Commun. Korean Math. Soc. **22** (2007), No. 2, pp. 183–194

COMPOSITION OF BINOMIAL POLYNOMIAL

EUNMI CHOI

ABSTRACT. For an irreducible binomial polynomial $f(x) = x^n - b \in K[x]$ with a field K, we ask when does the mth iteration f_m is irreducible but $m+1$th f_{m+1} is reducible over K. Let $S(n,m)$ be the set of b's such that f_m is irreducible but f_{m+1} is reducible over K. We investigate the set $S(n,m)$ by taking K as the rational number field.

1. Introduction

An iteration f_m $(m \geq 1)$ is the m-times composition $f \circ \cdots \circ f$ of a polynomial f, such as $f_1(x) = f(x)$ and $f_m(x) = f(f_{m-1}(x))$. For convenience, let $f_0(x) = x$. Let K be the field of quotient of a unique factorization domain R, and let $f(x) = x^n - b \in K[x]$ be an irreducible polynomial with nonzero, nonunit b over K. In [4], an interesting question was raised that under what conditions on K, n and b, are all iterates of $f(x)$ irreducible over K. If P is a property of polynomials, does the first m iterates of $f(x)$ possess P but the next iterate does not? It was studied in [9] in case P is irreducibility, separability, splitting completely or solvability by radical. We refer to the next property which will be used in this work.

Proposition 1. ([4, Theorem 3]) *Let K be the field of quotient of a unique factorization domain R, and $f(x) = x^n - \frac{b_1}{b_2} \in K[x]$ with relatively primes $b_1, b_2 \in R$. For some m, we assume f_m is irreducible but f_{m+1} is reducible over K. Then there exist a prime $p|n$, a unit $u \in R$, and d, z, $w_{m-1} \in R$ satisfying the followings:*

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

In fact, the sequence of w_i is defined by

$$w_0 = -1, \quad w_{j+1} = b_1^{n-1} w_j^n - b_2^{n^{j+1}-1} \text{ for } j \geq 0.$$

Received October 19, 2006.
2000 *Mathematics Subject Classification.* 12E05, 11D41.
Key words and phrases. iterated polynomial, Diophantine equation, ABC conjecture.

When $R = \mathbb{Z}$ (the integer ring), unit u is ± 1, so the equation in (2) Proposition 1 forms $\pm(d^{n-1}w_{m-1}^{\frac{n}{p}})^p \pm b_2^{n^m-1} = z^p$. Thus (3) provides relatively prime solutions to the equation $x^s + y^t = z^r$ for some $s, t, r > 1$.

Let $K = \mathbb{Q}$ (the rational field), and $S(n)$ be the set of $0 \neq b \in K$ such that $f(x) = x^n - b$ is irreducible but some iterates of f are reducible over $\mathbb{Q}$. It was shown ([4, Theorem 7]) that $S(2)$ is infinite, while $S(n)$ is finite if either $n \geq 5$ odd or $n \geq 4$ even with ABC conjecture. In order to describe, let

$$S(n,m) = \{b \in \mathbb{Q}^* \mid f(x) = x^n - b,\ f_m : \text{irreducible},\ f_{m+1} : \text{reducible over } \mathbb{Q}\}.$$

Then $S(n) = \bigcup_{m=1}^{\infty} S(n,m)$.

Lemma 2. [4] *Let the context be as above. Then*

(1) *$S(2,1)$ is infinite, and so is $S(2)$.*
(2) *$S(3,m)$ is finite for all m. Moreover $S(3,m) = \emptyset$ for m even and for $m \leq 11$.*
(3) *If $n > 3$ is odd, then $S(n)$ is finite. In particular $S(n) = \emptyset$ for $3 \nmid n$.*
(4) *If $n > 3$ is even, then $S(n)$ is finite by ABC conjecture. Moreover, $S(4,1) = \emptyset$, and $S(4,m)$ is finite for $m \geq 2$. And if $n \geq 6$ is even then $S(n,m)$ is finite for all m. In particular, $S(n,m) = \emptyset$ for large enough m.*

The purpose of this work is to investigate the set $S(n)$ intensively. When n is odd, $S(n)$ is determined in Theorems 10 through 13 if $3|n$, and in Theorem 14 if $3 \nmid n$. When n is even, $S(n)$ is studied in Theorems 15 and 17. A conclusion is obtained that $S(n,m)$ is empty for almost all n and m, except $S(2,1)$ with a series of examples in Corollary 18.

When $S(n)$ is empty, all iterates of $f(x) = x^n - b$ are irreducible so it is able to determine Galois group of $f(x)$ (refer to [12], [13] and [15], among others). On the other hand, if $S(n)$ is not empty, it can be seen that certain Diophantine equation has nontrivial solution due to Proposition 1.

2. Preliminaries

A Diophantine equation $\{s,t,r\} : x^s + y^t = z^r$ $(s,t,r \geq 2)$ is a generalization of the Fermat equation $x^m + y^m = z^m$. An integer triple (a,b,c) is called a solution of $\{s,t,r\}$ if $a^s + b^t = c^r$. Moreover it is primitive if $\gcd(a,b,c) = 1$, and nontrivial if $abc \neq 0$. Let $T(s,t,r)$ be the set of nonzero primitive solutions of $\{s,t,r\}$. Then due to Proposition 1, $T(s,t,r) \neq \emptyset$ for some $s,t,r \geq 1$ if $S(n) \neq \emptyset$ $(n > 0)$.

