

## ON THE IRREDUCIBILITY OF THE ITERATES OF $x^n - b$

LYNDA DANIELSON AND BURTON FEIN

(Communicated by Lance W. Small)

ABSTRACT. Let  $K$  be a field and suppose that  $f(x) = x^n - b$  is irreducible in  $K[x]$ . We discuss the following question: under what conditions are all iterates of  $f$  irreducible over  $K$ ?

Let  $K$  be a field and let  $f(x) \in K[x]$ . By the iterates of  $f$  we mean the sequence of polynomials  $f_r$  defined by  $f_0(x) = x$ , and  $f_{r+1}(x) = f(f_r(x))$  for  $r \geq 0$ . It is clear that if any iterate  $f_m$  of  $f$  is reducible in  $K[x]$ , then all successive iterates  $f_{m+i}(x) = f_m(f_i(x))$  are also reducible over  $K$ . If, however,  $f$  is irreducible in  $K[x]$ , then its various iterates may or may not also be irreducible over  $K$ . In this paper we investigate the irreducibility of the iterates of  $f$  for  $f$  an irreducible polynomial in  $K[x]$  of the form  $x^n - b$ .

Suppose that  $f(x) = x^n - b$  is irreducible in  $K[x]$ . Examples exist for every  $n \geq 2$  and  $m \geq 1$  of  $K$  and  $b \in K$  such that  $f_m$  is irreducible over  $K$  but  $f_{m+1}$  is reducible. This raises the following question which motivates this paper: under what conditions on  $K$ ,  $n$ , and  $b$  are all iterates of  $f(x) = x^n - b$  irreducible over  $K$ ? We show that all iterates of  $f$  as above are irreducible over  $K$  in the following cases: (i)  $K = \mathbb{Q}$  and  $b \in \mathbb{Z}$ , (ii)  $K = \mathbb{Q}(t)$  and  $b \in \mathbb{Z}[t]$ , (iii)  $K = F(t)$  and  $b \in F[t]$  for  $F$  an arbitrary algebraically closed field, and (iv)  $K = F(t)$ ,  $b \in F(t)$ ,  $b \notin F$ ,  $n \geq 3$ , and  $F$  an arbitrary field of characteristic 0. We also consider the case not covered by (i) above when  $K = \mathbb{Q}$  and  $b \in \mathbb{Q}$  but  $b \notin \mathbb{Z}$ . Fix  $n \geq 2$  and let  $S(n)$  denote the set of  $b \in \mathbb{Q}$  such that  $f(x) = x^n - b$  is irreducible in  $\mathbb{Q}[x]$  but some iterate of  $f$  is reducible over  $\mathbb{Q}$ . We show that  $S(2)$  is infinite, that  $S(n)$  is finite for  $n$  odd,  $n \geq 5$ , and that the *abc-conjecture* implies that  $S(n)$  is finite for  $n$  even,  $n \neq 2$ . The question of whether  $S(n)$  is or is not empty is particularly interesting since we also show that if there exists an odd  $n \geq 3$  for which  $S(n) \neq \emptyset$ , then there exists a primitive triple  $(x, y, z)$  satisfying  $x^p + y^p = z^r$  with  $p$  and  $r$  each  $\geq 3$ ; it is a fundamental open question whether such triples exist.

For the convenience of the reader, we begin our discussion with a special case of a result due to Capelli (see [FS, Lemma 0.1]):

**Proposition 1.** *Let  $K$  be a field and let  $f(x) = x^n - b \in K[x]$ . Assume that  $f_m$  is irreducible in  $K[x]$  for some  $m \geq 0$  and let  $\alpha_m$  be a root of  $f_m$ . Then  $f_{m+1}$  is*

---

Received by the editors April 13, 2000 and, in revised form, December 20, 2000.

2000 *Mathematics Subject Classification.* Primary 12E05; Secondary 11D41.

*Key words and phrases.* Iterated polynomial, irreducible, generalized Fermat equation, *abc*-conjecture.

The second author is grateful for support under NSA Grant MDA904-97-1-0040.

reducible over  $K$  if and only if either  $b + \alpha_m \in K(\alpha_m)^p$  for some prime  $p$  dividing  $n$  or  $4|n$  and  $b + \alpha_m \in -4K(\alpha_m)^4$ .

*Proof.* Let  $\alpha_{m+1}$  be a root of  $x^n - (b + \alpha_m)$  in an algebraic closure of  $K(\alpha_m)$ . Since  $\alpha_{m+1}^n - b = \alpha_m$ ,  $f_{m+1}(\alpha_{m+1}) = f_m(f(\alpha_{m+1})) = f_m(\alpha_{m+1}^n - b) = f_m(\alpha_m) = 0$  and so  $\alpha_{m+1}$  is a root of  $f_{m+1}$  such that  $K(\alpha_m) \subseteq K(\alpha_{m+1})$ .  $f_{m+1}$  is reducible over  $K$  if and only if  $[K(\alpha_{m+1}) : K] < \deg(f_{m+1}) = n^{m+1}$ . By assumption,  $f_m$  is irreducible over  $K$  and so  $[K(\alpha_{m+1}) : K] = [K(\alpha_{m+1}) : K(\alpha_m)][K(\alpha_m) : K] = n^m [K(\alpha_{m+1}) : K(\alpha_m)]$ . It follows that  $f_{m+1}$  is reducible over  $K$  if and only if  $[K(\alpha_{m+1}) : K(\alpha_m)] = n$ . Since  $\alpha_{m+1}$  is a root of  $x^n - (b + \alpha_m)$ ,  $f_{m+1}$  is reducible over  $K$  if and only if  $x^n - (b + \alpha_m)$  is reducible in  $K(\alpha_m)[x]$ . The proposition now follows from [L, Theorem 9.1, p. 297].  $\square$

