The American Mathematical Monthly

ISSN: 0002-9890 (Print) 1930-0972 (Online) Journal homepage: https://www.tandfonline.com/loi/uamm20

An Irreducibility Criterion for Polynomials Over the Integers

W. S. Brown & R. L. Graham

To cite this article: W. S. Brown & R. L. Graham (1969) An Irreducibility Criterion for Polynomials Over the Integers, The American Mathematical Monthly, 76:7, 795-797, DOI: 10.1080/00029890.1969.12000326

To link to this article: https://doi.org/10.1080/00029890.1969.12000326

Published online: 18 Apr 2018.

Submit your article to this journal

View related articles

Full Terms & Conditions of access and use can be found at
https://www.tandfonline.com/action/journalInformation?journalCode=uamm20

References

1. Errett Bishop, Holomorphic completions, analytic continuations and the interpolation of seminorms, Ann of Math., 78 (1963) 468–500.
2. J. L. Kelley, Isaac Namioka, *et al.*, Linear Topological Spaces, Van Nostrand, Princeton, 1963.
3. Shoshichi Kobayashi, Invariant distances on complex manifolds and holomorphic mappings, J. Math. Soc. Japan, 19 (1967) 460–480.
4. Walter Rudin, The closed ideals in an algebra of analytic functions, Canadian J. Math., 9 (1957) 426–434.

AN IRREDUCIBILITY CRITERION FOR POLYNOMIALS OVER THE INTEGERS

W. S. Brown and R. L. Graham, Bell Telephone Laboratories

1. Introduction. If $P(x)$ is a reducible polynomial of degree $d\geqq 1$ with integer coefficients, we should not expect the sequence

$$\mathcal{S}(P) = (\cdots, P(-1), P(0), P(1), \cdots)$$

to have many noncomposite (that is, prime or unit) elements. By making this idea precise, we shall obtain an irreducibility criterion. A special case of our main result is that if $\mathcal{S}(P)$ contains p primes and u units with $p+2u>d+4$, then P is irreducible.

2. Fatness. Let $P(x)$ be any polynomial of degree $d\geqq 1$ with integer coefficients, and let u be the number of units in $\mathcal{S}(P)$. We define the *fatness* of P to be

$$f(P) = u - d,$$

and we say that P is *fat* if $f(P)>0$.

If ϵ is a unit (that is, $+1$ or -1), and if $a_1, \cdots, a_d$ are distinct integers, then the polynomial $(x-a_1)\cdots(x-a_d)+\epsilon$ has fatness at least 0. If P is fat, then clearly $\mathcal{S}(P)$ must contain units of both signs.

Note that all polynomials in the set

$$\mathfrak{I}(P) = \{\pm P(\pm x + b)\},$$

where b ranges over the integers and where all possible choices of signs are taken, have the same fatness.

3. Notation. If $P(x)$ is a polynomial, we define

$$\begin{aligned} d &= d(P) &&= \text{degree of } P\\ p &= p(P) &&= \text{number of primes in } \mathcal{S}(P)\\ u &= u(P) &&= \text{number of units in } \mathcal{S}(P)\\ u_+ &= u_+(P) &&= \text{number of positive units in } \mathcal{S}(P)\\ u_- &= u_-(P) &&= \text{number of negative units in } \mathcal{S}(P)\\ f &= f(P) &&= \text{fatness of } P. \end{aligned}$$

Thus $u=u_+ + u_-$, and $f=u-d$.

4. Classification of fat polynomials.

THEOREM 1. *Let $P(x)$ be a fat polynomial (with $d\geqq 1$). Then $u\leqq 4$, $d\leqq 3$, $f\leqq 2$; and one of the following holds*:

(a) $P(x) \in \mathfrak{J}(x),\ u_+ = 1,\ u_- = 1,\ d = 1, f = 1$

(b) $P(x) \in \mathfrak{J}(x^2 + x - 1),\ u_+ = 2,\ u_- = 2,\ d = 2, f = 2$

(c) $P(x) \in \mathfrak{J}(x^3 + 2x^2 - x - 1),\ u_\pm = 3,\ u_\mp = 1,\ d = 3, f = 1$

(d) $P(x) \in \mathfrak{J}(2x - 1),\ u_+ = 1,\ u_- = 1,\ d = 1, f = 1$

(e) $P(x) \in \mathfrak{J}(2x^2 - 1),\ u_\pm = 2,\ u_\mp = 1,\ d = 2, f = 1$.

Proof. We first prove that $u\leqq 4$. Since P is fat, we have seen that $u_+\geqq 1$ and $u_-\geqq 1$. Clearly P may be written

$$P(x) = (x - a_1) \cdots (x - a_{u_+})Q(x) + 1,$$

where $a_1 < \cdots < a_{u_+}$. Now if $P(b)=-1$, we have $(b-a_1)\cdots(b-a_{u_+})Q(b) = -2$, $\{b-a_1, \cdots, b-a_{u_+}\} \subseteq \{-2, -1, 1, 2\}$. By the first of these relations, at least u_+-1 of the distinct integers $b-a_1, \cdots, b-a_{u_+}$ must be ± 1. Hence $1\leqq u_+\leqq 3$, and similarly $1\leqq u_-\leqq 3$. If $u_+=3$, there is at most one integer b for which the second relation holds, so $u_-=1$. If $u_+=2$, there are at most two such integers, so $u_-\leqq 2$. Thus in every case $u\leqq 4$.

Since P is fat, $d<u$, and therefore $d\leqq 3$. Since $u\leqq 4$ and $d\geqq 1$, we have $f\leqq 3$; however, we shall see that the case $f=3$ does not occur, and therefore $f\leqq 2$.