For $\{s,t,r\} : x^s + y^t = z^r$, the value $\chi = \frac{1}{s} + \frac{1}{t} + \frac{1}{r}$ plays a central role to determine the existence of solutions to permutations of $\{s,t,r\}$. If $\chi > 1$, then the possible sets for $\{s,t,r\}$ are permutations of $\{2,3,3\}$, $\{2,3,4\}$, $\{2,3,5\}$, and $\{2,2,r\}$ with $r \geq 2$. This type of equations has either none or infinitely many solutions ([1]). Indeed, solutions were founded when $\{s,t,r\} = \{3,3,2\}, \{2,3,4\}, \{2,4,3\}$ or $\{2,3,5\}$.

If $\chi = 1$, possible sets are permutations of $\{3,3,3\}$, $\{2,4,4\}$ and $\{2,3,6\}$, and it is long been known that no nontrivial solutions exist but $3^2+(-2)^3 = 1$.

If $\chi < 1$, it is often been conjectured that there are finitely many primitive solutions (Fermat-Catalan conjecture). The next theorem was proved in function field, and gives many applications to Fermat equation.

Proposition 3. (Mason theorem) *Let $a(t)$, $b(t)$ and $c(t) \in \mathbb{C}[t]$ be relatively prime polynomials. If $a+b=c$ then $\max\deg\{a,b,c\} \leq N(abc)-1$, where $N(f)$ is the number of distinct roots of a polynomial f.*

This can be applied to the Fermat theorem for polynomials which states that $x^m + y^m = z^m$ with $x(t), y(t), z(t) \in \mathbb{C}[t]$ has no solutions if $m \geq 3$. Mason theorem with respect to integers can be stated as the ABC conjecture posed by D.Masser and J.Oesterle in 1985.

Conjecture 4. (*ABC* [3, p.169]) *Let a, b, c be relatively prime integers. If $a + b = c$, then given $\varepsilon > 0$ there is $C(\varepsilon) > 0$ such that $\max\{|a|,|b|,|c|\} \leq C(\varepsilon)N(abc)^{1+\varepsilon}$, where $N(z)$ is the product of distinct prime divisors of an integer z.*

The ABC conjecture implies the asymptotic Fermat theorem which states that $x^m + y^m = z^m$ with $\gcd(x,y,z) = 1$ and sufficiently large m has no primitive solution. Hence $\{s,t,r\}$ has finitely many primitive solutions ([7]), while no primitive solution is expected when s, t and r are large enough ([11]). In particular $\{3,3,r\}$ has only trivial solution with large enough r. We record some results for Diophantine equations.

Proposition 5. *$T(3,3,r) = \emptyset$ if $r = 4, 5$ ([3, Theorem 1,2]), or if $r \geq 17$ with mild some conditions ([2], [10]), or if r is big enough with ABC conjecture ([3]).*

Proposition 6. *Assume the Shimura-Taniyama conjecture is true (: an elliptic curve over $\mathbb{Q}$ which is semi-stable at 2 and 3 is modular).*

(1) *$T(p,p,2) = \emptyset$ if $p \equiv 1 \pmod 4$ and prime $p > 13$* [6].
(2) *$T(p,p,3) = \emptyset$ if $p \equiv 1 \pmod 3$ and prime $p > 13$ is not Mersenne* [6].
(3) *$T(s,s,4) = \emptyset$ if $s \geq 3$* [6]. *In particular, $T(s,s,s) = \emptyset$ for $s \geq 3$.*
(4) *$T(3,3,p) = \emptyset$ if prime $3 \leq p < 10^4$* ([11]).
(5) *$T(3s,3t,p) = T(3s,p,3t) = \emptyset$ if $s,t \geq 2$ and prime $p \geq 3$* ([11]).
(6) *$x^3 + y^3 = z^p$ with even z and prime $p > 13$ has no primitive solution* ([7]).

We note that Shimura-Taniyama conjecture is now proven in all cases. So the assumption on the validity of the conjecture may be dropped.

Proposition 7. *For the equations $\{s,s,2\}$ and $\{s,s,3\}$,*

(1) *$T(s,s,2) = \emptyset$ if $s \geq 4$* ([14]). *And $T(4,t,4) = \emptyset$ if $t \geq 2$* ([5]).
(2) *$T(s,s,3) = \emptyset$ if $s \geq 3$ and Shimura-Taniyama conjecture is true* ([8], [14]).

