involve
a journal of mathematics

The irreducibility of polynomials related to a question of Schur

Lenny Jones and Alicia Lamarche

msp

2016 vol. 9, no. 3

INVOLVE 9:3 (2016)
dx.doi.org/10.2140/involve.2016.9.453

The irreducibility of polynomials related to a question of Schur

Lenny Jones and Alicia Lamarche

(Communicated by Kenneth S. Berenhaut)

In 1908, Schur raised the question of the irreducibility over $\mathbb{Q}$ of polynomials of the form $f(x) = (x + a_1)(x + a_2) \cdots (x + a_m) + c$, where the a_i are distinct integers and $c \in \{-1, 1\}$. Since then, many authors have addressed variations and generalizations of this question. In this article, we investigate the irreducibility of $f(x)$ and $f(x^2)$, where the integers a_i are consecutive terms of an arithmetic progression and c is a nonzero integer.

1. Introduction

Throughout this paper, unless indicated otherwise, "reducible polynomial" and "irreducible polynomial" pertain to reducibility and irreducibility over $\mathbb{Q}$. Schur [1908] raised the question of the irreducibility of polynomials of the form

$$g_{\pm}(x) = (x + a_1)(x + a_2) \cdots (x + a_m) \pm 1,$$

where the a_i are distinct integers. Westlund [1909] showed that $g_-(x)$ is always irreducible, and that if $g_+(x)$ is reducible, then $g_+(x)$ must be the square of a polynomial. Flügel [1909] showed that $g_+(x)$ is reducible if and only if there exists an integer z such that

$$g_+(x + z) = (x - 1)^2 \quad \text{or} \quad g_+(x + z) = (x^2 - 3x + 1)^2.$$

Since that time, numerous authors [Seres 1956; Győry et al. 2011] have addressed variations and generalizations of these questions. For some more recent generalizations, and a complete history and bibliography chronicling these results, see [Győry et al. 2011].

Here we investigate the irreducibility of polynomials $f(x)$ and $f(x^2)$, where

$$f(x) = (x + a_i)(x + a_{i+1}) \cdots (x + a_{i+m-1}) + c, \tag{1-1}$$

MSC2010: 12E05, 11C08.
Keywords: irreducible polynomial.

with the a_j being consecutive terms of an arithmetic progression

$$\mathcal{A} = \{k, k+d, k+2d, \dots\},$$

where $d > 0$ is the common difference. Since

$$f(x) = \big(x+k+jd\big)\big(x+k+(j+1)d\big)\cdots\big(x+k+(j+m-1)d\big)+c$$

is irreducible if and only if

$$f(x) = x(x+d)(x+2d)\cdots(x+(m-1)d)+c \tag{1-2}$$

is irreducible, our focus here is on (1-2). While we are placing restrictions on the values of a_i in (1-1), the fact that we are not initially placing any restrictions on c, other than $c \neq 0$, and that we are also concerned with the irreducibility of $f(x^2)$, make this investigation somewhat of a departure from previous ones. In particular, defining $F(x) := f(x^2)$, where $f(x)$ is as in (1-2), we are interested in determining values of d, m and c, with $d > 0$ and $m \geq 2$, for which

(I) $f(x)$ is reducible,

(II) $f(x)$ is irreducible, but $F(x)$ is reducible,

(III) both $f(x)$ and $F(x)$ are irreducible.

Note that if $F(x)$ is irreducible, then $f(x)$ is irreducible. However, the converse is false in general, as the example $f(x) = x-1$ illustrates, so that situation (II) is not, in general, vacuous. Clearly, a complete answer to (I) and (II), or to (I) and (III), provides an answer to (III), or to (II), respectively. Although a complete answer to (I) seems intractable, a reasonable approach seems to be to place restrictions on one or more of d, m and c. For example, one could place a bound on m and determine the appropriate values of d and c such that $f(x)$ satisfies (I), (II) or (III). This is the strategy we employ in Section 3. However, in this scenario, even small values of m prove to be challenging. In Section 4, by imposing different restrictions on d, m and c, we can establish the following theorem for larger degree polynomials:

