DIRICHLET'S THEOREM AND JACOBSTHAL'S FUNCTION

Idris Mercer
Department of Mathematics and Statistics, Florida International University, Miami, Florida
imercer@fiu.edu

Received: 3/21/17, Accepted: 3/13/18, Published: 3/23/18

Abstract

If a and d are relatively prime, we refer to the set of integers congruent to a mod d as an 'eligible' arithmetic progression. A theorem of Dirichlet says that every eligible arithmetic progression contains infinitely many primes; the theorem follows from the assertion that every eligible arithmetic progression contains at least one prime. The Jacobsthal function $g(n)$ is defined as the smallest positive integer such that every sequence of $g(n)$ consecutive integers contains an integer relatively prime to n. In this paper, we show by a combinatorial argument that every eligible arithmetic progression with $d \leq 76$ contains at least one prime, and we show that certain plausible bounds on the Jacobsthal function of primorials would imply that every eligible arithmetic progression contains at least one prime. That is, certain plausible bounds on the Jacobsthal function would lead to an elementary proof of Dirichlet's theorem.

1. Introduction

By an *arithmetic progression*, we mean any set of the form

$$a + d\mathbb{Z} = \{a + dn \mid n \in \mathbb{Z}\}$$

where a is an integer and d is a positive integer. For example,

$$2 + 7\mathbb{Z} = 9 + 7\mathbb{Z} = -5 + 7\mathbb{Z} = \{\ldots, -12, -5, 2, 9, 16, \ldots\}.$$

Note that $a + 1\mathbb{Z} = \mathbb{Z}$ is an example of an arithmetic progression, and note that any arithmetic progression $a + d\mathbb{Z}$ is equal to $a' + d\mathbb{Z}$ for some $a' \in \{0, \ldots, d-1\}$. We will sometimes abbreviate 'arithmetic progression' by 'AP'.

We say that the arithmetic progression $a + d\mathbb{Z}$ is *eligible* if a and d are relatively prime. This is equivalent to the condition that all elements of $a + d\mathbb{Z}$ are relatively prime to d.

Although our arithmetic progressions contain negative integers, we will use the word *prime* only for positive primes. We let p_k denote the kth prime, so we have

$$p_1 = 2, \qquad p_2 = 3, \qquad p_3 = 5, \qquad p_4 = 7, \qquad p_5 = 11, \qquad \ldots$$

Proposition 1 below is known to hold for all positive integers d, and the statement that it holds for all d implies Dirichlet's theorem. The usual proofs of Dirichlet's theorem involve functions of a complex variable (specifically, Dirichlet L-functions). Later, we will provide a combinatorial proof that Proposition 1 holds for all $d \leq 76$, and we will show how certain plausible bounds on the Jacobsthal function would lead to a combinatorial proof that Proposition 1 holds for all d.

Proposition 1. *If $a + d\mathbb{Z}$ is an eligible arithmetic progression, then $a + d\mathbb{Z}$ contains at least one prime.*

Proposition 2. *The statement that Proposition 1 holds for all positive integers d implies that every eligible arithmetic progression contains infinitely many primes (i.e., Dirichlet's theorem).*

Proof of Proposition 2. Let $a + d\mathbb{Z}$ be an eligible AP, and by Proposition 1, let p be a prime in $a + d\mathbb{Z}$. Notice that $a + d\mathbb{Z}$ is the disjoint union of $a + 2d\mathbb{Z}$ and $(a + d) + 2d\mathbb{Z}$, which are eligible APs. Let $a' + 2d\mathbb{Z}$ be the one of those APs not containing p. Then, applying Proposition 1 to $a' + 2d\mathbb{Z}$, we conclude there exists a prime $p' \in a' + 2d\mathbb{Z} \subset a + d\mathbb{Z}$, i.e., there is a prime $p' \neq p$ in $a + d\mathbb{Z}$. Next, we can write $a' + 2d\mathbb{Z}$ as the disjoint union of the two eligible APs $a' + 4d\mathbb{Z}$ and $(a' + 2d) + 4d\mathbb{Z}$. Applying Proposition 1 to the one of those APs not containing p', we can conclude there exists a prime p'' distinct from p and p' in a subset of $a + d\mathbb{Z}$. Continuing in this way, we get an infinite sequence of distinct primes in $a + d\mathbb{Z}$. $\square$

We now define primorials and the Jacobsthal function.