Remark 1. We may refer to [7] for more results about solutions to permutations of $\{s,t,r\}$ with $\chi = \frac{1}{s}+\frac{1}{t}+\frac{1}{r}$.

i) If $\chi < 1$, only 10 solutions have been found so far. The first 5 small solutions are $1+2^3 = 3^2$, $2^5+7^2 = 3^4$, $7^3+13^2 = 2^9$, $2^7+17^3 = 71^2$, $3^5+11^4 = 122^2$ (B.Kelly, R.Scott, B.deWeger). And the 5 large solutions are $17^7+76271^3 = 21063928^2$, $1414^3+2213459^2 = 65^7$, $9262^3+15312283^2 = 113^7$, $43^8+96222^3 = 30042907^2$, $33^8+1549034^2 = 15613^3$ (Beukers, Zagier [1] by computer search).

ii) If $\chi = 1$, $x^2-y^3 = -z^6$ has no primitive solution (Euler), while $x^2-y^3 = z^6$ has no primitive solution but $(\pm 3, 2, \pm 1)$ (Catalan (1844), Bachet). $x^4 \pm y^4 = z^2$ has no primitive solution (Fermat (1636), Leibniz (1678)).

iii) If $\chi > 1$, there are either none or infinitely many solutions. Solutions of $x^2-y^2 = z^r$ are parametrized to $(u^r+2^{r-2}v^r)^2-(u^r-2^{r-2}v^r)^2 = (2uv)^r$. These are primitive if v is even and $(u,v)=1$.

iv) Solutions to $x^3+y^3 = z^2$ are splitted into two cases:

Euler (1756) : $x = \frac{a(a^3-8b^3)}{t^2}$, $y = \frac{4b(a^3+b^3)}{t^2}$, $z = \frac{a^6+20a^3b^3-8b^6}{t^3}$ with $\gcd(a,b) = 1$, $t = \gcd(a+b,3)$, a odd.

Hoppe (1859) : $x = \frac{a^4+6a^2b^2-3b^4}{t^2}$, $y = \frac{3b^4+6a^2b^2-a^4}{t^2}$, $z = \frac{6ab(a^4+3b^4)}{t^3}$ with $\gcd(a,b) = 1$, $t = \gcd(a+1,b+1,2)$, $3 \nmid a$.

v) More recently, Zagier (1993) presents 3 classes of parametrized solutions which yield all integral solutions to $x^3+y^3 = z^2$:

$x = a^4+6a^2b^2-3b^4$, $y = -a^4+6a^2b^2+3b^4$, $z = 6ab(a^4+3b^4)$

$x = \frac{1}{4}(a^4+6a^2b^2-3b^4)$, $y = \frac{1}{4}(-a^4+6a^2b^2+3b^4)$, $z = \frac{3}{4}ab(a^4+3b^4)$

$x = a^4+8ab^3$, $y = -4a^3b+4b^4$, $z = a^6-20a^3b^3-8b^6$.

vi) Examples: $11^3+37^3 = 228^2$, $143^3+433^2 = 42^4$, $3^4+46^2 = 13^3$, $10^2+3^5 = 7^3$.

3. Irreducibility of iteration

Lemma 8. $4|3^m-1$ *if and only if* $2|m$, *while* $5|3^m-1$ *if and only if* $4|m$.

Proof. If $m = 2k$ with $k \in \mathbb{Z}$ then $3^m \equiv 1 \pmod 4$. If $m = 2k+1$ then $3^{2k+1}-1 \equiv 2 \not\equiv 0$ by mod 4. If $m = 4k$ then $3^m \equiv 1 \pmod 5$. If $3^m \equiv 1 \pmod 5$ and $m = 4q+v$ for some q and $0 \le v < 4$, then $1 \equiv 3^m = (3^4)^q 3^v = 3^v \pmod 5$. Thus v is a multiple of 4, so $v = 0$. □

Lemma 9. *If* $\{p,p,r\} : x^p+y^p = z^r$ *has a primitive solution and if* $r = r_1r_2$ *with* $r_1, r_2 > 0$ *then so does* $\{p,p,r_1\} : x^p+y^p = z^{r_1}$.

Proof. Let (α,β,γ) be a primitive solution satisfying $x^p+y^p = z^r$. It is clear that $(\alpha,\beta,\gamma^{r_2})$ satisfies $x^p+y^p = z^{r_1}$ and $\gcd(\alpha,\beta,\gamma^{r_2}) = 1$. □

Hence, if $\{n,m,r\} : x^n+y^m = z^r$ has a primitive solution and if $n_1|n$, $m_1|m$, and $r_1|r$ then so does $\{n_1,m_1,r_1\} : x^{n_1}+y^{m_1} = z^{r_1}$.

We keep the notations $S(n) = \bigcup_{m=1}^{\infty} S(n,m)$ where $S(n,m) = \{b \in \mathbb{Q}^* \mid f(x)=x^n-b,\ f_m$: irreducible, f_{m+1} : reducible in $\mathbb{Q}\}$.