Theorem 1.1. *Let $p \geq 3$ be prime, and let $c, d \in \mathbb{Z}$, with $c \neq 0$, $d > 0$ and $d \not\equiv 0 \pmod{p}$. Let*

$$\begin{aligned} f(x) &= x(x+d)(x+2d)\cdots(x+(p-1)d)+c \\ &= x^p + a_{p-1}x^{p-1} + \cdots + a_1 x + c. \end{aligned}$$

(1) *If $c \not\equiv 0 \pmod{p}$, then $f(x)$ is irreducible. If, in addition, $c \neq -z^2$ for any $z \in \mathbb{Z}$, then $F(x)$ is irreducible.*

(2) *Let k be a fixed positive integer, and suppose that $|c| = kp^w$, where*

$$p^w > k^{p-1} + a_{p-1}k^{p-2} + \cdots + a_2 k + a_1.$$

Then both $f(x)$ and $F(x)$ are irreducible if one of the sets of conditions below holds:

(a) $c > 0$.

(b) $c < 0$, $w \equiv 1 \pmod 2$ *and* $k \not\equiv 0 \pmod p$.

(c) $c < 0$ *and* $p \equiv 3 \pmod 4$.

Computations in this article were performed using either Maple or Magma.

2. Preliminaries

We now present, without proof, some facts that are used to establish the results in this article. The first two theorems for general fields $\boldsymbol{k}$ first appeared in [Schinzel 1982]. For fields $\boldsymbol{k} \subset \mathbb{C}$, they are originally due to Capelli [Schinzel 2000].

Theorem 2.1. *Let $\boldsymbol{k}$ be a field, and let $f(x)$ and $g(x)$ be polynomials in $\boldsymbol{k}[x]$ with $f(x)$ irreducible over $\boldsymbol{k}$. Suppose that $f(\alpha) = 0$. Then $f(g(x))$ is reducible over $\boldsymbol{k}$ if and only if $g(x) - \alpha$ is reducible over $\boldsymbol{k}(\alpha)$. Furthermore, if*

$$g(x) - \alpha = c_1 u_1(x)^{e_1} \cdots u_r(x)^{e_r},$$

where $c_1 \in \boldsymbol{k}(\alpha)$ and the $u_j(x)$ are distinct monic irreducible polynomials in $\boldsymbol{k}(\alpha)[x]$, then

$$f(g(x)) = c_2 \mathcal{N}(u_1(x))^{e_1} \cdots \mathcal{N}(u_r(x))^{e_r},$$

where $c_2 \in \boldsymbol{k}$, and the norms $\mathcal{N}(u_j(x))$ are distinct monic irreducible polynomials in $\boldsymbol{k}[x]$.

Theorem 2.2. *Let $\boldsymbol{k}$ be a field, and let $r \in \mathbb{Z}$ with $r \geq 2$. Let $\alpha \in \boldsymbol{k}$. Then $x^r - \alpha$ is reducible over $\boldsymbol{k}$ if and only if either $\alpha = \beta^p$ for some prime divisor p of r and $\beta \in \boldsymbol{k}$, or $4 \mid r$ and $\alpha = -4\beta^4$ for some $\beta \in \boldsymbol{k}$.*

The next result follows from direct applications of Theorem 2.1 with $g(x) = x^2$ and Theorem 2.2 with $r = 2$, and equating constant terms.

Theorem 2.3. *Let*

$$f(x) = x^n + \sum_{j=1}^{n-1} a_j x^j + c \in \mathbb{Z}[x],$$

with $f(x)$ irreducible. Then:

(1) *If $n \equiv 0 \pmod 2$ and $c \neq z^2$ for any $z \in \mathbb{Z}$, then $F(x)$ is irreducible.*

(2) *If $n \equiv 1 \pmod 2$ and $c \neq -z^2$ for any $z \in \mathbb{Z}$, then $F(x)$ is irreducible.*

The following result is well-known [Serret 1992].

Theorem 2.4. *Let p be a prime, and let $f(x) = x^p - x + c \in \mathbb{F}_p[x]$. If $c \not\equiv 0 \pmod p$, then $f(x)$ is irreducible over $\mathbb{F}_p$.*

Since the irreducibility of a polynomial over $\mathbb{F}_p$ implies its irreducibility over $\mathbb{Q}$, we immediately have the following corollary.

