Notes on Number Theory and Discrete Mathematics
ISSN 1310–5132
Vol. 21, 2015, No. 1, 36–41

Evaluationally relatively prime polynomials

Michelle L. Knox, Terry McDonald and Patrick Mitchell

Department of Mathematics, Midwestern State University
Wichita Falls, TX 76308, USA
emails: michelle.knox@mwsu.edu,
terry.mcdonald@mwsu.edu,
patrick.mitchell@mwsu.edu

Abstract: Two polynomials from $\mathbb{Z}[x]$ are called evaluationally relatively prime if the greatest common divisor of the two polynomials in $\mathbb{Z}[x]$ is 1 and $gcd(f(t), g(t)) = 1$ for all $t \in \mathbb{Z}$. A characterization is given for when a linear function is evaluationally relatively prime with another polynomial.
Keywords: Relatively prime, Polynomials, Resultant.
AMS Classification: 11C08.

1 Introduction

Suppose two polynomials are relatively prime. In this case we write $GCD(f, g) = 1$. In reality the 1 signifies a zero degree polynomial. One might ask: if we evaluate the two polynomials at a common integer, is the resulting pair of integers relatively prime. For example, let $f(x) = x^2 + 1$ and $g(x) = x^2 - 1$. Now $f(x)$ is irreducible over $\mathbb{Z}[x]$, thus $GCD(f(x), g(x)) = 1$. If we evaluate these polynomials at $x = 3$, we get

$$gcd(f(3), g(3)) = gcd(10, 8) = 2,$$

a pair of integers that are not relatively prime. Moreover, we can find polynomials $F(x), G(x) \in \mathbb{Z}[x]$ such that $f(x)F(x) + g(x)G(x) = 2$. In particular $F(x) = 1$ and $G(x) = -1$. Writing $f(x)$ and $g(x)$ in this linear combination is a result from the following well-known theorem. Results like this theorem can be found in [1] and [2].

Theorem 1.1. *Given any two polynomials $f(x)$ and $g(x)$ over $\mathbb{Q}$, not both identically zero, there corresponds a unique monic polynomial $d(x) \in \mathbb{Q}[x]$ such that*

(a) $d(x)|f(x)$ *and* $d(x)|g(x)$*,*

(b) $d(x)$ *is a linear combination of* $f(x)$ *and* $g(x)$*, and*

(c) any common divisor of $f(x)$ *and* $g(x)$ *is a divisor of* $d(x)$*, therefore there are no divisors having a higher degree than that of* $d(x)$*.*

We will be focusing our attention on $\mathbb{Z}[x]$, and since $\mathbb{Z}[x]$ is a GCD domain we have the previous theorem holding true when $\mathbb{Q}$ is replaced by $\mathbb{Z}$. The polynomial d in the above theorem is called the greatest common divisor of f and g. We write $d = GCD(f, g)$. The GCD is to signify that we are talking about the greatest common divisor in a polynomial sense. We will use lower case gcd when referring to the greatest common divisor in the integer sense.

Suppose f is a polynomial of degree n and g is a polynomial of degree m (both in $\mathbb{Z}[x]$). The Sylvester matrix of f and g is an $n + m$ square matrix whose entries consist of coefficients from f, coefficients from g, and zeros. For example, if $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = cx + d$, then the Sylvester matrix $S(f, g)$ is an $n + 1$ square matrix that looks like this:

$$S(f,g) = \begin{bmatrix} a_n & c & 0 & \cdots & 0 \\ a_{n-1} & d & c & & \vdots \\ \vdots & 0 & d & & \\ a_1 & \vdots & \vdots & & c \\ a_0 & 0 & 0 & \cdots & d \end{bmatrix}.$$

The resultant, denoted $Res(f, g)$, is the determinant of $S(f, g)$. In fact, in the special case above where g is a linear function, we will have $Res(f, g) = \sum_{i=0}^{n} a_i c^{n-i}(-d)^i$. It is well-known that there exist polynomials $F(x), G(x) \in \mathbb{Z}[x]$ such that $f(x)F(x) + g(x)G(x) = Res(f, g)$. Information on the resultant can be found in [3].

2 The set up

This brings us to the main question we would like to explore. What property must two polynomials have in order to ensure that: (1) they are relative prime in the polynomial sense, and (2) if we evaluate them at any integer value the resulting pair of integers are also relatively prime. Let us define the property that we are interested in exploring.