Definition. We define the *primorial* of the nth prime to be

$$p_n\# = \prod_{k=1}^{n} p_k$$

so for example, we have $p_1\# = 2$, $p_2\# = 6$, $p_3\# = 30$, $p_4\# = 210$, $\ldots$

Definition. If n is a positive integer, then the *ordinary Jacobsthal function* $g(n)$ is defined to be the smallest positive integer m such that among any m consecutive integers, there is always at least one that is coprime to n.

Example. To determine $g(10)$, note that an integer is coprime to 10 if and only if it is congruent to 1, 3, 7, or 9 mod 10. Thus the longest sequence of consecutive integers that are *not* coprime to 10 would be a sequence of the form $4 + 10n, 5 +$

$10n, 6+10n$, so any sequence of 4 or more consecutive integers must contain at least one integer that is coprime to 10. Therefore $g(10) = 4$.

Definition. If n is a positive integer, then the *primorial Jacobsthal function* is defined by

$$h(n) = g(p_n\#).$$

So for example, $h(1) = g(2)$, $h(2) = g(2\cdot 3)$, $h(3) = g(2\cdot 3\cdot 5)$, and so on.

Example. To bound $h(5) = g(2\cdot 3\cdot 5\cdot 7\cdot 11)$, we first observe that

$$114, 115, 116, \ldots, 125, 126$$

are 13 consecutive integers none of which are coprime to $2\cdot 3\cdot 5\cdot 7\cdot 11$. Next, if we exhaustively check all integers from 1 to $2\cdot 3\cdot 5\cdot 7\cdot 11 = 2310$, we find that the above is the longest such sequence, i.e., any sequence of 14 consecutive integers must contain an integer coprime to 2310. Thus $h(5) = 14$. (Note that since $p_n\#$ is a rapidly increasing function of n, naive exhaustive search is not necessarily the best way to calculate $h(n)$ in general.)

Other authors have explored upper and lower bounds for the functions $g(n)$ and $h(n)$. Such bounds can be expressed either in terms of n or of p_n. An elementary argument shows $h(n) \geq 2p_{n-1}$, and work of Rankin [7], Maier and Pomerance [5], and Pintz [6] leads to lower bounds of the form

$$h(n) \geq C \cdot \frac{p_n \log p_n \log\log\log p_n}{(\log\log p_n)^2}$$

(see Section 1 of [2]). As for upper bounds for $h(n)$, Iwaniec [3] showed

$$h(n) \leq C \cdot (n \log n)^2$$

for an unknown constant C. Recalling that the Prime Number Theorem implies $p_n \sim n \log n$, this is equivalent to $h(n) \leq C \cdot p_n^2$.

It has been conjectured that better upper bounds on $h(n)$ are possible. It was shown in [1] that

$$h(n) \leq 0.27749612254 \cdot n^2 \log n$$

for all n from 50 to 10,000. Upper bounds smaller than $h(n) = O(p_n^2)$ have interesting consequences. It was shown in [4] that a bound of the form

$$h(n) \leq C \cdot p_n^{2-\varepsilon}$$

that holds for all n would lead to a short proof of Linnik's theorem and Dirichlet's theorem. In Section 2, we will show that if $h(n)$ satisfies the weaker bound

$$h(n) = o(p_n^2),$$

for example, if $h(n) = O(p_n^2/\log p_n)$ or $h(n) = O(p_n^2/\log\log p_n)$, this would lead to a short proof of Dirichlet's theorem.

2. Main Result

To achieve our main result (Theorem 1), it is convenient to establish some definitions and state some lemmas.

Definition. A *segment* of an arithmetic progression $X = a + d\mathbb{Z}$ is any subset of X of the form

$$\{a_1, a_1 + d, \dots, a_1 + (k-1)d\}$$

where $a_1 \in X$. We refer to k as the *length* of the segment. For example, $\{-5, 1, 7, 13\}$ is a segment of $1 + 6\mathbb{Z}$ (of length 4), but $\{-5, 1, 13\}$ is not a segment of $1 + 6\mathbb{Z}$.