Corollary 2.5. *Let $f(x) \in \mathbb{Z}[x]$, and let p be a prime. If $f(x) \equiv x^p - x + c \pmod{p}$ and $c \not\equiv 0 \pmod{p}$, then $f(x)$ is irreducible.*

The next theorem and its corollary are special cases of results of Weisner [1934].

Theorem 2.6. *Let*

$$A(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

be such that $n \geq 2$, $a_n \neq 0$ and

$$|a_0| = kp^w, \quad \text{with } k, w \geq 1,$$

where p is a prime that does not divide a_1 if $w > 1$. Suppose further that there exists L such that $|r| \geq L \geq 1$ for all zeros r of $A(x)$. If $k < L$, then $A(x)$ is irreducible.

Corollary 2.7. *Let $k, w \geq 1$ and $n \geq 2$ be integers, and let*

$$A_{\pm}(x) = x^n + a_{n-1} x^{n-1} + \cdots + a_1 x \pm kp^w \in \mathbb{Z}[x],$$

where p is a prime that does not divide a_1. If

$$p^w > k^{n-1} + |a_{n-1}| k^{n-2} + \cdots + |a_2| k + |a_1|,$$

then each of $A_{\pm}(x)$ is irreducible.

3. A first approach

In this section, we investigate an approach to determine the values of c such that each of the conditions (I), (II) and (III) holds. The idea is to analyze the degree-type factorization of $f(x)$. The following proposition, whose proof is immediate from the definition of $f(x)$ in (1-2), represents a modest step in this direction.

Proposition 3.1. *The polynomial $f(x)$ has a zero $n \in \mathbb{Z}$ if and only if*

$$c = -n(n+d)(n+2d) \cdots (n+(m-1)d) \quad \text{for some } n \in \mathbb{Z}.$$

One difficulty in establishing a more general result similar to Proposition 3.1 is that the number of possible degree-type factorizations of $f(x)$ into irreducibles increases as m increases. To avoid this complication, we bound the value of m. However, even for small values of m, such a method proves to be challenging. To illustrate the difficulties that arise, we address the cases (I) and (II) for each value of $m \in \{2, 3, 4\}$. For case (I), we use the straightforward method of equating coefficients. Our investigation of case (II) also uses the method of equating coefficients, but we additionally utilize Theorem 2.1 and Theorem 2.2 with $g(x) = x^2$. Although the techniques are similar, each value of m presents distinct obstacles.

The case of $m = 2$.

Theorem 3.2. *Let $c, d \in \mathbb{Z}$, with $d > 0$, and let*

$$f(x) = x(x+d) + c.$$

Then

(1) *$f(x)$ is reducible if and only if*

$$c \in \{-n(n+d) \mid n \in \mathbb{Z}\},$$

(2) *$f(x)$ is irreducible and $F(x)$ is reducible if and only if*

$$c \in \left\{\tfrac{1}{4}(s^2+d)^2 \;\middle|\; s \in \mathbb{Z},\ \textit{with } s > 0 \textit{ and } s^2 \equiv d \pmod 2\right\}.$$

Proof. Observe that (1) follows immediately from Proposition 3.1. To prove (2), suppose first that $f(x)$ is irreducible and $f(\alpha) = 0$. Suppose that $\alpha = \beta^2$ for some $\beta \in \mathbb{Q}(\alpha)$. Then, by Theorem 2.1,

$$\begin{aligned} F(x) &= x^4 + dx^2 + c && (3\text{-}1)\\ &= \mathcal{N}(x+\beta)\mathcal{N}(x-\beta)\\ &= \big(x^2 + (\beta+\bar\beta)x + \beta\bar\beta\big)\big(x^2 - (\beta+\bar\beta)x + \beta\bar\beta\big)\\ &= (x^2+sx+t)(x^2-sx+t)\\ &= x^4 + (2t-s^2)x^2 + t^2 && (3\text{-}2)\end{aligned}$$

for some $s, t \in \mathbb{Z}$. Equating coefficients in (3-1) and (3-2) and solving the resulting system of equations gives $c = \frac{1}{4}(s^2+d)^2$.