Definition 2.1. We will say that $f, g \in \mathbb{Z}[x]$ are *evaluationally relatively prime* (ERP) if $GCD(f, g) = 1$ and $gcd(f(t), g(t)) = 1$ for all $t \in \mathbb{Z}$.

One immediate observation is that the constant coefficients must be relatively prime. If not, then $f(0)$ and $g(0)$ would have a common factor greater than one.

Proposition 2.2. Let $f, g \in \mathbb{Z}[x]$. If $f(0)$ and $g(0)$ are not relatively prime, then f and g are not ERP.

Suppose that $f, g \in \mathbb{Z}[x]$ and $GCD(f, g) = 1$. By Theorem 1.1 we can find polynomials $F, G \in \mathbb{Q}[x]$ such that $f(x)F(x)+g(x)G(x) = 1$. By clearing the denominators of the coefficients of F and G, we can make $F, G \in \mathbb{Z}[x]$ and thus have $f(x)F(x)+g(x)G(x) = k$, for some $k \in \mathbb{Z}$.

Lemma 2.3. Suppose that $f, g \in \mathbb{Z}[x]$, $t \in \mathbb{Z}$, and $GCD(f, g) = 1$. Now there exists polynomials $F, G \in \mathbb{Z}[x]$ and $k \in \mathbb{Z}$ such that $f(x)F(x) + g(x)G(x) = k$. If $d_t = gcd(f(t), g(t))$, then $d_t|k$.

Proof. We have $f(t)F(t) + g(t)G(t) = k$ for any $t \in \mathbb{Z}$. Now $d_t|f(t)$ and $d_t|g(t)$, thus $d_t|k$. □

Lemma 2.4. Suppose $f, g \in \mathbb{Z}[x]$ and $GCD(f, g) = 1$. Now there exists $F, G \in \mathbb{Z}[x]$ such that $f(x)F(x) + g(x)G(x) = k$ for some $k \in \mathbb{Z}$. If $k = 1$, then f and g are ERP.

Proof. Suppose $k = 1$, then $f(t)F(t) + g(t)G(t) = 1$ for all $t \in \mathbb{Z}$. Let $d_t = gcd(f(t), g(t))$, by lemma 2.3, $d_t|k$. So f and g are ERP. □

It is natural to wonder if the converse of the previous lemma is true, thus giving a complete characterization of two polynomials that are evaluationally relatively prime. However the following example demonstrates that the converse is indeed false.

Let $f(x) = 3x + 4$ and $g(x) = 3x + 1$. First we establish that f and g are ERP. Note that for any $t \in \mathbb{Z}$, $f(t)$ and $g(t)$ have opposite parity. Therefore 2 cannot divide both $f(t)$ and $g(t)$. Next note that $f(x) \equiv g(x) \equiv 1 \pmod 3$, thus 3 does not divide $f(t)$ or $g(t)$ for any $t \in \mathbb{Z}$. Since $f(t) - g(t) = 3$, no prime greater than 3 can divide both $f(t)$ and $g(t)$. Hence f and g are ERP. Now if we write f and g in the form cited in lemma 2.3, we have

$$f(x)F(x) + g(x)G(x) = 3,$$

where $F(x) = 1$ and $G(x) = -1$.

3 The main results

Since the previous proposition and lemmas fall short of fully classifying when two polynomials are ERP, we will now take a step back. We will begin by classifying when two linear functions have this property.

Proposition 3.1. Let $f(x) = ax + 1$ and $g(x) = cx + 1$ where $a, c \in \mathbb{Z}$ with $a < c$. Let $a = q_1^{m_1}...q_j^{m_j}$ and $c-a = p_1^{n_1}...p_l^{n_l}$ be prime factorizations. Let $B = \{p_1, ..., p_l\}$ and $A = \{q_1, ..., q_j\}$. Then f and g are ERP if and only if $B \subseteq A$.

Proof. First suppose $B \subseteq A$. Let $t \in \mathbb{Z}$ and let $p \in \mathbb{Z}$ be a prime dividing $f(t)$. Then p does not divide a or t, so $p \notin A$ and thus $p \notin B$. It follows that p does not divide $c - a$. Hence p does not divide $[(at + 1) + (c - a)t]$, i.e., p does not divide $g(t)$. Thus f and g are ERP.

