Polynomials and Primes

William Gasarch *

Univ. of MD at College Park

1 Introduction

If f is a polynomial is it possible that an infinite number of $f(0), f(1), f(2), \ldots$ are prime? It is well known that if $f \in Z[x]$ then the answer is no. We show this result for $f \in \mathsf{Q}[x]$ and also for $f \in \mathsf{C}[x]$. We then discuss what happens over other domains and also what happens with two variables. None of what we present is original.

We remind the reader that if p is a prime then $-p$ is a prime. More generally, there are three kinds of numbers: (1) units, which have multiplicative inverses (just $-1, 1$ in Z), (2) primes, numbers such that if $p = ab$ then one of a, b is a unit, (3) composites, numbers that are neither prime nor units.

2 Polynomials in $\mathsf{Z}[x]$

Theorem 2.1 *Let $f(x) = \sum_{L=0}^{d} a_L x^L$ be a polynomial over Z. If there exists $y \in \mathsf{Z}$ such that for all $0 \le m \le 2(d-1)$, $f(y + mf(y))$ $f(x)$ is prime then $f(x)$ is constant.*

Proof:

Let $0 \le m \le 2(d-1)$.

*University of Maryland, College Park, MD 20742, gasarch@cs.umd.edu

$$f(y+mf(y)) = \sum_{L=0}^{d} a_L(y+mf(y))^L = \sum_{L=0}^{d} a_L \sum_{i=0}^{L} \binom{L}{i}(mf(y))^i y^{L-i} = \sum_{L=0}^{d} a_L(y^L+\sum_{i=1}^{L} \binom{L}{i}(mf(y))^i) =$$

$$\sum_{L=0}^{d} a_L y^L + \sum_{L=0}^{d}\sum_{i=1}^{L} a_L \binom{L}{i}(mf(y))^i) = f(y)+f(y)(\sum_{L=0}^{d}\sum_{i=1}^{L} a_L \binom{L}{i} m^i f(y)^{i-1}) \equiv 0 \pmod{f(y)}$$

Hence, for all $0 \le m \le 2d-2$, $f(y)$ divides $f(y+mf(y))$. Since both $f(y)$ and $f(y+mf(y))$ are prime $f(y+mf(y)) \in \{-f(y), f(y)\}$. Hence for $d+1$ values of m we must have that $f(f(y)+mf(y))$ is the same. Since f is of degree $\le d$, f must be constant. ∎

Corollary 2.2 *Let $f(x) \in \mathsf{Z}[x]$. There are an infinite number of $y \in \mathsf{Z}$ such that $f(y)$ is not prime.*

Can we actually *find* a y such that $f(y)$ is not prime?

Theorem 2.3

1. *There exists an deterministic algorithm that will, on input $f(x) = \sum_{L=0}^{d} a_L x^L$, determine a y such that $f(y)$ is not prime. The algorithm takes $2d-1$ evaluations of f.*

2. *There exists a randomized algorithm that will, on input $f(x) = \sum_{L=0}^{d} a_L x^L$, determine a y such that $f(y)$ is not prime. The algorithm takes 1 evaluation of f and has failure probability $\frac{1}{2d-2}$.*

Proof:

1) Compute $f(1+mf(1))$ as $m = 0, 1, \ldots, 2d-2$ until you get a non prime. By Theorem 2 this algorithm works.

2) Pick a random $0 \le m \le (2d-1)^2$ and evaluate it. If it's not prime then you succeed, if not then you fail. By a slight modification of Theorem 2 at most $2d-2$ of the m will fail, so the probability of failure is $\frac{2d-2}{(2d-2)^2} = \frac{1}{2d-2}$.

∎

Open Question: Is there a better deterministic algorithm in terms of number of evaluations. Note that since the model of computation is just number-of-evals lower bounds may be possible.

Note 2.4 The above can all be adjusted to find y such that $f(y)$ is composite (so not -1,1) with slightly worse bounds.

3 Polynomials in $\mathsf{D}[x]$

What is is about Z that made the proof of Theorem 2 work? The only property of Z that we used was that it had a finite number of units. In this section proof we proof an analog of Theorem 2 for such integral domains.