Definition. An *isomorphism* between two arithmetic progressions X and Y is an order-preserving bijection, i.e., a bijection $\varphi : X \to Y$ such that $\varphi(x) < \varphi(x')$ if and only if $x < x'$.

If φ is a function from X to Y, and $Y' \subseteq Y$, then as is standard, we define $\varphi^{-1}(Y')$ to be the set of all $x \in X$ such that $\varphi(x) \in Y'$. It is straightforward to verify the following.

Proposition 3. *Suppose X and Y are arithmetic progressions and suppose φ is an isomorphism from X to Y. If Y' is a segment of Y of length k, then $\varphi^{-1}(Y')$ is a segment of X of length k.*

Definition. If c is a fixed element of $a + d\mathbb{Z}$, then we define the function $\Phi_{c,d}$ from $\mathbb{Z}$ to $a + d\mathbb{Z}$ by

$$\Phi_{c,d}(n) = c + dn.$$

If the value of d is clear from context, we may write $\Phi_c = \Phi_{c,d}$.

It is straightforward to verify the following.

Proposition 4. *If c is any fixed element of $a + d\mathbb{Z}$, then $\Phi_{c,d}$ is an isomorphism from $\mathbb{Z}$ to $a + d\mathbb{Z}$.*

Example. Two different isomorphisms from $\mathbb{Z}$ to $3 + 5\mathbb{Z}$ are $\Phi_3 = \Phi_{3,5}$ and $\Phi_{18} = \Phi_{18,5}$. They are illustrated below.

n	$\Phi_3(n)$	$\Phi_{18}(n)$
-3	-12	3
-2	-7	8
-1	-2	13
0	3	18
1	8	23
2	13	28
3	18	33

Notice that we have, for example,

$$\Phi_3^{-1}(\{3,8,13,18\}) = \{0,1,2,3\},$$
$$\Phi_{18}^{-1}(\{3,8,13,18\}) = \{-3,-2,-1,0\}.$$

Definition. Let S be a finite set of primes. We say that an isomorphism φ from $\mathbb{Z}$ to $a+d\mathbb{Z}$ is *S-good* if the implication

$$n \text{ coprime to all primes in } S \Longrightarrow \varphi(n) \text{ coprime to all primes in } S$$

is true for all $n \in \mathbb{Z}$. By a slight abuse of notation, we will sometimes write, e.g., $2{\cdot}3{\cdot}5$-good rather than $\{2,3,5\}$-good.

Lemma 1. *If $a+d\mathbb{Z}$ is any eligible arithmetic progression and S is any finite set of primes, then there is an S-good isomorphism from $\mathbb{Z}$ to $a+d\mathbb{Z}$.*

Proof. Let $q_1,\ldots,q_k$ be all the primes in S not dividing d. Since $d,q_1,\ldots,q_k$ are mutually coprime, the Chinese Remainder Theorem says there exists an integer c satisfying all the congruences

$$\begin{aligned} c &\equiv a \mod d,\\ c &\equiv 0 \mod q_1,\\ &\vdots\\ c &\equiv 0 \mod q_k. \end{aligned}$$

Note that then $c \in a+d\mathbb{Z}$ so $c+d\mathbb{Z} = a+d\mathbb{Z}$. We claim that $\Phi_c = \Phi_{c,d}$ is the desired S-good isomorphism. To see this, let $n \in \mathbb{Z}$, and suppose n is coprime to all primes in S. We must show $\Phi_c(n) = c+dn$ is coprime to all primes in S. Let $p \in S$. If $p \mid d$, then $p \nmid c+dn$ since $c+d\mathbb{Z} = a+d\mathbb{Z}$ is an eligible arithmetic progression. If $p \nmid d$, then $p \mid c$ by construction, and also $p \nmid n$, so $p \nmid c+dn$. $\square$

Example. If $S = \{2,3\}$, the following are S-good isomorphisms from $\mathbb{Z}$ to the eligible arithmetic progressions with $d = 3$ or 4.