There are two items of concern here. The first item to address is whether there are any restrictions that must be placed on s to guarantee that $c \in \mathbb{Z}$. The second item is whether there are any values of s such that $f(x)$ is reducible. Clearly, we can assume that $s \ge 0$ in any case, and imposing the restriction that $c \in \mathbb{Z}$ tells us that $s^2 \equiv d \pmod 2$. We must now check if there are any such values of c such that $f(x)$ is reducible. That is, are there values of $s, n \in \mathbb{Z}$ such that

$$\tfrac{1}{4}(s^2+d)^2 = -n(n+d)? \tag{3-3}$$

Solving (3-3), we get the single integer solution $s = 0$ and $n = -\frac{1}{2}d$, where $d \equiv 0 \pmod 2$, which corresponds to $c = \frac{1}{4}d^2$. Hence, we must have $s > 0$ to ensure that $f(x)$ is irreducible. Under these restrictions on c, we have conversely that $f(x)$ is irreducible and that

$$\begin{aligned} F(x) &= x^4 + dx^2 + \tfrac{1}{4}(s^2+d)^2\\ &= \big(x^2 + sx + \tfrac{1}{2}(s^2+d)\big)\big(x^2 - sx + \tfrac{1}{2}(s^2+d)\big). \end{aligned}$$

□

The case of $m = 3$.

Theorem 3.3. *Let $c, d \in \mathbb{Z}$, with $d > 0$, and let*

$$f(x) = x(x+d)(x+2d) + c.$$

Then

(1) *$f(x)$ is reducible if and only if*

$$c \in R = \{-n(n+d)(n+2d) \mid n \in \mathbb{Z}\},$$

(2) *$f(x)$ is irreducible and $F(x)$ is reducible if and only if $c \in S \setminus R$, where*

$$S = \left\{ -\left(\frac{s^4 + 6ds^2 + d^2}{8s}\right)^2 \;\middle|\; \text{all of the conditions in } A \text{ hold} \right\},$$

and A is the following list:

$$d \not\equiv 2, 3 \pmod 4, \quad s \in \mathbb{Z}^+, \quad \frac{d^2}{s} \in \mathbb{Z}^+,$$
$$s \equiv 0 \pmod 2 \text{ and } \frac{d^2}{8s} \in \mathbb{Z}^+ \text{ if } d \equiv 0 \pmod 4,$$
$$s \equiv 1 \pmod 2 \text{ if } d \equiv 1 \pmod 4.$$

Moreover, S contains at most finitely many elements for a fixed value of d.

Proof. As in the case of $m = 2$, observe that (1) follows immediately from Proposition 3.1. To establish (2), we proceed as in Theorem 3.2. We assume that $f(x)$ is irreducible and $f(\alpha) = 0$. Suppose also that $\alpha = \beta^2$ for some $\beta \in \mathbb{Q}(\alpha)$. Then, by Theorem 2.1, we have

$$\begin{aligned} F(x) &= x^6 + 3dx^4 + 2d^2x^2 + c && \text{(3-4)} \\ &= (x^3 + sx^2 + tx + u)(x^3 - sx^2 + tx - u) \\ &= x^6 + (2t - s^2)x^4 + (t^2 - 2su)x^2 - u^2 && \text{(3-5)} \end{aligned}$$

for some $s, t, u \in \mathbb{Z}$. Equating coefficients in (3-4) and (3-5) and solving the resulting system of equations, with $d > 0$, gives

$$c = -\left(\frac{s^4 + 6ds^2 + d^2}{8s}\right)^2,$$

where we can assume that $s > 0$. Since $c \in \mathbb{Z}$, it is necessary that $d^2 \equiv 0 \pmod s$. This restriction alone implies that there are at most finitely many such values of c for a fixed d, and therefore all such values of c in S can be effectively computed. Further analysis reveals that $d \not\equiv 2, 3 \pmod 4$, since $s^4 + 6ds^2 + d^2 \equiv 0 \pmod 8$. Additionally, we see that $s \equiv 0 \pmod 2$ when $d \equiv 0 \pmod 4$, and in this case we get the more restrictive condition that $d^2 \equiv 0 \pmod{8s}$. Finally, $s \equiv 1 \pmod 2$ when $d \equiv 1 \pmod 4$.