Throughout this section D is an integral domain with a finite number of units. We denote the set of units U.

The following theorem is from Steven Weintraub's article [2].

Theorem 3.1 *Let $f(x) = \sum_{L=0}^{d} a_L x^L$ be a polynomial over D. If there exists $y \in \mathsf{Z}$ such that for all $0 \le m \le |U|(d-1)$, $f(y + mf(y))$ $f(x)$ is prime then $f(x)$ is constant.*

Proof:

Let $0 \le m \le |U|(d-1)$.

$$f(y{+}mf(y)) = \sum_{L=0}^{d} a_L (y{+}mf(y))^L = \sum_{L=0}^{d} a_L \sum_{i=0}^{L} \binom{L}{i} (mf(y))^i y^{L-i} = \sum_{L=0}^{d} a_L (y^L {+} \sum_{i=1}^{L} a_L \binom{L}{i} (mf(y))^i) =$$

$$\sum_{L=0}^{d} a_L y^L {+} \sum_{L=0}^{d} \sum_{i=1}^{L} a_L \binom{L}{i} (mf(y))^i) = f(y){+}f(y)(\sum_{L=0}^{d} \sum_{i=1}^{L} a_L \binom{L}{i} m^i f(y)^{i-1}) \equiv 0 \pmod{f(y)}$$

Hence, for all $0 \le m \le 2d-2$, $f(y)$ divides $f(y+mf(y))$. Since both $f(y)$ and $f(y+mf(y))$ are prime $f(y+mf(y)) \in \{uf(y) : u \in U\}$. Hence for $d+1$ values of m we must have that $f(f(y)+mf(y))$ is the same. Since f is of degree $\le d$, f must be constant. ∎

Corollary 3.2 *Let $f(x) \in \mathsf{D}[x]$. There are an infinite number of $y \in \mathsf{D}$ such that $f(y)$ is not prime.*

The following has a proof similar to that of Theorem 2.3, and has similar open questions related to it.

Theorem 3.3

1. *There exists an deterministic algorithm that will, on input $f(x) = \sum_{L=0}^{d} a_L x^L$, determine a y such that $f(y)$ is not prime. The algorithm takes $|U|(d-1)$ evaluations of f.*
2. *There exists a randomized algorithm that will, on input $f(x) = \sum_{L=0}^{d} a_L x^L$, determine a y such that $f(y)$ is not prime. The algorithm takes 1 evaluation of f and has failure probability $\frac{1}{|U|(d-1)}$.*

Note 3.4 The above can all be adjusted to find y such that $f(y)$ is composite (so not a unit with slightly worse bounds.

4 Polynomials in $\mathsf{Q}[x]$

Is there a version of Theorem 2 for Q? There is!

Let $\omega(B)$ be the number of distinct prime divisors of B.

Theorem 4.1 *Let $f(x) = \sum_{L=0}^{d} \frac{a_L}{b_L} x^L$ be a polynomial over Q. Let $B = LCM(b_0, \ldots, b_L)$. If there exists $y_1, \ldots, y_{\omega(B)+1} \in \mathsf{Z}$ such that for all $0 \le m \le 2(d-1)$, $f(y+mf(y))$ $f(x)$ is prime then $f(x)$ is constant.*

Proof:

Let $y \in \{y_1, \ldots, y_{\omega(B)+1}$. Let $0 \le m \le 2(d-1)$.

$$f(y+mf(y)) = \sum_{L=0}^{d} \frac{a_L}{b_L}(y+mf(y))^L = \sum_{L=0}^{d} \frac{a_L}{b_L} \sum_{i=0}^{L} \binom{L}{i} (mf(y))^i y^{L-i} = \sum_{L=0}^{d} \frac{a_L}{b_L}(y^L + \sum_{i=1}^{L} \binom{L}{i} (mf(y))^i) =$$

$$\sum_{L=0}^{d} \frac{a_L}{b_L} y^L + \sum_{L=0}^{d} \sum_{i=1}^{L} \frac{a_L}{b_L} \binom{L}{i} (mf(y))^i) = f(y) + f(y)(\sum_{L=0}^{d} \sum_{i=1}^{L} \frac{a_L}{b_L} \binom{L}{i} m^i f(y)^{i-1}) = f(y)(1+(\sum_{L=0}^{d} \sum_{i=1}^{L} \frac{a_L}{b_L} \binom{L}{i}$$