$\Phi_{4,3}$ is a $2{\cdot}3$-good isomorphism from $\mathbb{Z}$ to $1+3\mathbb{Z}$
$\Phi_{2,3}$ is a $2{\cdot}3$-good isomorphism from $\mathbb{Z}$ to $2+3\mathbb{Z}$
$\Phi_{9,4}$ is a $2{\cdot}3$-good isomorphism from $\mathbb{Z}$ to $1+4\mathbb{Z}$
$\Phi_{3,4}$ is a $2{\cdot}3$-good isomorphism from $\mathbb{Z}$ to $3+4\mathbb{Z}$

In Table 1, there are boxes around all numbers coprime to 6, illustrating that for each of these isomorphisms $\Phi_{c,d}$, if n is coprime to all primes in $\{2,3\}$ then $\Phi_{c,d}(n)$ is also coprime to all primes in $\{2,3\}$, i.e., each of these isomorphisms is $2{\cdot}3$-good.

As another example, consider $S = \{2,3,5\}$ and $a+d\mathbb{Z} = 1+7\mathbb{Z}$. Since $120 \equiv 1 \mod 7$ and $2{\cdot}3{\cdot}5 \mid 120$, the function defined by $\Phi(n) = 120+7n$ is a $2{\cdot}3{\cdot}5$-good isomorphism from $\mathbb{Z}$ to $1+7\mathbb{Z}$.

n	$\Phi_{4,3}(n)$	$\Phi_{2,3}(n)$	$\Phi_{9,4}(n)$	$\Phi_{3,4}(n)$
-6	-14	-16	-15	-21
$\boxed{-5}$	$\boxed{-11}$	$\boxed{-13}$	$\boxed{-11}$	$\boxed{-17}$
-4	-8	-10	$\boxed{-7}$	$\boxed{-13}$
-3	$\boxed{-5}$	$\boxed{-7}$	-3	-9
-2	-2	-4	$\boxed{1}$	$\boxed{-5}$
$\boxed{-1}$	$\boxed{1}$	$\boxed{-1}$	$\boxed{5}$	$\boxed{-1}$
0	4	2	9	3
$\boxed{1}$	$\boxed{7}$	$\boxed{5}$	$\boxed{13}$	$\boxed{7}$
2	10	8	$\boxed{17}$	$\boxed{11}$
3	$\boxed{13}$	$\boxed{11}$	21	15
4	16	14	$\boxed{25}$	$\boxed{19}$
$\boxed{5}$	$\boxed{19}$	$\boxed{17}$	$\boxed{29}$	$\boxed{23}$
6	22	20	33	27
$\boxed{7}$	$\boxed{25}$	$\boxed{23}$	$\boxed{37}$	$\boxed{31}$
8	28	26	$\boxed{41}$	$\boxed{35}$

Table 1: Examples of $2{\cdot}3$-good isomorphisms

Lemma 2. *Suppose n is an integer such that $2 \leq n < p_{k+1}^2$ and n is coprime to $p_k\#$. Then n is prime.*

Proof. Since $n \geq 2$, we know n has at least one prime factor. If n is not prime, then n is a product of two or more primes, but those primes must be $\geq p_{k+1}$, which would imply $n \geq p_{k+1}^2$. $\square$

Theorem 1. *Let d be a positive integer. If there exists a positive integer k such that*

$$\frac{p_{k+1}^2 - 2}{h(k)+1} \geq d$$

then every eligible arithmetic progression $a + d\mathbb{Z}$ contains at least one prime.

Proof. Let $X = \{2, \ldots, p_{k+1}^2 - 1\}$. Partition X as

$$X = X_0 \cup \cdots \cup X_{d-1},$$

where for each $a = 0, \ldots, d-1$, we define

$$X_a = \{n \in X \mid n \equiv a \pmod{d}\}.$$

Then for each a, the set X_a is a segment of $a + d\mathbb{Z}$ of length $\geq \lfloor (p_{k+1}^2 - 2)/d \rfloor$. Now suppose $a + d\mathbb{Z}$ is an eligible AP, and let $S = \{2, 3, 5, \ldots, p_k\}$. By Lemma 1, there is an S-good isomorphism Φ from $\mathbb{Z}$ to $a+d\mathbb{Z}$. Since X_a is a segment of $a+d\mathbb{Z}$, we conclude that $Y=\Phi^{-1}(X_a)$ is a segment of $\mathbb{Z}$, and we have

$$|Y| \geq \left\lfloor \frac{p_{k+1}^2-2}{d} \right\rfloor \geq \frac{p_{k+1}^2-2}{d} - 1.$$