Conversely, assume $B \not\subseteq A$, say $p_i \in B \setminus A$. Since $gcd(p_i, a) = 1$, the equation $(ax+1) \equiv 0 \pmod{p_i}$ has a solution k. Since $p_i|(ak+1)$ and $p_i \in B$, $p_i|[(ak+1)+(c-a)k]$, that is, $p_i|g(k)$. Thus $p_i|gcd(f(k), g(k))$ and we conclude that f and g are not ERP. □

In the next proposition we will add the condition that f is a primitive polynomial. This allows us to keep track of common factors and will play an important role in many of the following results. Note if a polynomial is not primitive, then the coefficients have a common factor. This common factor will always divide the result of the polynomial evaluated at any integer.

Proposition 3.2. Let $a, b, c \in \mathbb{Z}$ such that $a \neq 0$, $c \neq 0$ and $gcd(b, c) = 1$. Suppose $f(x) = ax + b$ and $g(x) = c$ where f is a primitive polynomial. Then f and g are ERP if and only if $gcd(a, c) \neq 1$.

Proof. If $gcd(a, c) = 1$, then the equation $ax + b \equiv 0 \pmod{c}$ has a solution, call it k. Hence $f(k) = ak + b$ and $g(k) = c$ are both divisible by c, and so f and g are not ERP. If $gcd(a, c) \neq 1$, then since f is primitive we know that the equation $ax + b \equiv 0 \pmod{c}$ does not have a solution. Thus f and g are ERP. □

Lemma 3.3. *Let $a_n, a_{n-1}, ..., a_1, a_0, c, d \in \mathbb{Z}$, $n \geq 1$, and let $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = cx+d$ be primitive polynomials. If $p|Res(f, g)$ and $p|c$, then $p|a_n$.*

Proof. If $p|c$, then since $p|Res(f, g)$ and

$$Res(f, g) = \sum_{i=0}^{n} a_i c^{n-i}(-d)^i = c\left[\sum_{i=0}^{n-1} a_i c^{n-i-1}(-d)^i\right] + a_n(-d)^n,$$

we know p also divides $a_n(-d)^n$. But g is primitive, so $p \nmid d$ and hence $p|a_n$. □

Note that Lemma 3.3 could be stated as: if p is a prime dividing $Res(f, g)$, then either $p|gcd(a_n, c)$ or $p \nmid c$. This form will be applied in the proofs of the following results.

Theorem 3.4. *Let $a_n, a_{n-1}, ..., a_1, a_0, c, d \in \mathbb{Z}$ such that $a_n, a_0, c, d \neq 0$, $n \geq 1$, and $gcd(a_0, d) = 1$. Let $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = cx + d$ both be primitive polynomials.*

1. *If $gcd(a_n, c) = 1$, then f and g are ERP if and only if $|Res(f, g)| = 1$.*
2. *If $gcd(a_n, c) \neq 1$, then let $gcd(a_n, c) = p_1^{n_1} p_2^{n_2} ... p_s^{n_s}$ be the prime factorization of $gcd(a_n, c)$. Then f and g are ERP if and only if $|Res(f, g)| = p_1^{j_1} ... p_s^{j_s}$ for some $j_1, j_2, ..., j_s \in \mathbb{N} \cup \{0\}$.*

Before we prove this theorem, we would like to discuss the following corollary.

Corollary 3.5. *Let $a_1, a_0, c, d \in \mathbb{Z}$ such that $a_1, a_0, c, d \neq 0$ and $gcd(a_0, d) = 1$. Let $f(x) = a_1 x + a_0$ and $g(x) = cx + d$ both be primitive polynomials.*

1. *If $gcd(a_1, c) = 1$, then f and g are ERP if and only if $|a_1 d - a_0 c| = 1$.*
2. *If $gcd(a_1, c) \neq 1$, then let $gcd(a_1, c) = p_1^{n_1} p_2^{n_2} ... p_s^{n_s}$ be the prime factorization of $gcd(a_1, c)$. Then f and g are ERP if and only if $|a_1 d - a_0 c| = p_1^{m_1} ... p_s^{m_s}$ for some $m_1, m_2, ..., m_s \in \mathbb{N} \cup \{0\}$.*

