Values of Polynomials over Integral Domains

Steven H. Weintraub

Abstract. It is well known that no nonconstant polynomial with integer coefficients can take on only prime values. We isolate the property of the integers that accounts for this, and give several examples of integral domains for which there are polynomials that only take on unit or prime values.

Throughout this note, we let R denote an arbitrary UFD (unique factorization domain) that is not a field. Of course, R must be infinite.

As is well known, any nonconstant polynomial with integer coefficients cannot take on only prime values. We may ask what property of the integers $\mathbb{Z}$ accounts for this. Here is the answer.

Theorem 1. *Suppose that R has only finitely many units. If $f(x) \in R[x]$ is any nonconstant polynomial, then $f(a)$ is composite for some $a \in R$.*

Proof. Suppose that R has k units, and let $f(x)$ have degree d. Choose any distinct $kd + 1$ elements of R. Then for one of these elements b, $f(b)$ is not a unit, as otherwise $f(x)$ would have to take the same value more than d times, and so would be constant. Let p be any prime dividing $f(b)$. Choose any distinct $(k + 1)d + 1$ elements of R congruent to b mod p. Then for one of these elements a, $f(a)$ is neither a unit multiple of p nor is equal to 0, for the same reason, so $f(a)$ is composite. ∎

We now want to investigate cases when we do have nonconstant polynomials that take on only prime or unit values.

Definition 2. Let $f(x) \in R[x]$ be a polynomial. Then $f(x)$ is a *p-polynomial* if $f(r)$ is prime for every $r \in R$, $f(x)$ is a *u-polynomial* if $f(r)$ is a unit for every $r \in R$, and $f(x)$ is a *up-polynomial* if $f(r)$ is a unit or is prime for every $r \in R$.

Let $\mathcal{P}$ be any set of primes in $\mathbb{Z}$, and let $\mathbb{Z}_{\mathcal{P}}$ denote the localization of $\mathbb{Z}$ at $\mathcal{P}$; concretely, $\mathbb{Z}_{\mathcal{P}} = \{\text{rational numbers } m/n \text{ with no prime factor of } n \text{ in } \mathcal{P}\}$.

Example 3.

(a) Let $\mathcal{P} = \{p \equiv 3 \pmod 4\} \cup \{2\}$, and let $R = \mathbb{Z}_{\mathcal{P}}$. Then $f(x) = x^2 + 1$ is an *up-polynomial*.

(b) Let $\mathcal{P} = \{p \equiv 3 \pmod 4\}$, and let $R = \mathbb{Z}_{\mathcal{P}}$. Then $f(x) = x^2 + 1$ is a *u-polynomial*.

(c) Let $\mathcal{P} = \{p \equiv 5 \text{ or } 7 \pmod 8\} \cup \{2\}$, and let $R = \mathbb{Z}_{\mathcal{P}}$. Then $f(x) = (x(x + 1))^2 + 2$ is a *p-polynomial*.

http://dx.doi.org/10.4169/amer.math.monthly.121.01.073
MSC: Primary 13G05

(Parts (a) and (b) use the fact that -1 is not a quadratic residue of any prime $p \equiv 3 \pmod 4$, and part (c) uses the fact that -2 is not a quadratic residue of any prime $p \equiv 5 \text{ or } 7 \pmod 8$.)

Note that in all parts of this example, $f(x)$ is a monic polynomial and the ring R has infinitely many distinct primes.

Remark 4. We observe that if $f(x) \in R[x]$ has a root in R, i.e., if $f(b) = 0$ for some $b \in R$, then $f(x)$ must take on composite values. The reason is much the same as above. Choose any composite element $c \in R$. Then for any element r of R with $r \equiv b \pmod c$, $f(r) \equiv 0 \pmod c$, so for some $a \equiv b \pmod c$, $0 \neq f(a) \equiv 0 \pmod c$ is composite.

We also observe that if $f(x) \in R[x]$ takes on two distinct (i.e., nonassociated) prime values, then $f(x)$ must take on composite values. For if $f(b_1) \equiv 0 \pmod{p_1}$ and $f(b_2) \equiv 0 \pmod{p_2}$, then by the Chinese Remainder Theorem there is a b with $b \equiv b_1 \pmod{p_1}$ and $b \equiv b_2 \pmod{p_2}$. For any such b, $f(b) \equiv 0 \pmod{p_1 p_2}$, so for some $a \equiv b \pmod{p_1 p_2}$, $0 \neq f(a) \equiv 0 \pmod{p_1 p_2}$ is composite.

Theorem 1 has a generalization, whose proof we leave to the reader.

Theorem 5. *Suppose that R has only finitely many units. Let Q be the quotient field of R. If $f(x) \in Q[x]$ is any nonconstant polynomial such that $f(q_0) \in R$ for some $q_0 \in Q$, then $f(q_1) \in R$ is composite for some $q_1 \in Q$.*

Our focus in this note has been on properties of polynomials over general integral domains. But we will remark that polynomials over the (ordinary) integers have a number of special properties. In [**1**] it is shown that for any integer M, there is a polynomial of any given degree of a specific form that takes on prime values for at least M positive integer arguments. In [**3**] it is shown that, assuming a standard conjecture in number theory, for any integer M there is a quadratic polynomial of a specific form that takes on prime values for at least M consecutive positive integer arguments. Passing to polynomials in more than one variable, [**2**] gives an explicit polynomial of degree 25 in 26 variables whose values at integer arguments are either negative integers or (positive) primes, and which takes on all prime values. [**2**] also shows that any algebraic function, of any number of variables, that takes on integer values at all positive integer arguments must be a polynomial. (We have just sketched the main results of these papers and we refer the reader to them for more specific statements.) The proofs of these results use very different ideas than our proofs above.

REFERENCES

1. B. Garrison, Polynomials with large numbers of prime values, *Amer. Math. Monthly* **97** (1990) 316–317, available at http://dx.doi.org/10.2307/2324515.
2. J. P. Jones, D. Sato, H. Wada, D. Wiens, Diophantine representation of the set of prime numbers, *Amer. Math. Monthly* **83** (1976) 449–464, available at http://dx.doi.org/10.2307/2318339.
3. R. A. Mollin, Prime-producing quadratics, *Amer. Math. Monthly* **104** (1997) 529–544, available at http://dx.doi.org/10.2307/2975080.

Department of Mathematics, Lehigh University, Bethlehem, PA 18015-3174
shw2@lehigh.edu