As mentioned above, examples exist for every  $n \geq 2$  and  $m \geq 1$  of  $K$  and  $b \in K$  such that for  $f(x) = x^n - b$ ,  $f_m$  is irreducible over  $K$  but  $f_{m+1}$  is reducible. Our next result proves this assertion and also classifies such examples when  $n = 2$  and  $m = 1$ .

**Proposition 2.** (1) *Let  $n \geq 2$  and  $m \geq 1$ . Then there exists a field  $K$  and  $f(x) = x^n - b \in K[x]$  such that  $f_m$  is irreducible over  $K$  but  $f_{m+1}$  is reducible.*  
 (2) *Let  $K$  be an arbitrary field and let  $f(x) = x^2 - b \in K[x]$  be irreducible over  $K$ . Then  $f_2$  is reducible over  $K$  if and only if  $b = 4z^4/(4z^2 - 1)$  for some  $z \in K$  such that  $4z^2 - 1 \notin K^2$ .*

*Proof.* (1) Let  $F = \mathbb{C}(t)$  be the rational function field in one variable over  $\mathbb{C}$ , and let  $f(x) = x^n - t \in F[x]$ . By [O, Theorem 1, p. 101],  $f_r$  is irreducible in  $F[x]$  for every  $r \geq 1$  and has Galois group over  $F$  isomorphic to the  $r$ -fold wreath product  $[C_n]^r$  of the cyclic group  $C_n$  of order  $n$  with itself. Let  $E$  be the splitting field of  $f_{m+1}$  over  $F$ . By the proof of [FS, Lemma 1.1, p. 491], there exists  $\sigma \in \text{Gal}(E/F)$  such that  $\sigma$  acts as a  $n^m$ -cycle on the roots of  $f_m$  and as a product of disjoint  $n^m$ -cycles on the roots of  $f_{m+1}$ . (The proof of the existence of  $\sigma$  only used the fact that the Galois group of  $f_r$  is the  $r$ -fold wreath product  $[G]^r$  of a group  $G$  with itself such that  $G$  contains an  $n$ -cycle. This holds in our situation since the Galois group of  $f$  is cyclic of order  $n$  and acts transitively on the roots of  $f$ .) Taking  $K = E^{(\sigma)}$  as in [FS, Lemma 1.1, p. 491], it follows that  $f_m$  is irreducible in  $K[x]$  but  $f_{m+1}$  is reducible.

(2) Since  $\sqrt{b}$  is a root of  $f_1 = f$ , it follows from Proposition 1 that  $f_2$  is reducible over  $K$  if and only if  $b + \sqrt{b} = (z + w\sqrt{b})^2$  for some  $z, w \in K$ . Thus  $f_2$  is reducible over  $K$  if and only if there exist  $z, w \in K$  such that  $b = z^2 + w^2b$  and  $1 = 2zw$ . This implies that  $f_2$  is irreducible over  $K$  if  $K$  has characteristic 2. If the characteristic of  $K$  is different from 2, then solving the above equations simultaneously leads to  $w = 1/2z$  and  $b = 4z^4/(4z^2 - 1)$ . Since  $f$  is assumed to be irreducible over  $K$ ,  $4z^2 - 1 \notin K^2$  by Proposition 1. Conversely, if  $f$  has the given form, then  $f_2$  is reducible by the above argument.  $\square$

Suppose that  $K$  is the quotient field of a unique factorization domain  $R$  and  $b = b_1/b_2 \in K$  where  $b_1$  and  $b_2$  are relatively prime elements of  $R$ . Let  $f(x) = x^n - b$  and suppose that  $f_m$  is irreducible over  $K$  but  $f_{m+1}$  is reducible. We show next that this forces  $b_1$  and  $b_2$  to satisfy a certain Diophantine equation over  $R$ . An analysis of this equation for particular fields  $K$  will yield our main results.

**Theorem 3.** *Let  $K$  be the quotient field of a unique factorization domain  $R$  and let  $f(x) = x^n - (b_1/b_2) \in K[x]$  where  $b_1$  and  $b_2$  are relatively prime elements of  $R$ . Assume, for some  $m \geq 1$ , that  $f_m$  is irreducible in  $K[x]$  but  $f_{m+1}$  is reducible over  $K$ . Define a sequence of elements  $w_j$  of  $R$  by  $w_0 = -1$  and  $w_{j+1} = b_1^{n-1}w_j^n - b_2^{n^{j+1}-1}$  for  $j \geq 0$ . Then there exist a prime  $p$  dividing  $n$ , a unit  $u$  of  $R$ , and  $d, z \in R - \{0\}$  such that the following hold:*

- (1)  $b_1 = ud^p$ ,
- (2)  $(-1)^{n^m} u(u^{n-1}d^{p(n-1)}w_{m-1}^n - b_2^{n^m-1}) = z^p$ , and
- (3)  $d, w_{m-1}, b_2$ , and  $z$  are pairwise relatively prime non-zero elements of  $R$ .