Theorem 10. *$S(3,m) = \emptyset$ for all $m \neq 13$ with ABC conjecture.*

Proof. Due to Lemma 2, $S(3,m) = \emptyset$ for $1 \leq m \leq 12$. If $b \in S(n,m)$, there is $f(x) = x^n - b = x^n - \frac{b_1}{b_2}$ with relatively primes b_1 and b_2 such that f_m is irreducible but f_{m+1} is reducible. By Proposition 1, there exist a prime divisor p of n, a unit u in $\mathbb{Z}$ and relatively prime integers d, w_{m-1}, b_2 and z satisfying the following equation, where we shall call it Eq(1) throughout the paper

$$\text{Eq(1):}\ \ (-1)^{n^m}\ u\big(u^{n-1}d^{p(n-1)}w_{m-1}^n\ -\ b_2^{n^m-1}\big) = z^p.$$

In $\mathbb{Z}$, $u = \pm 1$. Thus Eq(1) forms $d^6 w_{m-1}^3 - b_2^{3^m-1} = (-uz)^3$, for $n = 3$, $u^{n-1} = 1$ and $p = 3$. Hence $(uz)^3 + \big(d^2 w_{m-1}\big)^3 = b_2^{3^m-1}$ provides a primitive solution $\big(uz, d^2 w_{m-1}, b_2\big)$ to $\{3,3,r\} : x^3 + y^3 = z^r$ with $r = 3^m - 1$.

When m is even, it is proved in [4] that $S(3,m) = \emptyset$, in fact since $r = 3^m - 1$ is divisible by 4 by Lemma 8, Eq(1) equals

$$\{3,3,4\} : (uz)^3 + \big(d^2 w_{m-1}\big)^3 = (b_2^{\frac{3^m-1}{4}})^4$$

which is known to have no primitive solution due to Proposition 5, contradicting to the solution $\big(uz, d^2 w_{m-1}, b_2\big)$.

We shall assume m is odd which is not 13. Then $2|3^m - 1$ but $4 \not| 3^m - 1$ by Lemma 8, and Eq(1) can be translated to $(uz)^3 + \big(d^2 w_{m-1}\big)^3 = (b_2^2)^{\frac{3^m-1}{2}}$.

If m is small odd integers 3,5,7,9 or 11, then $\frac{3^m-1}{2}$ is equal to 13, $(11)^2$, 1093, (13)(757) and (23)(3851) respectively. By choosing a prime divisor q of $\frac{3^m-1}{2}$ as 13, 11, 1093, 13 and 23 respectively, Eq(1) can be regarded as an equation $\{3,3,q\}$ where $3 < q < 10^4$. Since the equation has no primitive solutions due to Proposition 6 (4), it contradicts to the solution to $\{3,3,r\}$. Hence $S(3,m) = \emptyset$.

If $m > 13$, it can be verified by Maple program that $\frac{3^m-1}{2}$ contains prime factors $q < 10^4$ for all odd $m < 150$ except $m \in \Omega = \{37, 59, 61, 71, 73, 79, 97, 101, 103, 107\}$. Hence Eq(1) forms $\{3,3,q\}$ with $3 \leq q \leq 10^4$, which has no primitive solution. Thus $S(n,m)$ should be empty for $13 < m < 150$ with only 10 exceptions in Ω.

When $m \in \Omega$, the smallest cases are $3^{37} - 1 = 2(17189128703)(13097927) > 10^{17}$ and $3^{59} - 1 > 10^{28}$. Moreover if $m \geq 151$ then $3^m - 1 > 10^{72}$ which are very large integers. By applying ABC to $\{3,3,r\} : x^3 + y^3 = z^{3^m-1}$ where $3^m - 1$ either has no small prime divisors $< 10^4$ or is a large enough integer $> 10^{72}$, it contradicts to the existence of solutions. So we conclude $S(3,m) = \emptyset$ for all $m \neq 13$. □

In summary, we have $S(3,m) = \emptyset$ for all $m \neq 13$:
(i) $S(3,m) = \emptyset$ if $m \leq 12$ ([4]), and
(ii) $S(3,m) = \emptyset$ if m is even (Theorem 7).
(iii) $S(3,m) = \emptyset$ if $m \leq 150$ and $m \notin \Omega = \{37, 59, 61, 71, 73, 79, 97, 101, 107\}$.
(iv) $S(3,m) = \emptyset$ if $m \in S$, or if $m > 150$ by ABC conjecture.

Theorem 11. *Let $n = 3^k$ $(k > 1)$. Then $S(n) = \emptyset$ if k is even. And $S(n, m) = \emptyset$ if m is even. Assuming ABC conjecture, $S(n, m) = \emptyset$ for all k and m.*

Proof. Assume $b = \frac{b_1}{b_2} \in S(n, m)$ with $(b_1, b_2) = 1$, i.e., $f(x) = x^n - b$, f_m irreducible but f_{m+1} reducible. The prime divisor p of n is 3, so Eq(1) forms

$$\left(d^{3^k-1} w_{m-1}^{3^{k-1}}\right)^3 + (uz)^3 = b_2^{3^{km}-1},$$

that provides a primitive solution to $\{3, 3, r\} : x^3 + y^3 = z^r$ with $r = 3^{km} - 1$.

If either m or k is even then $3^{km} - 1$ is divisible by 4 due to Lemma 8. Say $3^{km} - 1 = 4v$ for some $v \in \mathbb{Z}$. Then Eq(1) forms $\{3, 3, 4\}$ with a primitive solution $(d^{3^k-1} w_{m-1}^{3^{k-1}}, \pm z, b_2^v)$. But it contradicts to Proposition 6 (3). Thus $S(3^k) = \emptyset$ for all even k, and $S(3^k, m) = \emptyset$ for all even m.