The right hand side has fractions in it so we cannot say anything about divisibility. We multiply both sides to B to clear fractions and obtain

$$Bf(y+mf(y)) = f(y)(B + (\sum_{L=0}^{d} \sum_{i=1}^{L} \frac{a_L B}{b_L} \binom{L}{i} m^i f(y)^{i-1}))$$

Since B, $f(y+mf(y))$, $f(y)$, and $(B+\cdots)$ are all in Z, and $f(y+mf(y))$ and $f(y)$ are primes, we have that either $f(y)$ divides $f(y+mf(y))$ (so $f(y+mf(y)) \in \{-f(y), f(y)\}$) or $f(y)$ is a prime factor of B. We rephrase this as

$(\forall y \in \{y_1, \ldots, y_{\omega(B)+1}(\forall 0 \le m \le 2(d-1))[f(y+mf(y)) \in \{-f(y), f(y)\}$ OR $f(y)$ is prime factor of B].

There are two cases.

1) $(\forall y \in \{y_1, \ldots, y_{\omega(B)+1}$ y is a prime factor of B. This cannot happen since B only has $\omega(B)$ prime factors.

2)

$$(\exists y \in \{y_1, \ldots, y_{\omega(B)+1}(\forall 0 \le m \le 2(d-1))[f(y+mf(y)) \in \{-f(y), f(y)\}.]$$

Then there would be $d+1$ points mapping to the same thing. Hence f is constant. ▮

5 Polynomials in $\mathsf{C}[x]$

Is there a version of Theorem 4.1 for C? There is!

Theorem 5.1 *Let* $f(x) = \sum_{L=0}^{d} \frac{a_L}{b_L} x^L$ *be a polynomial over* C*. Let* $B = LCM(b_0, \ldots, b_L)$*. If there exists* $y_1, \ldots, y_{\omega(B)+1} \in \mathsf{Z}$ *such that for all* $0 \le m \le 2(d-1)$*,* $f(y+mf(y))$ $f(x)$ *is prime then* $f(x)$ *is constant.*

Proof: By the premise there are $(\omega(B)+1)(2(d-1)+1)$ integers that map to integers. Since the polynomial is of degree d, by Lagrange interpolation the polynomial is actually in $\mathsf{Q}[x]$. Now apply Theorem 4.1. ▮

6 Polynomials in Two Variables

Similar questions for polynomails in two variables are much harder. See Mollin's article [1] for a survey.

7 A Polynomials that Produces a Long Sequence of Primes

Euler noted that $x^2 - x + 41$ is prime for $x = 0, \ldots, 40$.

Ribenboim (*The new book of prime records, Springer 1995*) mentions a cubic polynomial that produces a run of 24 non-composites: $x^3 - 34x^2 + 381x - 1511$.

8 Do Primes Occur Infinitely Often?

If $f(x) \in \mathsf{Z}[x]$ then for an infinite number of y, $f(y)$ is composite. Do we have that for an infinite number of y, $f(y)$ is prime? The short stupid answer is NO: let $f(x) = 2x$.

Let us rephrase is: Let $f(x) \in \mathsf{Z}[x]$ be such that the coefficients of f are relatively prime. Are there an infinite number of y such that $f(y)$ is prime?

1. Dirichlet's theorem: if $GCD(a, b) = 1$ then $f(x) = ax + b$ is a prime infinitely often.

2. Open Question: is $f(x) = x^2 + 1$ is prime infinitely often.

3. Are there any degree $d \geq 2$ polynomials in $\mathsf{Z}[x]$ that produce primes infinitely often. I think this is open, but the good money says that all polynomials have this property.

References

[1] R. Rollin. Prime producing quadratics. *The American Mathematical Monthly*, 104:529–544, 1997.

[2] S. Weintraub. Values of polynomials over integral domains. *The American Mathematical Monthly*, 121:73–74, 2014.