By hypothesis, this implies $|Y| \geq h(k)$. We conclude that Y contains at least one integer m that is coprime to $p_k\#$. Then, since Φ is S-good, we conclude that $\Phi(m) \in X_a$ is coprime to $p_k\#$. Since $\Phi(m) \in X_a \subseteq X = \{2, \dots, p_{k+1}^2-1\}$, Lemma 2 says $\Phi(m)$ is prime. That is, the eligible AP $a+d\mathbb{Z}$ must contain at least one prime. □

Corollary 1. *If $d \leq 76$, then every eligible arithmetic progression $a+d\mathbb{Z}$ contains at least one prime. That is, Proposition 1 holds for all $d \leq 76$.*

Proof. In [8], values of $h(n)$ are computed for $n \leq 54$, improving upon [2] which computes $h(n)$ for $n \leq 49$. We find that

$$\frac{p_{55}^2-2}{h(54)+1} = \frac{257^2-2}{858+1} > 76,$$

so the result follows from Theorem 1. □

Corollary 2. *Suppose* $\lim_{n\to\infty} h(n)/p_{n+1}^2 = 0$ *(which is the case if, for example, $h(n) \leq C \cdot p_{n+1}^2/\log p_{n+1}$ or $h(n) \leq C \cdot p_{n+1}^2/\log\log p_{n+1}$). Then every eligible arithmetic progression contains at least one prime, i.e., Proposition 1 holds for all d.*

Proof. If $\lim_{n\to\infty} h(n)/p_{n+1}^2 = 0$, then $\lim_{n\to\infty} p_{n+1}^2/h(n) = \infty$, and then also

$$\lim_{n\to\infty} \frac{p_{n+1}^2-2}{h(n)+1} = \lim_{n\to\infty} \frac{p_{n+1}^2}{h(n)} \cdot \frac{p_{n+1}^2-2}{p_{n+1}^2} \cdot \frac{h(n)}{h(n)+1} = \infty$$

so for every d, there exists k with $(p_{k+1}^2-2)/(h(k)+1) \geq d$. The result follows. □

Remark. Known values of $h(k)$ appear to give support to the conjecture that $(p_{k+1}^2-2)/(h(k)+1)$ grows without bound. This is illustrated below.

k	p_{k+1}	$h(k)$	$(p_{k+1}^2-2)/(h(k)+1)$
5	13	14	11.133
10	31	46	20.404
15	53	100	27.792
20	73	174	30.440
25	101	258	39.378
30	127	330	48.722
35	151	432	52.654
40	179	538	59.442
45	199	642	61.585
50	233	762	71.149

References

[1] F. Costello and P. Watts, An upper bound on Jacobsthal's function, *Math. Comp.* **84** (2015), 1389–1399.

[2] T.R. Hagedorn, Computation of Jacobsthal's function $h(n)$ for $n < 50$, *Math. Comp.* **78** (2009), 1073–1087.

[3] H. Iwaniec, On the error term in the linear sieve, *Acta Arith.* **19** (1971), 1–30.

[4] H.-J. Kanold, Über Primzahlen in arithmetischen Folgen. II, *Math. Ann.* **157** (1965), 358–362.

[5] H. Maier and C. Pomerance, Unusually large gaps between consecutive primes, *Trans. Amer. Math. Soc.* **322** (1990), 201–237.

[6] J. Pintz, Very large gaps between consecutive primes, *J. Number Theory* **63** (1997), 286–301.

[7] R.A. Rankin, The difference between consecutive prime numbers, *J. London Math. Soc.* **4** (1938), 242–247.

[8] M. Ziller and J.F. Morack, Algorithmic concepts for the computation of Jacobsthal's function, `arXiv:1611.03310v2` (2017).