*Proof.* We begin by proving by induction on  $j$  that for all  $j \geq 0$ ,  $w_j \neq 0$ ,  $w_j$  and  $b_1b_2$  are relatively prime, and  $f_j(-(b_1/b_2)) = b_1w_j/b_2^{n^j}$ . This is clear for  $j = 0$  since  $f_0(x) = x$  and  $w_0 = -1$ . Let  $j \geq 0$  and assume that  $w_j \neq 0$ ,  $w_j$  is relatively prime to  $b_1b_2$ , and  $f_j(-(b_1/b_2)) = b_1w_j/b_2^{n^j}$ . Since  $w_{j+1} = b_1^{n-1}w_j^n - b_2^{n^{j+1}-1}$ ,  $w_{j+1} \neq 0$  since  $b_1, b_2$ , and  $w_j$  are pairwise relatively prime. If a prime  $\pi$  of  $R$  divides both  $b_2$  and  $w_{j+1}$ , then  $\pi$  divides  $b_1^{n-1}w_j^n$ . Since  $R$  is a unique factorization domain,  $\pi$  must divide either  $b_1$  or  $w_j$ , contradicting either the relative primeness of  $b_1$  and  $b_2$  or the relative primeness of  $b_2$  and  $w_j$ . Similarly, no prime of  $R$  can divide both  $b_1$  and  $w_{j+1}$  and so  $w_{j+1}$  is relatively prime to  $b_1b_2$ . Finally,

$$\begin{aligned} f_{j+1}(-(b_1/b_2)) &= f(f_j(-(b_1/b_2))) = (b_1w_j/b_2^{n^j})^n - (b_1/b_2) \\ &= b_1(b_1^{n-1}w_j^n - b_2^{n^{j+1}-1})/b_2^{n^{j+1}} = b_1w_{j+1}/b_2^{n^{j+1}}, \end{aligned}$$

completing the induction.

Now let  $b = b_1/b_2$  and let  $\alpha_m$  be a root of  $f_m$ . Since  $f_m$  is irreducible over  $K$  but  $f_{m+1}$  is reducible, it follows from Proposition 1 that one of the following occurs. Either there exist a prime  $p$ ,  $p|n$ , and  $\beta \in K(\alpha_m)$  such that  $b + \alpha_m = \beta^p$  or  $4|n$  and there exists  $\gamma \in K(\alpha_m)$  with  $b + \alpha_m = -4\gamma^4$ . Let  $N$  denote the norm map from  $K(\alpha_m)$  to  $K$ . Since  $f_m$  is irreducible over  $K$  by assumption and has  $\alpha_m$  as a root,  $f_m(x - b)$  is the monic irreducible polynomial in  $K[x]$  having  $b + \alpha_m$  as a root. Since  $f_m$  has degree  $n^m$ , it follows that  $N(b + \alpha_m) = (-1)^{n^m} f_m(-b)$ . Define  $c \in K$  by  $c = N(\beta)$  if  $b + \alpha_m = \beta^p$  and by  $c = N(2\gamma^2)$  if  $b + \alpha_m = -4\gamma^4$ . If  $b + \alpha_m = \beta^p$ , then  $c^p = N(\beta^p) = N(b + \alpha_m) = (-1)^{n^m} f_m(-b)$ . Suppose that  $b + \alpha_m = -4\gamma^4$ . Then  $n$  is even and so  $[K(\alpha_m) : K]$  is even. It follows that  $N(-1) = 1$  and so  $c^2 = N((2\gamma^2)^2) = N(-4\gamma^4) = N(b + \alpha_m) = (-1)^{n^m} f_m(-b)$ . Thus, in either case we have  $(-1)^{n^m} f_m(-b) = c^p$  where  $p$  divides  $n$ . By the properties of the  $w_j$  established above,  $c^p = (-1)^{n^m} f_m(-b) = (-1)^{n^m} b_1w_m/b_2^{n^m}$ . Since  $b_1$  and  $w_m$  are non-zero,  $c$  is non-zero.

Let  $c = c_1/c_2$  where  $c_1$  and  $c_2$  are relatively prime elements of  $R$ . Then  $(-1)^{n^m} b_1w_m c_2^p = c_1^p b_2^{n^m}$ . Since  $b_1w_m$  divides  $c_1^p b_2^{n^m}$  and is relatively prime to  $b_2^{n^m}$ ,  $b_1w_m$  divides  $c_1^p$ . Since  $c_1$  and  $c_2$  are relatively prime, it follows that  $b_1, w_m$ , and  $c_2$  are pairwise relatively prime. Since  $p$  divides  $n$ ,  $p$  divides  $n^m$ . Let  $n^m = pk$ . Then  $c_1^p b_2^{n^m} = (c_1 b_2^k)^p$ . Since  $b_1$  is relatively prime to  $w_m c_2^p$  and  $(-1)^{n^m} b_1w_m c_2^p = (c_1 b_2^k)^p$ , it follows that  $b_1 = ud^p$  for some unit  $u \in R$  and some  $d \in R$ . Thus  $(-1)^{n^m} ud^p w_m c_2^p = (c_1 b_2^k)^p$  and so  $(-1)^{n^m} u w_m = (c_1 b_2^k / d c_2)^p$ . Let  $z = c_1 b_2^k / d c_2$ .  $z \neq 0$  since  $c \neq 0$ . Since  $z^p = (-1)^{n^m} u w_m \in R$  and  $R$  is integrally closed,  $z \in R$ . Finally,  $z^p = (-1)^{n^m} u w_m = (-1)^{n^m} u(b_1^{n-1}w_{m-1}^n - b_2^{n^m-1}) = (-1)^{n^m} u(u^{n-1}d^{p(n-1)}w_{m-1}^n - b_2^{n^m-1})$ , as was to be shown. Since  $b_1b_2$  and  $w_{m-1}$