We shall assume both m and k are odd. In particular if $m = 1$, then $w_0 = -1$ and Eq(1) is $\left(-d^{3^k-1}\right)^3 + (uz)^3 = b_2^{3^k-1}$. Since $3^k - 1$ is even (say $3^k - 1 = 2v$ for $v \in \mathbb{Z}$), the above equation can be translated to

$$(b_2^v)^2 - (uz)^3 = -(d^v)^6$$

having primitive solution (b_2^v, uz, d^v). This yields a contradiction to Euler (Remark 1 (i)) that $x^2 - y^3 = -z^6$ has no primitive solution Thus $S(3^k, 1) = \emptyset$.

Hence we shall investigate the set $S(3^k, m)$ with odd $m, k \geq 3$. Since $3^{km} - 1$ is divisible by both $3^m - 1$ and $3^k - 1$, we can express Eq(1) as

$$\text{either } \left(d^{3^k-1} w_{m-1}^{3^{k-1}}\right)^3 + (uz)^3 = \left(b_2^T\right)^{3^m-1}, \text{ or } \left(d^{3^k-1} w_{m-1}^{3^{k-1}}\right)^3 + (uz)^3 = \left(b_2^T\right)^{3^k-1}$$

for some $T \in \mathbb{Z}$, where both of them have primitive solutions. However when $m \neq 13$ or $k \neq 13$, it was discussed in Theorem 10 that the above equations do not have primitive solutions, so contradict.

Suppose $k = m = 13$. Since $r = 3^{km} - 1 = 3^{169} - 1$ has a small prime factor $2029 < 10^4$, we still can use Proposition 6 (4) to conclude no primitive solutions exist. Thus $S(3^k, m) = \emptyset$. □

Remark 2. For the sets $S(3^k, m)$, the only case we are left from Theorems 10 and 11 is when $k = 1$ and $m = 13$. Consider Eq(1) $\{3, 3, r\} : x^3 + y^3 = z^r$ for $r = 3^m - 1$. Since $r = 3^{13} - 1 = 1594322 = (2)(797161)$ with moderate length 7, neither Proposition 6 nor ABC conjecture can be applicable.

Suppose that $\{3, 3, 3^{13}-1\}$ has a solution. Then so does $\{3, 3, 2\}$ by Lemma 9. Due to Remark 1 (v), we can classify solutions to $\{3, 3, 2\}$ in 3 categories:

(i) uz or $d^2 w_{12}$ equals either $\alpha^4 + 6\alpha^2\beta^2 - 3\beta^4$ or $-\alpha^4 + 6\alpha^2\beta^2 + 3\beta^4$, and $b_2^{797161} = 6\alpha\beta(\alpha^4 + 3\beta^4)$

(ii) uz or $d^2 w_{12}$ equals either $\frac{1}{4}(\alpha^4 + 6\alpha^2\beta^2 - 3\beta^4)$ or $\frac{1}{4}(-\alpha^4 + 6\alpha^2\beta^2 + 3\beta^4)$, and $b_2^{797161} = \frac{3\alpha\beta}{4}(\alpha^4 + 3\beta^4)$

(iii) uz or $d^2 w_{12}$ equals either $\alpha^4 + 8\alpha\beta^3$ or $-4\alpha^3\beta + 4\beta^4$, and $b_2^{797161} = \alpha^6 - 20\alpha^3\beta^3 - 8\beta^6$.

Then with various α and β, we need to find integer solution $x = b_2$ of $x^{797161} - 6\alpha\beta(\alpha^4 + 3\beta^4) = 0$, or $x^{797161} - \frac{3\alpha\beta}{4}(\alpha^4 + 3\beta^4) = 0$, or $x^{797161} - \alpha^6 - 20\alpha^3\beta^3 - 8\beta^6 = 0$. We suppose for a moment that we have found integer solution b_2 from those equations of degree 797161. Since $w_{12} = b_1^2(b_1^2(b_1^2(b_1^2(b_1^2(b_1^2(b_1^2(b_1^2(b_1^2(b_1^2(-b_1^2 - b_2^2)^3 - b_2^8)^3 - b_2^{26})^3 - b_2^{80})^3 - b_2^{242})^3 - b_2^{728})^3 - b_2^{2186})^3 - b_2^{6560})^3 - b_2^{19682})^3 - b_2^{59048})^3 - b_2^{177146})^3 - b_2^{531440}$, we have relations $w_{12} = -b_1^{531440} + \cdots - b_2^{531440}$ and $b_1 = ud^3 = \pm d^3$ and $d^2 w_{12} = \Gamma$, where Γ equals one of $\pm\alpha^4 + 6\alpha^2\beta^2 \mp 3\beta^4$, $\frac{1}{4}(\pm\alpha^4 + 6\alpha^2\beta^2 \mp 3\beta^4)$, $\alpha^4 + 8\alpha\beta^3$ or $-4\alpha^3\beta + 4\beta^4$. It thus follows that $0 = d^2 w_{12} - \Gamma = d^2(-b_1^{531440} + \cdots - b_2^{531440}) - \Gamma = d^2(-d^{3\cdot 531440} + \cdots - b_2^{531440}) - \Gamma$.