Conversely, if $c \in S \setminus R$, then $f(x)$ is irreducible and

$$F(x) = x^6 + 3dx^4 + 2d^2x^2 - \left(\frac{s^4 + 6ds^2 + d^2}{8s}\right)^2 = F_1(x)F_2(x),$$

where

$$F_1(x) = x^3 + sx^2 + \tfrac{1}{2}(s^2 + 3d)x + \frac{s^4 + 6ds^2 + d^2}{8s} \in \mathbb{Z}[x]$$

and

$$F_2(x) = x^3 - sx^2 + \tfrac{1}{2}(s^2 + 3d)x - \frac{s^4 + 6ds^2 + d^2}{8s} \in \mathbb{Z}[x]. \qquad \square$$

As in the proof of Theorem 3.2, a somewhat more explicit description of the values of c such that (II) holds would be desirable. To determine whether any values of $c \in S$ from (2) are such that $f(x)$ is reducible when $d \equiv 0, 1 \pmod 4$, we must solve the Diophantine equation

$$\left(\frac{s^4 + 6ds^2 + d^2}{8s}\right)^2 = n(n+d)(n+2d). \tag{3-6}$$

Again, because of the restriction on s for a given value of d, the solutions to (3-6) can be effectively computed. We conjecture that there are no solutions to (3-6) for any value of d, so that $S \cap R = \varnothing$.

Remark 3.4. Any solutions to (3-6) are integral solutions of the so-called "congruent-number" elliptic curve $y^2 = x(x^2 - d^2)$, which has been studied extensively [Bremner et al. 2000; Koblitz 1993; Silverman 2009].

The case of $m = 4$.

Theorem 3.5. *Let $c, d \in \mathbb{Z}$, with $d > 0$, and let*

$$f(x) = x(x+d)(x+2d)(x+3d) + c.$$

Then

(1) *$f(x)$ is reducible if and only if $c \in R = R_1 \cup R_2$, where*

$$R_1 = \{v(2d^2 - v) \mid v \in \mathbb{Z}\},$$
$$R_2 = \left\{\tfrac{1}{4}(u-d)(u-2d)(u-4d)(u-5d) \in \mathbb{Z} \mid u \in \mathbb{Z}\right\},$$

(2) *$f(x)$ is irreducible and $F(x)$ is reducible if and only if $c \in S \setminus R$, where*

$$S = \left\{\left(\frac{u^2 + 6d^3}{2t}\right)^2 \in \mathbb{Z} \;\middle|\; \text{all of the conditions in } B \text{ hold}\right\},$$

and B is the following list:

$$u, t \in \mathbb{Z}^+, \quad t = \tfrac{1}{2}(s^2 + 6d) \text{ for some } s \in \mathbb{Z},$$
$$8u^2 + (-8s^3 - 48sd)u + s^6 + 18s^4 + 64s^2d^2 = 0.$$

Moreover, S contains at most finitely many elements.

Proof. Logically, since

$$f(x) = x^4 + 6dx^3 + 11d^2x^2 + 6d^3x + c \tag{3-7}$$

is a fourth-degree polynomial, there are five possibilities that could occur when factoring $f(x)$ into irreducibles:

(1) $f(x)$ is irreducible.

(2) $f(x)$ is the product of a linear factor and an irreducible cubic.

(3) $f(x)$ is the product of two linear factors and an irreducible quadratic.

(4) $f(x)$ is the product of two irreducible quadratics.

(5) $f(x)$ is the product of four linear factors.

Proposition 3.1 gives us conditions under which $f(x)$ has a linear factor, but it is not delicate enough alone to distinguish among possibilities (2), (3) and (5). In fact, it turns out that (2) is vacuous. To see this, first note that if $f(r) = 0$ for some $r \in \mathbb{Z}$, then

$$\begin{aligned} f(-r-3d) &= (-r-3d)(-r-2d)(-r-d)(-r) + c \\ &= r(r+d)(r+2d)(r+3d) + c \\ &= f(r) = 0. \end{aligned}$$