Next we prove that $d(Q)=0$. We may assume $u_+\geqq u_-$, (otherwise replace P by $-P$). Since $u\leqq 4$, it follows that $u_-\leqq 2$. Since P is fat, $d(Q)<u_-$, and therefore $d(Q)=0$ or 1. If $d(Q)=1$, then $u_+=u_-=2$. Hence, for some $b_1\neq b_2$,

$$(b_1 - a_1)(b_1 - a_2)Q(b_1) = (b_2 - a_1)(b_2 - a_2)Q(b_2) = -2,$$
$$\{b_1 - a_1, b_1 - a_2, b_2 - a_1, b_2 - a_2\} \subseteq \{-2, -1, 1, 2\}.$$

Since $\{b_1-a_1, b_1-a_2\}$ is a translate of $\{b_2-a_1, b_2-a_2\}$, it follows that $(b_1-a_1)(b_1-a_2)=(b_2-a_1)(b_2-a_2)$ and $Q(b_1)=Q(b_2)$. Hence $Q(x)$ is constant.

We now have

$$P(x) = c(x - a_1) \cdots (x - a_{u_+}) + 1.$$

Since $u_-\geqq 1$, we may assume $P(0)=-1$; that is, $(-1)^{u_+}ca_1\cdots a_{u_+}=-2$. It follows that $|c|=1$ or 2.

If $|c|=1$, then $a_1\cdots a_{u_+}=\pm 2$, so either $a_1=-2$ or $a_{u_+}=2$. We may assume $a_1=-2$. (Otherwise replace $P(x)$ by $P(-x)$.) If $u_+=1$, then $ca_1=2$, $c=-1$, and $P(x)=-(x+2)+1=-(x+1)$, so $-P(x-1)=x$. If $u_+=2$, then $ca_1a_2=-2$, $ca_2=1$, $a_2=c=\pm 1$, and $P(x)=c(x+2)(x-c)+1$. If $c=1$, then $P(x)=x^2+x-1$. If $c=-1$, then $P(x)=-(x+2)(x+1)+1$, so $-P(x-1)=x^2+x-1$. Finally, if $u_+=3$, then $ca_1a_2a_3=2$, $ca_2a_3=-1$, $a_2=-1$, $a_3=1$, $c=1$, and $P(x)=x^3+2x^2-x-1$.

If $|c|=2$, then $a_1 \cdots a_{u_+}=\pm 1$, so $u_+=1$ or 2. If $u_+=1$, then $ca_1=2$, $c=\pm 2$, $a_1=\pm 1$, and $P(\pm x)=2x-1$. If $u_+=2$, then $ca_1a_2=-2$, $a_1=-1$, $a_2=1$, $c=2$, and $P(x)=2x^2-1$. This completes the proof.

COROLLARY 1. *If P is a fat polynomial with $d=1$ or 2, then there is an integer b such that $P(-x)=(-1)^dP(x-b)$.*

5. Irreducibility criterion.

THEOREM 2. *Let $P(x)$ be a polynomial with $p+2u>d\geqq 2$. Then either P is irreducible or $P=QR$ with $f(Q)+f(R)\geqq p+2u-d$.*

Proof. If P is reducible, we can write $P=QR$ with $f(Q)\geqq f(R)$. Now for each integer n such that $P(n)$ is prime, either $Q(n)$ or $R(n)$ must be a unit, while for each n such that $P(n)$ is a unit, both $Q(n)$ and $R(n)$ must be units. Therefore $u(Q)+u(R)\geqq p+2u$, and $f(Q)+f(R)\geqq p+2u-d$, as was to be shown.

COROLLARY 2: *If $p+2u>d+4$, then P is irreducible.*

6. Example. Let $P(x)=x^5-x^4+2x^3-x^2+x-1$. Then

$$\begin{aligned} P(0) &= -1\\ P(1) &= 1\\ P(2) &= 29\\ P(4) &= 883\\ P(-1) &= -7\\ P(-2) &= -71\\ P(-4) &= -1429. \end{aligned}$$

Thus $p\geqq 5$, $u\geqq 2$, and $p+2u-d\geqq 4$. Hence if P is reducible, we have $P=QR$ with $f(Q)=f(R)=2$. But this implies $d=4$, which is a contradiction, so P is irreducible.

If we fail to notice that $P(4)$ and $P(-4)$ are prime, then we have $p\geqq 3$, $u\geqq 2$, and $p+2u-d\geqq 2$. In this case, if P is reducible, we have $P=QR$ with $f(Q)+f(R)\geqq 2$. Thus either $f(Q)=f(R)=1$ or $f(Q)=2$. In the first case we may assume $d(Q)=2$, and therefore $Q\in\mathfrak{J}(2x^2-1)$. But this is impossible because P is monic. Therefore $f(Q)=2$, and $Q\in\mathfrak{J}(x^2+x-1)$. Now by Corollary 1 we have $Q(x)=(x-b)^2+(x-b)-1$, and so x^2+x-1 divides $P(x+b)$. However the remainder of $P(x+b)$ modulo x^2+x-1 is $R_1(b)+xR_2(b)$, where

$$\begin{aligned} R_1(b) &= b^5-b^4+12b^3-17b^2+21b-9\\ R_2(b) &= 5b^4-14b^3+32b^2-31b+14. \end{aligned}$$

Since R_1 and R_2 have no common integer root, the remainder cannot vanish for any integer b. This contradiction proves that P is irreducible.

We thank the referee for his very helpful suggestions.