By letting $x = d$ we have an equation of degree $531440 \cdot 3 + 2 = 1,594,322$ that

$$x^{1595322} + \cdots - b_2^{531440} x^2 + \Gamma = 0.$$

It seems to have few chance to find integer solution d, so that we have neither b_1 nor b, so contradicts to $b \in S(3,13)$. Thus $S(3,13)$ and $S(3)$ are empty.

It would be great if the set $S(3,13)$ can be determined explicitly.

Theorem 12. *Let $n \geq 5$ be odd divisible by 3 but not a power of 3. If m is even then $S(n,m) = \emptyset$ for all n. If $n \equiv 1$ by* mod 4 *or 5 then $S(n,m) = \emptyset$ for all m.*

Proof. Suppose $b = \frac{b_1}{b_2} \in S(n,m)$. Let $n = 3^k p_1^{e_1} \cdots p_l^{e_l}$ with distinct primes. The prime divisor of n is $p = 3$ or $p \geq 5$. Since $n^m - 1$ is even, Eq(1) forms

$$(uz)^p + \left(d^{n-1} w_{m-1}^{n/p}\right)^p = b_2^{n^m - 1} = \left(b_2^{(n^m-1)/2}\right)^2,$$

which gives a primitive solution to both $\{p, p, n^m - 1\} : x^p + y^p = z^{n^m - 1}$ and $\{p, p, 2\} : x^p + y^p = z^2$.

If $p \geq 5$ then no primitive solution of $\{p, p, 2\}$ by Proposition 7 yields a contradiction. So we must have $p = 3$. Since n is odd, $n \equiv \pm 1 \pmod 4$.

If m is even then $4 | n^m - 1$, so $\{3, 3, n^m - 1\}$ has no solution by Proposition 7.

If $n \equiv 1$ by mod 4 or 5 then $n^m - 1$ is a multiple by 4 or 5 for all m. Thus $\{3, 3, n^m - 1\}$ has no primitive solution by Proposition 6, so $S(n,m) = \emptyset$. □

By making use of Maple package program, we can compute $S(n)$ more precisely.

Theorem 13. *Let n be an odd integer divisible by 3.*

(1) *If $n \equiv 9, 21, 33, 45, 51, 57 \pmod{60}$ then $S(n) = \emptyset$.*
(2) *If $n \equiv 3, 15, 27, 39 \pmod{60}$ then $S(n) = \emptyset$ by ABC conjecture.*

Proof. Let $b = \frac{b_1}{b_2} \in S(n,m)$ with $(b_1, b_2) = 1$ and some m. Then with a prime divisor p of n and $r = n^m - 1$, Eq(1) forms $\{p, p, r\} : x^p + y^p = z^r$, that has primitive solutions $(uz, d^{n-1} w_{m-1}^{n/p}, b_2)$ where z, d, w_j, b_2 are defined in Proposition 1.

Due to Theorem 11 and 12, we may assume $m \geq 3$ is odd and $p = 3$. We classify every odd integer n divisible by 3 into five categories by Chineses remainder theorem.

If $n \equiv 0 \pmod 5$, then $n \equiv 15, 45 \pmod{60}$.

If $n \equiv 1 \pmod 5$, $n \equiv 21, 51 \pmod{60}$. If $n \equiv 2 \pmod 5$, $n \equiv 27, 57 \pmod{60}$.

If $n \equiv 3 \pmod 5$, $n \equiv 3, 33 \pmod{60}$. If $n \equiv 4 \pmod 5$, $n \equiv 9, 39 \pmod{60}$.

(1) If $n \equiv 9, 21, 33, 45, 51$ or $57 \pmod{60}$ then $n - 1$ is divisible by either 4 or 5, so is $r = n^m - 1$. Hence by Proposition 6, the equation $\{3, 3, r\}$ has no nontrivial primitive solution, a contradiction. So we have $S(n) = \emptyset$, this proves (1).

(2) We now consider four remaining cases $n \equiv 3, 15, 27, 39 \pmod{60}$.

(i) Let $n = 60k + 3$. Then $n - 1$ has odd prime factors $q < 10^4$ for all integers $k < 350$ (i.e., $n < 21003$) except for only k =337, 338, 344 (by using Maple). Since $q | r = n^m - 1$ for all m, $\{3, 3, r\}$ can be regarded as $\{3, 3, q\}$ having no primitive solution, hence lead to a contradiction. Thus $S(n) = \emptyset$ when $n = 60k + 3$ for $0 \leq k < 350$ but k =337, 338, 344.

If k =337, 338 and 344, then $n = 20223, 20283$ and 20643 which are the first 3 integers congruent to 3 by mod 60 such that $n - 1$ has no odd prime factor $< 10^4$. If $m = 3$ then prime factorizations for $n^m - 1$ are

$20223^3 - 1 = 2(19)(181)(10111)(118927)$;

$20283^3 - 1 = 2(7)(13)(10141)(4521103)$;

$20643^3 - 1 = 2(10321)(16633)(25621)$.