were shown to be pairwise relatively prime earlier in the argument,  $d, w_{m-1}, b_2,$  and  $z$  are also pairwise relatively prime.  $\square$

As a consequence of Theorem 3, we obtain several large classes of  $f$  as above with the property that all iterates of  $f$  are irreducible.

**Corollary 4.** *Let  $K$  be the quotient field of a unique factorization domain  $R$  and let  $f(x) = x^n - b$  be irreducible in  $K[x]$  where  $b \in R$ . Then all iterates of  $f$  are irreducible if any of the following hold:*

- (1)  $b \notin uR^p$  for all units  $u$  of  $R$  and all primes  $p$  dividing  $n$ , or
- (2) the unit group,  $U(R)$ , of  $R$  is  $p$ -divisible for all primes  $p$  dividing  $n$ , or
- (3)  $n$  is even and  $U(R) = \{1, -1\}$ .

*Proof.* We apply Theorem 3 with  $b_1 = b$  and  $b_2 = 1$ . (1) is immediate from Theorem 3(1). Now suppose that there exists  $m \geq 1$  such that over  $R$ ,  $f_m$  is irreducible but  $f_{m+1}$  is reducible. By Theorem 3, there exist a prime  $p$  dividing  $n$ ,  $u \in U(R)$ , and  $d, z \in R$  such that  $b = ud^p$  and (\*):  $(-1)^{n^m} u(u^{n-1}d^{p(n-1)}w_{m-1}^n - 1) = z^p$ . If (2) holds, then there exists  $v \in U(R)$  such that  $u = v^p$ . But then  $b = ud^p = (vd)^p$  and so  $x^n - b$  is reducible over  $R$ , contrary to assumption. Thus we may assume that we are in case (3):  $p = 2$ ,  $n$  is even, and  $U(R) = \{1, -1\}$ . If  $u = 1$ , then  $x^n - b = x^n - d^2$  is reducible over  $R$  so we may assume that  $u = -1$ . Let  $n = 2k$  and let  $e = d^{n-1}w_{m-1}^k$ . By (\*),  $z^2 = -(-d^{2(n-1)}w_{m-1}^n - 1) = (d^{n-1}w_{m-1}^k)^2 + 1 = e^2 + 1$  and so  $-1 = e^2 - z^2 = (e - z)(e + z)$ . It follows that  $e - z, e + z \in U(R)$  and so either  $e - z = 1$  and  $e + z = -1$  or  $e - z = -1$  and  $e + z = 1$ . In either case,  $2e = 0$ . The characteristic of  $R$  is different from 2 since  $x^n - b = x^n + d^2$  is assumed to be irreducible over  $R$ . But then  $e = 0$ , a contradiction.  $\square$

Stoll [S, Corollary 1.3] proved that if  $f(x) = x^2 - b \in \mathbb{Z}[x]$  is irreducible over  $\mathbb{Q}$ , then so also are all of its iterates. In view of Corollary 4 we have the following improvement of Stoll’s result:

**Corollary 5.** *Let  $R$  be either  $\mathbb{Z}$  or a polynomial ring over either  $\mathbb{Z}$  or an algebraically closed field. Let  $f(x) = x^n - b \in R[x]$  be irreducible in  $R[x]$ . Then all iterates of  $f$  are irreducible in  $R[x]$ .*

Let the context be as in Corollary 4. As noted in Proposition 2, if  $b \notin R$ , then for  $n = 2$  there can exist  $b \in K$  such that  $f(x) = x^n - b$  is irreducible over  $K$  but  $f_2$  is reducible. We next consider the special case when  $K = F(t)$  where  $F$  is a field of characteristic 0 and show that this behavior cannot occur if  $n \geq 3$  and  $b$  is non-constant.

**Theorem 6.** *Let  $K = F(t)$  be the rational function field in one variable over a field  $F$  of characteristic 0, let  $n \geq 3$ , and let  $b \in K, b \notin F$ , be such that  $f(x) = x^n - b$  is irreducible over  $K$ . Then all iterates of  $f$  are irreducible over  $K$ .*

