A FAMILY OF TESTS FOR IRREDUCIBILITY OF POLYNOMIALS

STEVEN H. WEINTRAUB

(Communicated by Ken Ono)

ABSTRACT. We combine a simple observation about factorization of polynomials with some previous work to obtain a family of irreducibility tests, which we then illustrate.

Let $f(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$ be a polynomial. It is convenient to introduce the following language:

Definition 1. Let q be a prime. Then $f(x)$ satisfies condition (q, ℓ) if its $(\text{mod } q)$ reduction $\overline{f}(x)$ is not divisible by any irreducible polynomial of degree ℓ in $\mathbb{F}_q[x]$.

We then have the following result.

Theorem 2. Let $f(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$ be a polynomial and suppose there is a prime p such that p does not divide a_n , p divides a_i for $i = 0, \dots, n-1$, and for some k with $1 \leq k \leq n-1$, p^2 does not divide a_k . Let k_0 be the smallest such value of k . Suppose furthermore that for some prime $q \neq p$, $f(x)$ satisfies condition (q, ℓ) for $1 \leq \ell \leq k_0$. Then $f(x)$ is irreducible in $\mathbb{Z}[x]$.

Proof. Suppose not. Then, as we showed in [1], in this situation any factorization of $f(x)$ must be of the form $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ with $\overline{h}(x)$, say, of degree at most k_0 . But then $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ with $\overline{h}(x)$ of degree at most k_0 , and in particular with $\overline{h}(x)$ divisible by an irreducible polynomial of degree $\ell \leq k_0$. But that contradicts condition (q, ℓ) . $\square$

Now for any (q, ℓ) , there are only finitely many such polynomials, so condition (q, ℓ) can be checked. This can be done directly, or, more easily, by observing that if $\overline{f}(x)$ does not have a root in $\mathbb{F}_{q^\ell}$, it satisfies this condition. This can then be translated into conditions on the coefficients of $f(x)$. Here are the first few cases:

Condition (2,1): $a_0 \not\equiv 0 \pmod{2}$ and $\sum_i a_i \not\equiv 0 \pmod{2}$.

Condition (3,1): $a_0 \not\equiv 0 \pmod{3}$, $\sum_i a_i \not\equiv 0 \pmod{3}$, and $\sum_i (-1)^i a_i \not\equiv 0 \pmod{3}$.

Condition (2,2): $\sum_{i \equiv 0,2 \pmod{3}} a_i \not\equiv 0 \pmod{2}$ or $\sum_{i \equiv 1,2 \pmod{3}} a_i \not\equiv 0 \pmod{2}$.

Received by the editors October 17, 2015.

2010 *Mathematics Subject Classification.* Primary 12E05.

Key words and phrases. Irreducible polynomials.

Condition (3,2): (i) $\sum_{i \equiv 0 \pmod{4}} a_i - \sum_{i \equiv 2 \pmod{4}} a_i \not\equiv 0 \pmod{3}$ or
 $\sum_{i \equiv 1 \pmod{4}} a_i - \sum_{i \equiv 3 \pmod{4}} a_i \not\equiv 0 \pmod{3}$,

and

(ii) $\sum_{i \equiv 0,2,3 \pmod{8}} a_i - \sum_{i \equiv 4,6,7 \pmod{8}} a_i \not\equiv 0 \pmod{3}$ or
 $\sum_{i \equiv 1,2,7 \pmod{8}} a_i - \sum_{i \equiv 3,5,6 \pmod{8}} a_i \not\equiv 0 \pmod{3}$,

and

(iii) $\sum_{i \equiv 0,2,7 \pmod{8}} a_i - \sum_{i \equiv 3,4,6 \pmod{8}} a_i \not\equiv 0 \pmod{3}$ or
 $\sum_{i \equiv 1,6,7 \pmod{8}} a_i - \sum_{i \equiv 2,3,5 \pmod{8}} a_i \not\equiv 0 \pmod{3}$.

Condition (2,3): (i) $\sum_{i \equiv 0,3,4,5 \pmod{7}} a_i \not\equiv 0 \pmod{2}$ or

$\sum_{i \equiv 1,4,5,6 \pmod{7}} a_i \not\equiv 0 \pmod{2}$ or

$\sum_{i \equiv 2,3,4,6 \pmod{7}} a_i \not\equiv 0 \pmod{2}$,

and

(ii) $\sum_{i \equiv 0,3,5,6 \pmod{7}} a_i \not\equiv 0 \pmod{2}$ or

$\sum_{i \equiv 1,3,4,5 \pmod{7}} a_i \not\equiv 0 \pmod{2}$ or

$\sum_{i \equiv 2,4,5,6 \pmod{7}} a_i \not\equiv 0 \pmod{2}$.

This leads us to see that the following polynomials, with $k_0 = 2$ or 3 , are irreducible. (We omit $k_0 = 1$, as that is very simple and in any case is superceded by the fact that $f(x)$ has a linear factor if and only if it has a rational root.)

Example 3. (a) Suppose that for some odd prime p , p divides a_2 but p^2 does not divide a_2 , and that p^2 divides a_0 . Suppose that a_2 and a_0 are both odd. Then, by condition (2, ℓ) for $1 \leq \ell \leq 2$, for any $n \geq 3$, $n \not\equiv 1 \pmod{3}$, the polynomial $x^n + a_2x^2 + a_0$ is irreducible.

(b) Suppose that for some prime $p \neq 3$, p divides a_2 but p^2 does not divide a_2 , and that p^2 divides a_0 . Suppose that $a_0 \equiv 1 \pmod{3}$ and $a_2 \equiv -1 \pmod{3}$ or that $a_0 \equiv -1 \pmod{3}$ and $a_2 \equiv 1 \pmod{3}$. Then, by condition (3, ℓ) for $1 \leq \ell \leq 2$, for any $n \geq 3$, if $n \not\equiv 0, 1, 5 \pmod{8}$ in case $a_0 \equiv 1 \pmod{3}$ and $a_2 \equiv -1 \pmod{3}$, and if $n \not\equiv 1, 2, 5 \pmod{8}$ in case $a_0 \equiv -1 \pmod{3}$ and $a_2 \equiv 1 \pmod{3}$, the polynomial $x^n + a_2x^2 + a_0$ is irreducible.

(c) Suppose that for some odd prime p , p divides a_3 but p^2 does not divide a_3 , and that p^2 divides a_0 . Suppose that a_3 and a_0 are both odd. Then, by condition (2, ℓ) for $1 \leq \ell \leq 3$, for any $n \geq 4$, $n \not\equiv 1 \pmod{3}$ and $n \not\equiv 1, 2 \pmod{7}$, the polynomial $x^n + a_3x^3 + a_0$ is irreducible.

REFERENCES

- [1] Steven H. Weintraub, *A mild generalization of Eisenstein's criterion*, Proc. Amer. Math. Soc. **141** (2013), no. 4, 1159–1160, DOI 10.1090/S0002-9939-2012-10880-9. MR3008863

DEPARTMENT OF MATHEMATICS, LEHIGH UNIVERSITY, BETHLEHEM, PENNSYLVANIA 18015-3174
E-mail address: shw2@lehigh.edu