Cleraly, $S(20223, 3) = S(20283, 3) = \emptyset$. Though $20643^3 - 1$ has no small prime factor, $20643^3 - 1 > 10^{12}$ can be regarded as large enough to be $\{3, 3, r\}$ has only trivial primitive solution by ABC. So $S(20643, 3) = \emptyset$.

Similarly, for $m = 5$, the factorizations of $20223^5 - 1$, $20283^5 - 1$ and $20643^5 - 1$ show that $S(20223, 5) = S(20643, 5) = \emptyset$. We may also say $S(20283, 5) = \emptyset$, since $r = 20283^5 - 1 > 10^{21}$ is too large to provide a primitive solution to $\{3, 3, r\}$ by ABC.

When $m = 7$ and $k = 351$, $r = (60 \cdot 351 + 3)^7 - 1$ is of length 31, and moreover the values $(60(k + 1) + 3)^m - (60k + 3)^m$ and $(60k + 3)^{m+1} - (60k + 3)^m$ are of length 29 and 35 respectively. This shows that r increases very fast by just one increment of k (or m), hence in all cases we can conclude that $S(n, m) = \emptyset$ by ABC.

(ii) When $n = 60k + 15$, $n - 1$ has odd prime factors $q < 10^4$ for all $k \leq 350$ (i.e., $n \leq 22215$) except $k = 339, 342, 345, 349$, so $S(n) = \emptyset$. If k =339, 342, 345, 349, each $r = n^m - 1$ with $m = 3$ or 5 has odd prime factors $< 10^4$. The smallest values of k where r has no prime factors $< 10^4$ are 354 and 366 with respect to $m = 3$ and $m = 5$ respectively. However $21255^3 - 1$ (for $k = 354$) and $21975^5 - 1$ (for $k = 366$) are larger than 10^{13} which can be considered as big enough to be $\{3, 3, r\}$ have only trivial solution by ABC. Moreover, when $m = 7$and $k = 351$, $(60(k + 1) + 15)^m - (60k + 15)^m$ is of length 29, which

shows a huge increment. Therefore, $S(n,m) = \emptyset$ for $n \equiv 15 \pmod{60}$ and for all $m > 1$.

(iii) When $n = 60k+27$, $n-1$ has odd prime factors $q < 10^4$ for all $k < 350$ (i.e., $n < 21027$) but k =336, 341, 342, 343, 344, 348. For all the listed 6 k's, there are small odd prime factors $< 10^4$ of $r = n^m - 1$ with $m = 3$, and with $m = 5$ except only $k = 336$. Thus $\{3,3,r\}$ has only trivial solution. Furthermore ABC conjecture implies the nonexistence of primitive solution of $\{3,3,r\}$ when $k = 336$ and $m = 5$, because $r = 20187^5 - 1 > 10^{21}$. And, one step increase of $m \geq 7$ or $k \geq 351$ produces large leaps of r. Hence $S(n,m) = \emptyset$ by ABC.

Similar arguments go to $n = 60k + 39$ that $n - 1$ has odd prime factors $q < 10^4$ for all $k \leq 350$ (i.e., $n \leq 21039$) but some exceptions k =333, 334, 335, 336, 338, 345, 346, 347, 348. When $m = 3$, every $r = n^m - 1$ with all the above k's contains odd prime factors $q < 10^4$. The smallest case of r with no prime factors $< 10^4$ is when $k = 394$. But $23679^3 - 1 > 10^{13}$ is large enough having no solution of $\{3,3,r\}$. On the other hand when $m = 5$, $k = 333$ and 348 are the cases without prime divisors $< 10^4$ of r, and both $20019^5 - 1$ and $20919^5 - 1 > 10^{21}$. So $S(n) = \emptyset$. □

Remark 3. In Theorem 12, the situation left is when n is odd, multiple of 3 but not a perfect power of 3, and $n \not\equiv 1 \pmod 5$, $n \equiv -1 \pmod 4$. Those n are contained in the case $n \equiv 3, 15, 27, 39 \pmod{60}$ as in (2) Theorem 13.

Theorem 14. *If $n \geq 5$ is odd not divisible by 3 then $S(n) = \emptyset$.*

Proof. Assume contrary that $b = \frac{b_1}{b_2} \in S(n,m)$ for some $m \geq 1$. Since $n^m - 1 = 2v$ ($v \in \mathbb{Z}$), with a certain prime divisor p of n, Eq(1) forms $\left(d^{n-1}w_{m-1}^k\right)^p + (uz)^p = (b_2^v)^2$, which gives a primitive solution to $\{p,p,2\}$. But since $p \geq 5$, it contradicts to Proposition 7. So $S(n) = \emptyset$. □

All investigations above provide good evidence to be $S(n) = \emptyset$ if n is odd. From now on we assume n is even. It is known that $S(2)$ is infinite for $S(2,1)$ is infinite, while $S(4,1) = \emptyset$ (see [4]). We will prove $S(2^k,1) = \emptyset$ for all $k > 1$.