*Proof.* Assume, for some  $m \geq 1$ , that  $f_m$  is irreducible in  $K[x]$  but  $f_{m+1}$  is reducible over  $K$ . Let  $R = F[t]$  and let  $b = b_1/b_2$  where  $b_1$  and  $b_2$  are relatively prime polynomials in  $R$ . By Theorem 3, there exist a prime  $p$  dividing  $n$ ,  $u \in F$ , and polynomials  $d, z \in R$  so that  $b_1 = ud^p$  and  $(-1)^{n^m} u(u^{n-1}d^{p(n-1)}w_{m-1}^n - b_2^{n^m-1}) = z^p$ . Moreover,  $d, w_{m-1}, b_2,$  and  $z$  are pairwise relatively prime in  $R$ . Since  $b$  is not a constant by assumption and  $b_1 = ud^p$ , either  $d$  or  $b_2$  is not a constant. Let  $g = (-1)^{n^m} u^n d^{p(n-1)} w_{m-1}^n$  and  $h = -(-1)^{n^m} u b_2^{n^m-1}$ . Then  $g + h = z^p$  and the polynomials  $g, h,$  and  $z^p$  are pairwise relatively prime. Let  $\bar{F}$  be an algebraic

closure of  $F$ . For  $j \in F[t]$ , let  $\deg(j)$  denote the degree of  $j$  and let  $n_0(j)$  denote the number of distinct zeros of  $j$  in  $\overline{F}$ . Since  $g = (-1)^{n^m} u^n d^{p(n-1)} w_{m-1}^n$  and  $u \in F$ ,  $\deg(g) = p(n-1) \cdot \deg(d) + n \cdot \deg(w_{m-1})$ ; since  $d$  and  $w_{m-1}$  are relatively prime,  $n_0(g) \leq \deg(d) + \deg(w_{m-1})$ . We also have  $\deg(h) = (n^m - 1) \cdot \deg(b_2)$ ,  $n_0(h) \leq \deg(b_2)$ ,  $\deg(z^p) = p \cdot \deg(z)$  and  $n_0(z^p) \leq \deg(z)$ . Since  $g$ ,  $h$ , and  $z$  are pairwise relatively prime in  $F[t]$ ,  $n_0(ghz^p) = n_0(g) + n_0(h) + n_0(z^p)$ . By Mason's Theorem [L, Theorem 7.1, p. 194],  $\max\{\deg(g), \deg(h), \deg(z^p)\} < n_0(ghz^p)$ . In particular,

$$\begin{aligned} \max\{p(n-1) \cdot \deg(d) + n \cdot \deg(w_{m-1}), (n^m - 1) \cdot \deg(b_2) p \cdot \deg(z)\} \\ < \deg(d) + \deg(w_{m-1}) + \deg(b_2) + \deg(z). \end{aligned}$$

This leads to the equations:

- (1)  $p(n-1) \cdot \deg(d) + n \cdot \deg(w_{m-1}) < \deg(d) + \deg(w_{m-1}) + \deg(b_2) + \deg(z)$ ,
- (2)  $(n^m - 1) \cdot \deg(b_2) < \deg(d) + \deg(w_{m-1}) + \deg(b_2) + \deg(z)$ ,
- (3)  $p \cdot \deg(z) < \deg(d) + \deg(w_{m-1}) + \deg(b_2) + \deg(z)$ .

Adding equations (1), (2), and (3) together and simplifying, we obtain

$$(4) \quad (p(n-1) - 3) \cdot \deg(d) + (n-3) \cdot \deg(w_{m-1}) + (n^m - 4) \cdot \deg(b_2) + (p-3) \cdot \deg(z) < 0$$

Since  $n \geq 3$  by assumption and  $p|n$ , equation (4) is clearly impossible except possibly when  $n$  is even and  $p = 2$  or when  $n = 3, p = 3$ , and  $m = 1$ . Suppose first that  $n$  is even and  $p = 2$ . Then  $n \geq 4$  and from equations (3) and (4), we obtain

$$(2(n-1) - 3) \cdot \deg(d) + (n-3) \cdot \deg(w_{m-1}) + (n^m - 4) \cdot \deg(b_2) + \deg(z) < 2 \cdot \deg(z) < \deg(d) + \deg(w_{m-1}) + \deg(b_2) + \deg(z)$$

and so  $(2(n-1) - 4) \cdot \deg(d) + (n-4) \cdot \deg(w_{m-1}) + (n^m - 5) \cdot \deg(b_2) < 0$ . This is clearly impossible if  $n \geq 5$  or if  $n = 4$  and  $m \geq 2$ . Assume then that  $n = 4$  and  $m = 1$ . Then  $w_{m-1} = w_0 = -1$  has degree 0. Let  $D = \deg(d) + \deg(b_2) + \deg(z)$ . Then equations (1), (2), and (3) become  $6 \cdot \deg(d) < D$ ,  $3 \cdot \deg(b_2) < D$ , and  $2 \cdot \deg(z) < D$ . Thus  $1/6 > \deg(d)/D$ ,  $1/3 > \deg(b_2)/D$ , and  $1/2 > \deg(z)/D$ . Adding these equations together and using  $D = \deg(d) + \deg(b_2) + \deg(z)$ , we obtain  $1/6 + 1/3 + 1/2 > 1$ , a contradiction. Finally, suppose that  $n = 3, p = 3$ , and  $m = 1$ . Since  $w_{m-1} = w_0 = -1$ , equations (1), (2), and (3) become  $6 \cdot \deg(d) < D$ ,  $2 \cdot \deg(b_2) < D$ , and  $3 \cdot \deg(z) < D$  and so we obtain a contradiction exactly as above. □

Our last result treats the case when  $K = \mathbb{Q}$ , the rational field. We say that a triple  $(x, y, z)$  of integers is *primitive* if  $xyz \neq 0$  and  $x, y$ , and  $z$  are pairwise relatively prime.