If $r \neq -r-3d$, then $f(x)$ has at least two distinct linear factors. If $r = -r-3d$, then

$$4r^3 + 18dr^2 + 22d^2r + 6d^3 = f'(r) = f'(-r-3d) = -4r^3 - 18dr^2 - 22d^2r - 6d^3,$$

so that $f'(r) = 0$. Hence, $(x-r)^2$ divides $f(x)$, and therefore (2) does not occur. Thus, to determine exactly the values of c for which $f(x)$ is reducible, we proceed as follows. Assuming $f(x)$ is reducible, we write

$$\begin{aligned} f(x) &= (x^2 + sx + t)(x^2 + ux + v) \\ &= x^4 + (s+u)x^3 + (t + su + v)x^2 + (tu + sv)x + tv. \end{aligned} \tag{3-8}$$

Solving the system of equations that results by equating coefficients in (3-7) and (3-8), we arrive at the two solutions for c,

$$c = v(2d^2 - v) \quad \text{and} \quad c = \tfrac{1}{4}(u-d)(u-2d)(u-4d)(u-5d),$$

where if $c = v(2d^2 - v)$, then

$$f(x) = \big(x^2 + 3dx + (2d^2 - v)\big)(x^2 + 3dx + v),$$

and if $c = \frac{1}{4}(u-d)(u-2d)(u-4d)(u-5d) \in \mathbb{Z}$, then

$$f(x) = \big(x^2 + (6d-u)x + \tfrac{1}{2}(u-5d)(u-4d)\big)\big(x^2 + ux + \tfrac{1}{2}(u-2d)(u-d)\big).$$

We note that the infinite sets R_1 and R_2 are not disjoint, and further analysis is required to determine the particular degree-types given in (3), (4) and (5).

We turn now to an examination of when

$$F(x) = x^8 + 6dx^6 + 11d^2x^4 + 6d^3x^2 + c \tag{3-9}$$

is reducible, assuming that $f(x)$ is irreducible. As before, we have from Theorem 2.1 and Theorem 2.2 that

$$\begin{aligned} F(x) &= (x^4 + sx^3 + tx^2 + ux + v)(x^4 - sx^3 + tx^2 - ux + v) \\ &= x^8 + (2t - s^2)x^6 + (t^2 - 2us + 2v)x^4 + (2vt - u^2)x^2 + v^2. \end{aligned} \tag{3-10}$$

Equating coefficients in (3-9) and (3-10), and solving the resulting system of equations yields

$$\begin{aligned} v = \frac{u^2+6d^3}{2t}, \quad t = \tfrac{1}{2}(s^2 + 6d), \\ 8u^2 - (8s^3 + 48sd)u + s^6 + 18s^4d + 64s^2d^2 = 0. \end{aligned} \tag{3-11}$$

Note that if $s = 0$ in (3-11), then $u = 0$ and $c = d^4$, so that $f(x) = (x^2+3dx+d^2)^2$. Viewing the third equation in (3-11) as a quadratic equation in the variable u, and solving gives

$$u = \tfrac{1}{4}\big(2s^3 + 12ds \pm s\sqrt{2s^4 + 12ds^2 + 16d^2}\big). \tag{3-12}$$

From (3-12), we see that a necessary condition for u to be an integer is that $2s^4 + 12ds^2 + 16d^2$ be a square. To determine when this occurs, we think of s as a variable and we seek nontrivial ($s \neq 0$) integral solutions to the elliptic curve

$$y^2 = 2s^4 + 12ds^2 + 16d^2 = 2(s^2 + 2d)(s^2 + 4d). \tag{3-13}$$

For a given value of d, it is well known that there are at most finitely many nontrivial solutions to (3-13), and these solutions can be found using the command

`IntegralQuarticPoints(`$[2, 0, 12d, 0, 16d^2]$`)`

in Magma. Hence, there are at most finitely many polynomials $f(x)$ that satisfy (II), and for a given value of d, these polynomials can effectively be found.

Conversely, if $c \notin R$, then $f(x)$ is irreducible, and it is straightforward to derive (3-9) by the substitution of conditions (3-11) into (3-10). □

Remark 3.6. For bounds on the number of solutions to (3-13), the interested reader should see [Bennett 1998; Bugeaud et al. 2011].

