same constant. Thus, all 3 cases occur infinitely often but asymptotically 100% of Sophie Germain cyclic pairs $n, 2n+1$ have $n \equiv 2 \pmod 3$. This settles Cohen's Conjecture 37.

Not every pattern is "cyclic admissible". For example, there are just two cyclic numbers n with $n+1$ also cyclic, namely $n = 1, 2$. Here is a criterion for a linear pattern to represent infinitely many cyclic numbers: *The pattern is all odd infinitely often and has no complete residue system modulo m for every $m \in \mathcal{N}$.*

For example, $n, n+2, n+4, n+6, n+8, n+10, n+12, n+14$ represents infinitely many cyclic 8-tuples, but throwing in $n+16$, one of the numbers is divisible by 9, so is not cyclic.

It would be nice to show in relation to Theorem 2 that *every* even $n > 0$ is the sum of two cyclic numbers, and probably this is doable. Somewhat more difficult are some of the short-interval conjectures in [1]. For example, it is conjectured there that there is always a cyclic number between consecutive squares.

Acknowledgment. I thank Joel Cohen for his interest in this work and for his encouragement.

References

[1] J. E. Cohen, Conjectures about primes and cyclic numbers, preprint, 2025.

[2] T. Dence and C. Pomerance, Euler's function in residue classes, *Ramanujan J.* **2** (1998), 7–20.

[3] P. Erdős, Some asymptotic formulas in number theory, *J. Indian Math. Soc. (N.S.)* **12** (1948), 75–78

[4] P. Erdős, F. Luca, and C. Pomerance, On the proportion of numbers coprime to a given integer, Proceedings of the Anatomy of Integers Conference, Montreal, March 2006, J.-M. De Koninck, A. Granville, F. Luca, eds., *CRM Proceedings and Lecture Notes* **46** (2008), 47–64.

[5] G. H. Hardy and J. E. Littlewood, Some problems of 'Partitio Numerorum'; III: On the expression of a number as a sum of primes, *Acta Math.* **44** (1923), 1–70.

[6] H. L. Montgomery and R. C. Vaughan, The large sieve, *Mathematika* **20** (1973), 119–134.

[7] R. Nedela and C. Pomerance, Density of singular pairs of integers, *Integers* **18** (2018), paper A82, 7 pp.

[8] P. Pollack, Numbers which are orders only of cyclic groups, *Proc. Amer. Math. Soc.* **150** (2022), 515–524.