#A65 INTEGERS 16 (2016)

EVALUATIONALLY COPRIME LINEAR POLYNOMIALS

Randell Heyman
School of Mathematics and Statistics, University of New South Wales, Sydney, New South Wales, Australia
randell@unsw.edu.au

Received: 3/2/16, Revised: 6/13/16, Accepted: 8/6/16, Published: 8/26/16

Abstract

Two polynomials $f, g \in \mathbb{Z}[x]$ are *evaluationally coprime at x* if $\gcd(f(x), g(x)) = 1$. We give necessary and sufficient conditions for two such linear polynomials to have a positive proportion of evaluated coprime values.

1. Introduction

A natural extension of the greatest common divisor of two polynomials is to consider the greatest common divisor of the evaluation of the two polynomials at a particular value. This then leads to the concept of polynomials $f, g \in \mathbb{Z}[x]$ that are evaluationally coprime. That is, $\gcd(f(x), g(x)) = 1$ for all $x \in \mathbb{Z}$. We can extend this line of enquiry to tuples of evaluationally pairwise coprime polynomials; that is, $f_1, \dots, f_n$ such that for any $1 \leq i < j \leq n$ we have $\gcd(f_i(x), f_j(x)) = 1$ for all $x \in \mathbb{Z}$.

Denote the greatest common divisor of integers $a_1, \dots a_n$ by $(a_1, \dots, a_n)$. Recently, Knox, McDonald and Mitchell [1] examined pairs of polynomials $f, g \in \mathbb{Z}[x]$ that have greatest common divisors equal to 1, and have greatest common divisors equal to 1 when evaluated at every integer value. In [1, Corollary 3.5] necessary and sufficient conditions are given for two primitive linear polynomials to exhibit both of these conditions. The main result of the present paper, Theorem 1 below, gives necessary and sufficient conditions for the less demanding result that a positive proportion of evaluated values are coprime. Unlike the proof in [1], the proof of Theorem 1 does not use the resultant.

Theorem 1. *Suppose* $f(x) = ax + b,\ g(x) = cx + d, \quad a, b, c, d \in \mathbb{Z},\ a, c \neq 0$. *Then*

$$\liminf_{N\to\infty} \frac{1}{2N+1} \left|\{x : (f(x), g(x)) = 1, -N \leq x \leq N\}\right| > 0$$

if, and only if,

$$(a, b, c, d) = 1 \text{ and } ad \neq bc.$$

2. Preparation

We use the following GCD algorithm ('the algorithm'). Given two polynomials $a_1x + b_1,\ a_2x + b_2 \in \mathbb{Z}[x]$ with $a_1 \geq a_2 > 0$ we let

$$a_ix + b_i = e_{i+1}(a_{i+1}x + b_{i+1}) + a_{i+2}x + b_{i+2},\ i = 1, 2, \ldots, \tag{1}$$

where e_{i+1} is the largest integer such that $e_{i+1}a_{i+1} \leq a_i$. So $a_i \geq a_{i+1} > a_{i+2} \geq 0$. The algorithm terminates when $a_{i+2} = 0$. Let m be this value $i+2$. So the algorithm terminates when $a_m = 0$. We note that for any $x \in \mathbb{Z}$ and for any $1 \leq i, j \leq m - 1$ we have

$$(a_ix + b_i, a_{i+1}x + b_{i+1}) = (a_jx + b_j, a_{j+1}x + b_{j+1}).$$

We simplify the last part of the algorithm by denoting $a_{m-1} = u,\ b_{m-1} = v$ and $b_m = s$. So we can write

$$(ax + b, cx + d) = (ux + v, s). \tag{2}$$

To prove Theorem 1, we require three simple lemmas, below.

Lemma 1. *Let $u, v, s \in \mathbb{Z}$. We have $(xu + v, s) = ((x + s)u + v, s)$ for all $x \in \mathbb{Z}$.*

Proof. Fix $x \in \mathbb{Z}$. Let $g_1 = (xu + v, s), g_2 = ((x + s)u + v, s)$. We have $g_1|su$ so $g_1|(x + s)u + v$; hence $g_1|g_2$. Similarly, $g_2|su$ so $g_2|xu + v$; hence $g_2|g_1$. So $g_1 = g_2$ as required. □

Lemma 2. *Suppose by comparing the first and last line of the algorithm we have, as shown in* (2)*,*

$$(ax + b, cx + d) = (ux + v, s). \tag{3}$$

Then $(a, c) = u$ and $(b, d) = (v, s)$.

Proof. Recalling the algorithm, we have

$$a_ix + b_i = e_{i+1}(a_{i+1}x + b_{i+1}) + a_{i+2}x + b_{i+2},\ i = 1, 2, \ldots m - 2.$$

Setting $x = 0$ and then $x = 1$ we have

$$b_i = e_{i+1}b_{i+1} + b_{i+2}, \quad a_i + b_i = e_{i+1}(a_{i+1} + b_{i+1}) + a_{i+2} + b_{i+2}$$

respectively. Subtracting equations we obtain

$$a_i = e_{i+1}a_{i+1} + a_{i+2},$$

where e_{i+1} is the biggest integer such that $e_{i+1}a_{i+1} \leq a_i$. This is Euclid's algorithm for integers. Thus $(a_i, a_{i+1}) = (a_{i+1}, a_{i+2})$. Since this applies for any i it follows that $(a_1, a_2) = (a_{m-1}, 0) = a_{m-1}$. Letting $a_1 = a,\ a_2 = c$ and recalling that $a_{m-1} = u$ concludes the proof that $(a, c) = u$. Setting $x = 0$ in (3) yields $(b, d) = (v, s)$ which completes the proof. □

Lemma 3. *Let $a, b, c, d \in \mathbb{Z}$. We have $(a, b, c, d) = ((a, b), (c, d))$.*

Proof. Let $g_1 = (a, b, c, d), g_2 = ((a, c), (b, d))$. We have g_1 divides both (a, c) and (b, d), so $g_1 | g_2$. Similarly, $g_2 | g_1$. So $g_1 = g_2$ as required. □

3. Proof of Theorem

Suppose $f(x) = ax + b,\ g(x) = cx + d, \quad a, b, c, d \in \mathbb{Z},\ a, c \neq 0$. Without loss of generality we will assume that $a \geq c$.