4. A second approach

In this section, we prove Theorem 1.1, which can be deduced easily using the following theorem and some results presented in Section 2.

Theorem 4.1. *Let p be a prime and let*

$$f(x) = x^n + \sum_{j=1}^{n-1} a_j x^j + c \in \mathbb{Z}[x],$$

where $n \geq 2$ and $c \equiv 0 \pmod p$. Suppose that $f(x)$ is irreducible. Then

(1) *If $n \equiv 0 \pmod 2$ and $a_1 \not\equiv -z^2 \pmod p$ for any $z \in \mathbb{F}_p$, then $F(x)$ is irreducible.*

(2) *If $n \equiv 1 \pmod 2$ and $a_1 \not\equiv z^2 \pmod p$ for any $z \in \mathbb{F}_p$, then $F(x)$ is irreducible.*

Proof. Since $f(x)$ is irreducible, we can apply Theorem 2.1 and Theorem 2.2 to deduce that if $F(x)$ is reducible, then

$$\begin{aligned} F(x) &= x^{2n} + \sum_{j=1}^{n-1} a_j x^{2j} + c \\ &= \left(x^n + \sum_{j=0}^{n-1} b_j x^j\right)\left(x^n + \sum_{j=0}^{n-1} (-1)^{n-j} b_j x^j\right) \\ &= \begin{cases} x^{2n} + \cdots + (2b_0b_2 - b_1^2)x^2 + b_0^2 & \text{if } n \equiv 0 \pmod 2, \\ x^{2n} + \cdots + (b_1^2 - 2b_0b_2)x^2 - b_0^2 & \text{if } n \equiv 1 \pmod 2. \end{cases} \end{aligned}$$

Since $c \equiv 0 \pmod p$, equating coefficients gives that $b_0 \equiv 0 \pmod p$ and

$$a_1 \equiv \begin{cases} -b_1^2 \pmod p & \text{if } n \equiv 0 \pmod 2, \\ b_1^2 \pmod p & \text{if } n \equiv 1 \pmod 2. \end{cases}$$ □

For the convenience of the reader, we restate Theorem 1.1 here.

Theorem 1.1. *Let $p \geq 3$ be prime, and let $c, d \in \mathbb{Z}$, with $c \neq 0$, $d > 0$ and $d \not\equiv 0 \pmod p$. Let*

$$\begin{aligned} f(x) &= x(x+d)(x+2d)\cdots(x+(p-1)d) + c \\ &= x^p + a_{p-1}x^{p-1} + \cdots + a_1 x + c. \end{aligned}$$

(1) *If $c \not\equiv 0 \pmod p$, then $f(x)$ is irreducible. If, in addition, $c \neq -z^2$ for any $z \in \mathbb{Z}$, then $F(x)$ is irreducible.*

(2) *Let k be a fixed positive integer, and suppose that $|c| = kp^w$, where*

$$p^w > k^{p-1} + a_{p-1}k^{p-2} + \cdots + a_2 k + a_1.$$

Then both $f(x)$ and $F(x)$ are irreducible if one of the sets of conditions below holds:

(a) $c > 0$.

(b) $c < 0$, $w \equiv 1 \pmod 2$ *and* $k \not\equiv 0 \pmod p$.

(c) $c < 0$ *and* $p \equiv 3 \pmod 4$.

Proof. Since $d \not\equiv 0 \pmod p$, we have that

$$f(x) \equiv x(x-1)(x-2)\cdots(x-(p-1)) + c \equiv x^p - x + c \pmod p.$$

Hence, since $c \not\equiv 0 \pmod p$, we have from Corollary 2.5 that $f(x)$ is irreducible. If, in addition, $c \neq -z^2$ for any $z \in \mathbb{Z}$, then $F(x)$ is irreducible by Theorem 2.3(2).

To prove (2), note that since $d \not\equiv 0 \pmod p$, we have

$$a_1 = d^{p-1}(p-1)! \equiv -1 \pmod p \not\equiv 0 \pmod p \tag{4-1}$$

by Fermat's little theorem and Wilson's theorem. Hence, $f(x)$ is irreducible by Corollary 2.7.