**Theorem 7.** *Let  $n \geq 2$ . For each  $m \geq 1$ , let  $S(n, m)$  denote the set of  $b \in \mathbb{Q}$  such that, for  $f(x) = x^n - b$ ,  $f_m$  is irreducible in  $\mathbb{Q}[x]$  but  $f_{m+1}$  is reducible over  $\mathbb{Q}$ . Let  $S(n) = \bigcup_{m=1}^{\infty} S(n, m)$ . Then:*

- (1)  $S(2, 1)$  and  $S(2)$  are infinite.
- (2) If  $S(n)$  is non-empty for any odd  $n$ , then there exists a primitive solution to a generalized Fermat equation  $x^p + y^p = z^r$  where  $p$  is a prime dividing  $n$  and  $r \geq 3$  is even.

- (3) Let  $n$  be odd,  $n \geq 5$ . Then  $S(n)$  is finite and  $S(n) = \emptyset$  if  $n$  is not divisible by 3.
- (4)  $S(3, m)$  is finite for all  $m \geq 1$  and  $S(3, m) = \emptyset$  for  $m$  even and for  $m \leq 11$ .
- (5) The ‘abc’-conjecture implies that  $S(n)$  is finite for  $n$  even,  $n \geq 4$ .

*Proof.* (1) Let  $z$  be any integer divisible by 3 and let  $b = 4z^4/(4z^2 - 1)$ . Since  $4z^2 - 1 \equiv 2 \pmod{3}$ ,  $b \notin \mathbb{Q}^2$  and so  $f(x) = x^2 - b$  is irreducible in  $\mathbb{Q}[x]$ . By Proposition 2(2),  $f_2$  is reducible over  $\mathbb{Q}$  and so  $b \in S(2, 1)$ , proving (1).

Now let  $n \geq 3$  and suppose that  $b \in S(n, m)$  for some  $m \geq 1$ . Let  $f(x) = x^n - b$ , and let  $b = b_1/b_2$  where  $b_1, b_2 \in \mathbb{Z}$ ,  $b_2 > 0$ , and  $\gcd(b_1, b_2) = 1$ . By Theorem 3, there exist a prime  $p$  dividing  $n$ ,  $\epsilon \in \{1, -1\}$ , and  $d, z \in \mathbb{Z} - \{0\}$  such that  $b_1 = \epsilon d^p$  and  $(-1)^{n^m} \epsilon (\epsilon^{n-1} d^{p(n-1)} w_{m-1}^n - b_2^{n^m-1}) = z^p$ . The integers  $d, w_{m-1}, b_2$ , and  $z$  are non-zero and pairwise relatively prime.

We show first that  $S(3, 1) = \emptyset$ . Suppose that  $n = 3$  and  $m = 1$ . Then  $p = 3$  and  $w_{m-1} = w_0 = -1$ . It follows that  $(\epsilon z)^3 - d^6 = b_2^3$ ; Euler showed, however, that such integers do not exist [DG, p. 535]. Thus  $S(3, 1) = \emptyset$ .

Now let  $n = pk$  and  $x = d^{n-1} w_{m-1}^k$ . If  $n$  is odd, the triple  $(x, \epsilon z, b_2)$  is primitive and satisfies  $x^p + (\epsilon z)^p = b_2^{n^m-1}$ . Since  $S(3, 1) = \emptyset$ ,  $n^m - 1 > 3$ , proving (2).

Now let  $n^m - 1 = (n - 1)r$  and  $y = b_2^r$ . Then  $(y, x, z)$  is a primitive triple satisfying  $y^{n-1} = x^p + \epsilon z^p$  if  $n$  is odd and  $\epsilon y^{n-1} = x^p - z^p$  if  $n$  is even. If  $n$  is odd but not divisible by 3, then  $p \geq 5$ . In this case, results of Poonen, Darmon, and Merel show that primitive triples as above do not exist [K, p. 319]. This proves (3) unless  $n$  is odd and divisible by 3.

Suppose that  $1/p + 1/p + 1/(n - 1) < 1$ . Then there are only finitely many primitive triples  $(y, x, z)$  as above [DG, Theorem 2, p. 515]. Since  $d$  divides  $x$ , there are only finitely many possible values of  $d$  and since  $b_1 = \epsilon d^p$ , there are only finitely many possible values of  $b_1$ . Since  $y = b_2^r$ , there are only finitely many possible values of  $b_2$  and  $r$ . It follows that there are only finitely many possible values for  $b$  and since  $n^m - 1 = (n - 1)r$ , there are only finitely many possible values of  $m$ . Thus,  $S(n, m) = \emptyset$  for  $m$  sufficiently large and  $S(n, m)$  is finite for all  $m \geq 1$ . This proves that  $S(n)$  is finite if  $1/p + 1/p + 1/(n - 1) < 1$ . Since  $p$  divides  $n$ , this holds if  $n$  is odd and  $n \geq 5$ , or if  $n$  is even,  $n \geq 6$ , and  $p$  is odd. This proves (3) and reduces the proof of (5) to the case when  $p = 2$ .