Corollary 3.5. is a special case of Theorem 3.4 for two primitive linear functions. When proving this corollary, we notice that clearly f and g are ERP if $|Res(f,g)| = 1$. Otherwise, if there exists a prime q dividing $Res(f,g)$ and $q \nmid gcd(a_1, c)$, by lemma 3.3 we know $q \nmid c$. In this linear case, however, we can say even more: $q \nmid c$ and $q \nmid a_1$. To see this, notice if q divides $Res(f,g)$ and q divides a_1, then q divides $a_0 c$. But f(x) is primitive, hence q divides c. It follows that if $q|Res(f,g)$ and $q \nmid gcd(a_1, c)$, then $q \nmid a_1$ and $q \nmid c$. Thus a_1^{-1} and c^{-1} both exist modulo q and the following equivalences are satisfied:

$$\begin{aligned} a(-a^{-1}b) + b &\equiv 0 \pmod{q} \text{ and} \\ c(-c^{-1}d) + d &\equiv 0 \pmod{q} \end{aligned}$$

where

$$-a^{-1}b \equiv -c^{-1}d \pmod{q}.$$

These equivalences provide a value $k = -dc^{-1}$ such that $f(k)$ and $g(k)$ are both divisible by q. This approach for linear functions is the motivation for the following proof of Theorem 3.4.

Proof. Recall that we can write $Res(f,g) = f(x)F(x)+g(x)G(x)$. It follows that $gcd(f(t), g(t))$ divides $Res(f,g)$ for all $t \in \mathbb{Z}$.

First assume that $gcd(a_n, c) = 1$. If $|Res(f,g)| = 1$, then $gcd(f(t), g(t)) = 1$ for all $t \in \mathbb{Z}$ and so f and g are ERP. Next suppose there exists a prime dividing $Res(f,g)$, say q. By Lemma 3.3, we know $q \nmid c$. So let c^{-1} be an inverse of c modulo q. Let $k = -dc^{-1}$, then k is a solution to $cx + d \equiv 0 \pmod{q}$. Moreover, k is a solution to $f(x) \equiv 0 \pmod{q}$ since

$$\begin{aligned} f(k) &\equiv a_n(-dc^{-1})^n + ... + a_1(-dc^{-1}) + a_0 \\ &\equiv c^{-n}[a_n(-d)^n + a_{n-1}(-d)^{n-1}c + ... + a_1(-d)c^{n-1} + a_0 c^n] \\ &\equiv c^{-n} Res(f,g) \\ &\equiv 0 \pmod{q} \end{aligned}$$

So let $k = -dc^{-1}$, then both $f(k)$ and $g(k)$ are divisible by q. Hence f and g are not ERP.

Next assume that $gcd(a_n, c) \neq 1$. Suppose that $|Res(f,g)| = p_1^{j_1}...p_s^{j_s}$ for some $j_1, j_2, ..., j_s \in \mathbb{N} \cup \{0\}$. Assume, by way of contradiction, that f and g are not ERP, say q is a prime dividing $gcd(f(r), g(r))$ for some $r \in \mathbb{Z}$. Since $q \in \{p_1, ..., p_s\}$, we know $q|a_n$ and $q|c$. Since q also divides $g(r)$, q must also divide d. However, g is primitive, a contradiction. Thus f and g are ERP.

Conversely, suppose that there exists a prime q such that q divides $|Res(f,g)|$ but $q \notin \{p_1, ..., p_s\}$. In particular, $q \nmid gcd(a_n, c)$. So by Lemma 3.3, $q \nmid c$. Again let $k = -dc^{-1}$, then k is a solution to $cx + d \equiv 0 \pmod{q}$. The same argument as above yields that k is a solution to $f(x) \equiv 0 \pmod{q}$. So both $f(k)$ and $g(k)$ are divisible by q. Therefore f and g are not ERP. □

Theorem 3.4. classifies when a nonconstant linear function and a polynomial are evaluationally relatively prime. Recall that if $gcd(a,b) = 1$ and $gcd(a,c) = 1$, then the $gcd(a, bc) = 1$.

Therefore, if f and g are ERP and f and h are ERP, then we have that f and $g \cdot h$ are ERP. This gives a method of constructing two polynomials that are evaluationally relatively prime. In addition, given two polynomials one can determine if they are evaluationally relatively prime provided that at least one of the polynomials is the product of linear terms over $\mathbb{Z}[x]$.

References

[1] Cohn, P. M. (2000) *An Introduction to Ring Theory*, Springer, London.

[2] Niven, I., Zuckerman, H., & Montgomery. H. (1991) *An Introduction to The Theory of Numbers, 5th edition*, John Wiley & Sons, Inc.

[3] Prasolov, V. (2004) Polynomials, *Algorithms and Computation in Mathematics Vol. 11*, Springer-Verlag, Berlin.