To prove sufficiency suppose firstly that $(a, b, c, d) = j \neq 1$. Then for all $x \in \mathbb{Z}$ we have $j|(ax + b)$ and $j|(cx + d)$, which implies that $j|(ax + b, cx + d)$, and so $(ax + b, cx + d) > 1$. Therefore

$$\liminf_{N\to\infty} \frac{1}{2N+1} \big|\{x : (f(x), g(x)) = 1, -N \leq x \leq N\}\big| = 0.$$

Alternately, if $ad = bc$ then, since $a, c \neq 0$, we have $a/c = b/d$. Thus $a = kc, b = kd$ for some $k \in \mathbb{Q}, k \geq 1$. So $f(x) = kg(x)$ and the termination line of the algorithm will be $(f(x), g(x)) = (ux + v, 0)$, for some $u \in \mathbb{N}, v \in \mathbb{Z}$.

Since $(xu + v, 0) = xu + v$ for all $x \in \mathbb{Z}$, the sequence $(u + v, 0), (2u + v, 0), \ldots,$ is monotonic. It follows that

$$\liminf_{N\to\infty} \frac{1}{2N+1} \big|\{x : (f(x), g(x)) = 1, -N \leq x \leq N\}\big| = 0.$$

To prove necessity suppose that $(a, b, c, d) = 1$ and $ad \neq bc$. Since $ad \neq bc$ then, as argued above, the right-hand side of the termination line of the algorithm must be

$$(ux + v, s), \text{ for some } u \in \mathbb{Z}, s \neq 0. \tag{4}$$

Using Lemma 1 we see that the sequence $(u + v, s), (2u + v, s), \ldots$ has maximum period s. So it will suffice to show that for some $x \in \mathbb{Z}$ we have $(xu + v, s) = 1$, for then

$$\liminf_{N\to\infty} \frac{1}{N} \big|\{x : (f(x), g(x)) = 1, -N \leq x \leq N\}\big| \geq \frac{1}{s} > 0.$$

We may assume $(u, v, s) = 1$ for otherwise, by Lemmas 2 and 3, we have $((b, d), (a, c)) = ((u, v), s) \neq 1$ which contradicts our supposition that $(a, b, c, d) = 1$. Let s have the following prime factorisation

$$s = \prod_{\substack{p|s \\ p\nmid uv}} p^{\alpha} \times \prod_{\substack{p|s \\ p|uv}} p^{\alpha} := x \times y,$$

where α for each prime p is such that $p^\alpha | s$ and $p^{\alpha+1} \nmid s$. Clearly $(x, y) = 1$. We are going to show that for this x, $(xu+v, s) = 1$. Suppose not and p is a prime dividing $(xu + v, s)$. Then, since $p|s$, either $p|x$ or $p|y$.

If $p|x$ then $p|(v, s)$, but this implies that $p|y$ and this contradicts $(x, y) = 1$.

If $p|y$ then either $p|u$ or $p|v$. If $p|u$ then $p|(v, s)$ and this contradicts $(x, y) = 1$. If $p|v$ then $p|xu$ and hence $p|u$ because $(x, y) = 1$. Hence we have $p|(u, v, s)$ and this contradicts $(u, v, s) = 1$.

So for some $x \in \mathbb{Z}$ we have $(xu + v, s) = 1$ which concludes the proof.

4. Comments

There are two lines of enquiry that naturally follow from Theorem 1. Firstly, suppose we have (not necessarily linear) integer coefficient polynomials f and g. What are necessary and sufficient coefficient conditions such that

$$\liminf_{N\to\infty} \frac{1}{N} \left|\{x : (f(x), g(x)) = 1, -N \le x \le N\}\right| > 0?$$

Secondly, suppose we have linear integer coefficient polynomials, $f_1, \ldots, f_n$. What are necessary and sufficient coefficient conditions such that

$$\liminf_{N\to\infty} \frac{1}{N} \left|\{x : (f_1(x), \ldots, f_n(x)) = 1, -N \le x \le N\}\right| > 0?$$

Acknowledgements. The author thanks Adrian Dudek for posing the question that resulted in Theorem 1, in a project unrelated to [1]. The author thanks Gerry Myerson for some views on results in this area and Thomas Britz for some useful comments Finally, the author thanks an anonymous referee that pointed out that the claim that $(xu + v, s) = 1$ for some $x \in \mathbb{Z}$ could be proved without resorting to Dirichlet's theorem on arithmetic progressions [2].

References

[1] M. L. Knox, T. McDonald and P. Mitchell. Evaluationally relatively prime polynomials, *Notes on Number Theory and Discrete Mathematics.* **21** (2015), 36-41.

[2] P. G. L. Dirichlet. Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält, *Abhand. Ak. Wiss.* **48** (1837), 45-81.