Let  $l = n^m - 1$ . Since  $y = b_2^r$  and  $l = n^m - 1 = (n - 1)r$ , the triple  $(b_2, x, z)$  satisfies  $b_2^l = x^3 + \epsilon z^3$  if  $n = 3$  and  $\epsilon b_2^l = x^2 - z^2$  if  $n$  is even and  $p = 2$ .

Suppose first that  $n = 3$ . Then  $m \geq 2$  since  $S(3, 1) = \emptyset$ . Since  $l = 3^m - 1$ ,  $1/l + 1/3 + 1/3 < 1$ . By [DG, Theorem 2, p. 515], there are only finitely many triples  $(b_2, x, z)$  satisfying  $b_2^{3^m-1} = x^3 + \epsilon z^3$ . In particular, there are only finitely many possible values of  $b_2$  and  $x$ . It follows as above that there are only finitely many possible values of  $b$ . Thus  $S(3, m)$  is finite for  $m \geq 1$ . If  $m$  is even, then  $3^m - 1 = 4s$  and so the triple  $(b_2^s, x, \epsilon z)$  satisfies  $(b_2^s)^4 = x^3 + (\epsilon z)^3$ . This is impossible by [B, Theorem 1]. If  $3 \leq m \leq 11$ , then  $3^m - 1$  is divisible by an odd prime  $q < 10^4$ . Let  $3^m - 1 = qj$ . Then the triple  $(b_2^j, x, \epsilon z)$  satisfies  $(b_2^j)^q = x^3 + (\epsilon z)^3$ . This is impossible by [K, Theorem 10]. This completes the proof of (4).

Now suppose that  $n$  is even,  $n \geq 4$ , and  $p = 2$ . As shown above, the triple  $(b_2, x, z)$  satisfies  $\epsilon b_2^l = x^2 - z^2 = (x - z)(x + z)$ . Let  $x - z = 2^i u^l$  and  $x + z = 2^j v^l$  where  $u$  and  $v$  are odd. Then  $2x = 2^i u^l + 2^j v^l$  and  $2z = 2^j v^l - 2^i u^l$ . Since  $x$  and  $y$  are relatively prime,  $u$  and  $v$  are relatively prime and either  $i = j = 0$  or  $i \neq j$  and either  $i$  or  $j$  equals 1. Let  $w = w_{m-1}$ . Since  $x = d^{m-1} w^k$ , dividing by 2 if  $i \neq j$ ,

we obtain  $c_1 d^{n-1} w^k = c_2 u^l + c_3 v^l$  where the  $c_i$  are powers of 2 and where the triple  $(c_1 d^{n-1} w^k, c_2 u^l, c_3 v^l)$  is primitive.

For  $m$  a non-zero integer, let  $N_0(m)$  denote the product of the primes dividing  $m$ . In particular,  $N_0(m) \leq m$ . Let  $t = \max\{|c_1 d^{n-1} w^k|, |c_2 u^l|, |c_3 v^l|\}$  and let  $\alpha > 0$ . By the ‘*abc*’-conjecture [L, p. 196], there exists a positive integer  $C_0(\alpha)$  such that  $t \leq C_0(\alpha) N_0(|c_1 d^{n-1} w^k c_2 u^l c_3 v^l|)^{1+\alpha} = C_0(\alpha) N_0(|2d w u v|)^{1+\alpha} \leq C_1(\alpha) (|d w u v|)^{1+\alpha}$ . Since  $k = n/2 < n-1$ ,  $|d w| \leq |c_1 d^{n-1} w^k|^{1/k} = |c_1 d^{n-1} w^k|^{2/n} \leq t^{2/n}$ . Let  $\beta = 2/n + 1/l + 1/l$ . Since  $|u| \leq |c_2 u^l|^{1/l} \leq t^{1/l}$  and, similarly,  $|v| \leq t^{1/l}$ , it follows that  $t \leq C_1(\alpha) (|d w u v|)^{1+\alpha} \leq C_1(\alpha) t^{\beta(1+\alpha)}$ .