To establish parts (2a), (2b) and (2c), first note that $\deg(f(x)) = p$ is odd. Thus, if $c = kp^w > 0$, then $F(x)$ is irreducible by Theorem 2.3(2), which resolves (2a). For (2b), observe that kp^w is not a square since $w \equiv 1 \pmod 2$ and $k \not\equiv 0 \pmod p$. Thus, again it follows from Theorem 2.3(2) that $F(x)$ is irreducible. Finally, for (2c), since $p \equiv 3 \pmod 4$, we have from (4-1) that $a_1 \not\equiv z^2 \pmod p$ for any $z \in \mathbb{F}_p$. Therefore, $F(x)$ is irreducible by Theorem 4.1(2). □

Acknowledgements

The authors thank the referee for the very careful reading of the manuscript, the many excellent suggestions, and most of all, the very timely manner in which the report was received.

References

[Bennett 1998] M. A. Bennett, "On the number of solutions of simultaneous Pell equations", *J. Reine Angew. Math.* **498** (1998), 173–199. MR 1629862 Zbl 1044.11011

[Bremner et al. 2000] A. Bremner, J. H. Silverman, and N. Tzanakis, "Integral points in arithmetic progression on $y^2 = x(x^2 - n^2)$", *J. Number Theory* **80**:2 (2000), 187–208. MR 1740510 Zbl 1009.11035

[Bugeaud et al. 2011] Y. Bugeaud, C. Levesque, and M. Waldschmidt, "Équations de Fermat–Pell–Mahler simultanées", *Publ. Math. Debrecen* **79**:3-4 (2011), 357–366. MR 2907971 Zbl 1249.11053

[Flügel 1909] W. Flügel, "Solution to problem 226", *Archiv. der Math. und Physik* **15** (1909), 271.

[Győry et al. 2011] K. Győry, L. Hajdu, and R. Tijdeman, "Irreducibility criteria of Schur-type and Pólya-type", *Monatsh. Math.* **163**:4 (2011), 415–443. MR 2820371 Zbl 1232.11112

[Koblitz 1993] N. Koblitz, *Introduction to elliptic curves and modular forms*, 2nd ed., Graduate Texts in Mathematics **97**, Springer, New York, 1993. MR 1216136 Zbl 0804.11039

[Schinzel 1982] A. Schinzel, *Selected topics on polynomials*, University of Michigan Press, Ann Arbor, MI, 1982. MR 649775 Zbl 0487.12002

[Schinzel 2000] A. Schinzel, *Polynomials with special regard to reducibility*, Encyclopedia of Mathematics and its Applications **77**, Cambridge University Press, 2000. MR 1770638 Zbl 0956.12001

[Schur 1908] I. Schur, "Problem 226", *Archiv Math. Physik* **13**:3 (1908), 367.

[Seres 1956] I. Seres, "Lösung und Verallgemeinerung eines Schurschen Irreduzibilitätsproblems für Polynome", *Acta Math. Acad. Sci. Hungar.* **7** (1956), 151–157. MR 0082952 Zbl 0071.01801

[Serret 1992] J.-A. Serret, *Cours d'algèbre supérieure, II*, 4th ed., Éditions Jacques Gabay, Sceaux, 1992. MR 1190472

[Silverman 2009] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics **106**, Springer, Dordrecht, 2009. MR 2514094 Zbl 1194.11005

[Weisner 1934] L. Weisner, "Criteria for the irreducibility of polynomials", *Bull. Amer. Math. Soc.* **40**:12 (1934), 864–870. MR 1562990 Zbl 0010.29001

[Westlund 1909] J. Westlund, "On the irreducibility of certain polynomials", *Amer. Math. Monthly* **16**:4 (1909), 66–67. MR 1517192 JFM 40.0123.01

Received: 2015-03-14 Revised: 2015-05-18 Accepted: 2015-06-17

lkjone@ship.edu *Department of Mathematics, Shippensburg University, Shippensburg, PA 17257-2299, United States*

al5903@ship.edu *Department of Mathematics, Shippensburg University, Shippensburg, PA 17257-2299, United States*

mathematical sciences publishers msp

involve

msp.org/involve

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2016 is US $160/year for the electronic version, and $215/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2016 vol. 9 no. 3

1944-4176(2016)9:3;1-2