Suppose that  $\beta < 1$ . Choose  $\alpha > 0$  such that  $\beta(1+\alpha) < 1$ . There clearly can be only finitely many  $t$  satisfying  $t \leq C_1(\alpha) t^{\beta(1+\alpha)}$ . Since  $|d|$ ,  $|w|$ ,  $|u^l|$ , and  $|v^l|$  are each at most  $t$ , there are only finitely many possibilities for each of these. In particular, there are only finitely many possibilities for  $l = n^m - 1$  and so there are only finitely many possible values of  $m$ . Since  $x = d^{n-1} w^k$ , there are only finitely many possibilities for  $x$ . As above, this implies that there are only finitely many possible values of  $b_1$ . Since  $2x = 2^i u^l + 2^j v^l$ , there are only finitely many possibilities for  $i$  and  $j$ . Since  $z = x - 2^i u^{n-1}$ , there are only finitely many possibilities for  $z$ . Thus, there are only finitely many possible values for  $(x - z)(x + z) = \epsilon b_2^l$ . It follows that there are only finitely many possible values for  $b_2$  and hence for  $b$ . Since  $l = n^m - 1$ ,  $\beta < 1$  if and only if  $2/n + 2/(n^m - 1) < 1$ . In particular, this holds if  $n \geq 6$  or  $n = 4$  and  $m \geq 2$ . We have shown that, in these cases,  $S(n, m) = \emptyset$  for  $m$  sufficiently large and  $S(n, m)$  is finite if  $n \geq 6$  and  $m \geq 1$  or if  $n = 4$  and  $m \geq 2$ . Suppose then that  $n = 4$  and  $m = 1$ . Then  $(b_2, x, z)$  satisfies  $\epsilon b_2^3 = x^2 - z^2$ . Since  $w_0$  is defined in Theorem 3 to be  $-1$  and  $x = d^3 w_0^2$ , the triple  $(b_2, d, z)$  satisfies  $\epsilon b_2^3 = d^6 - z^2$ . In particular,  $(z, -\epsilon b_2, d)$  satisfies  $z^2 - (-\epsilon b_2)^3 = d^6$ . Bachet showed that the only primitive solutions to this equation are  $z = \pm 3$ ,  $-\epsilon b_2 = 2$ , and  $d = \pm 1$  [DG, p. 535]. Thus  $S(4, 1)$  is finite. (Although we do not need it for the proof of Theorem 7,  $S(4, 1)$  is, in fact, empty. Since  $b_2 > 0$ ,  $b_2 = 2$  and  $\epsilon = -1$ . Since  $b_1 = \epsilon d^2$ ,  $b_1 = -1$  and so  $b = b_1/b_2 = -1/2$ . Using a computer algebra package (e.g., Maple), one can verify that for  $f(x) = x^4 - (-1/2)$ ,  $f_2$  is reducible over  $\mathbb{Q}$  and so  $S(4, 1) = \emptyset$ .) This completes the proof of (5).  $\square$

*Remark.* It is a fundamental open question whether there exist any primitive triples  $(x, y, z)$  satisfying  $x^p + y^q = z^r$  with  $p, q$ , and  $r$  each  $\geq 3$ . Indeed, there are only ten such triples known where  $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ ; in each of these, one of the exponents equals 2. We refer the reader to [K] for an excellent survey of most of the known results in this area. In view of part (2) of Theorem 7, it is tempting to conjecture, at least for  $n$  odd, that if  $n \geq 3$  and  $f(x) = x^n - b$  is irreducible in  $\mathbb{Q}[x]$ , then so are all of its iterates; by part (3) of Theorem 7, this holds if  $n$  is odd and not divisible by 3. Next, we note that, although part (4) of Theorem 7 shows that  $S(3, m)$  is finite for all  $m \geq 1$ , we do not know whether  $S(3)$  is finite; we have not been able to rule out the possibility that  $S(3, m)$  is non-empty for infinitely many  $m$ . Finally, we note that if  $b \in S(3, m)$ , then  $b$  must be a 2-adic unit. For suppose that  $b \in S(3, m)$  for some  $m$ . By part (4) of Theorem 7,  $m \geq 13$  and so there exists an odd prime  $q \geq 7$  dividing  $3^m - 1$ ; the existence of such a  $q$  follows, for example, from Zsigmondy’s Theorem. We maintain the notation of the proof of Theorem 7. By [K, IV.6.1, Prop. 1],  $b_2$  is odd and the 2-adic valuation of  $xz$  is 1. Since  $d^2$  divides  $x$  and  $b_1 = d^3$ , this forces  $b_1$  to also be odd and so  $b$  is a 2-adic unit.

## ACKNOWLEDGEMENT

The authors would like to thank the anonymous referee for the proof of part (5) of Theorem 7 and for other valuable suggestions.

## REFERENCES

- [B] Nils Bruin, *On powers as sums of two cubes*, in Algorithmic Number Theory, Proceedings 4th International Symposium, ANTS-IV (W. Bosma, ed.), Lecture Notes in Computer Science 1838, Springer, New York, 2000, pp. 169-184.
- [DG] H. Darmon and A. Granville, *On the equations  $z^m = F(x, y)$  and  $Ax^p + By^q = Cz^r$* , Bull. London Math. Soc. **27** (1995), 513-543. MR **96e**:11042
- [FS] B. Fein and M. Schacher, *Properties of iterates and composites of polynomials*, J. London Math. Soc. **54** (1996), 489-497. MR **97h**:12007
- [K] A. Kraus, *On the equation  $x^p + y^q = z^r$ , A survey*, Ramanujan J. **3** (1999), 315-333. MR **2001f**:11046
- [L] S. Lang, *Algebra*, third edition, Addison-Wesley, Reading, 1993. MR **33**:5416 (review of first edition); MR **86j**:00003 (review of second edition)
- [O] R. W. K. Odoni, *Realizing wreath products of cyclic groups as Galois groups*, Mathematika **35** (1988), 101-113. MR **90a**:12013
- [S] M. Stoll, *Galois groups over  $\mathbb{Q}$  of some iterated polynomials*, Arch. Math. **59** (1992), 239-244. MR **93h**:12004

DEPARTMENT OF MATHEMATICS, ALBERTSON COLLEGE OF IDAHO, CALDWELL, IDAHO 83605  
*E-mail address*: [ldanielson@albertson.edu](mailto:ldanielson@albertson.edu)

DEPARTMENT OF MATHEMATICS, OREGON STATE UNIVERSITY, CORVALLIS, OREGON 97331  
*E-mail address*: [fein@math.orst.edu](mailto:fein@math.orst.edu)