Theorem 15. *$S(2^k,1) = \emptyset$ for all $k > 1$.*

Proof. Let $n = 2^k$ and $b = \frac{b_1}{b_2} \in S(n,1)$ with $(b_1,b_2) = 1$. Then Eq(1) forms $(d^2)^{2^k-1} + (-ub_2)^{2^k-1} = z^2$. If $k = 2$, then $z^2 + (ub_2)^3 = d^6$ yields a primitive solution, and so $\{3,3,2\} : (d^2)^3 + (-ub_2)^3 = z^2$. It contradicts to Proposition 7. If $k > 2$, then $2^k - 1 \geq 7$. Since equation of the form $\{s,s,2\}$ ($s \geq 7$) has no primitive solution, it follows that $S(2^k,1) = \emptyset$ for all $k > 1$. □

Remark 4. In case $k = 2$, i.e., if $b = \frac{b_1}{b_2} \in S(4,1)$, the equation $z^2 + (ub_2)^3 = d^6$ can be written as $z^2 - (-ub_2)^3 = d^6$. Due to Remark 1 (ii) (Catalan (1844) and Bachet), $x^2 - y^3 = z^6$ has no primitive solution except $(\pm 3, 2, \pm 1)$. Suppose that $(z, -ub_2, d) = (\pm 3, 2, \pm 1)$.

If $u = 1$ then $b_2 = -2$ and $b_1 = ud^2 = 1$, so $b = \frac{b_1}{b_2} = -\frac{1}{2}$. Thus $f(x) = x^4 + \frac{1}{2}$ is irreducible but $f_2(x) = x^{16} + 2x^{12} + \frac{3}{2}x^8 + \frac{1}{2}x^4 + \frac{9}{16}$ is reducible. However it can be checked by Maple program that $f_2(x)$ is not reducible. If $u = -1$ then $b_2 = 2$, $b_1 = -1$ and $b = -\frac{1}{2}$. Hence, we have the same conclusion as above that $(\pm 3, 2, \pm 1)$ can not be the solution of $x^2 - y^3 = z^6$, so $S(4,1)$ should be empty.

Lemma 16. *For even $n \geq 4$ but $n \neq 2^k$, assume $b \in S(n,1)$ and the Shimura-Taniyama conjecture. Then the prime divisor p of n satisfying Eq(1) is $p \geq 5$.*

Proof. Write $b \in S(n,1)$ as $b = \frac{b_1}{b_2}$. Then $f(x) = x^n - \frac{b_1}{b_2}$ is irreducible while $f_2(x)$ is not. And there is a prime $p|n$ satisfying Eq(1): $d^{p(n-1)} - ub_2^{n-1} = z^p$.

If $p = 2$ or 3, then Eq(1) forms either $(d^2)^{n-1} + (-ub_2)^{n-1} = z^2$ or $(d^3)^{n-1} + (-ub_2)^{n-1} = z^3$ which have primitive solution, contradicting to Proposition 7 under Shimura-Taniyama conjecture. Thus $p \geq 5$. □

Theorem 17. *Assume the Shimura-Taniyama conjecture. Then $S(n,1) = \emptyset$ if either $n \equiv 4 \pmod 6$ or $n = 2^k p_1^{e_1} \cdots p_l^{e_l} > 4$ where k,e_i are all even and $3 \nmid n$.*

Proof. Due to Theorem 15, we may assume $n \neq 2^k$. If $n \equiv 4 \pmod 6$, then n is even ≥ 10 and $n \equiv 1 \pmod 3$. On the other hand, if $n = 2^k p_1^{e_1} \cdots p_l^{e_l}$ with even k,e_i, then $n = (n_0)^2$ with $2|n_0$, every $p_i \equiv \pm 1 \pmod 3$ and $n \equiv 1 \pmod 3$, since all e_i, k are even and $p_i \neq 3$. Thus in both cases, $n - 1$ is a multiple of 3. If $b \in S(n,1)$, then Eq(1) is $(d^{n-1})^p + (-z)^p = (ub_2)^{n-1}$ with a prime $p|n$, which provides a primitive solution to $\{p, p, 3\}$. But since $p \geq 5$ by Lemma 16, it follows from Proposition 7 that $\{p, p, 3\}$ has no primitive solutions. Thus $S(n,1) = \emptyset$. □

The infiniteness of $S(2,1)$ was verified in [4] by presenting polynomials $f(x) = x^2 - b$ with $b = \frac{4z^4}{4z^2-1}$ and $3|z$. Clearly $f(x)$ is irreducible over $\mathbb{Q}$ but $f_2(x)$ is reducible. In fact, if $z = 3$ then $f(x) = x^2 - \frac{324}{35}$ and

$$f_2(x) = x^4 - \frac{648}{35}x^2 + \frac{93636}{1225} = \frac{1}{1225}(35x^2 - 210x + 306)(35x^2 + 210x + 306).$$

Saying explicitly, if $z = 3t$ for some $t \in \mathbb{Z}$ then irreducible $f(x) = x^2 - \frac{(18t^2)^2}{(6t+1)(6t-1)}$ while reducible

$$\begin{aligned} f_2(x) &= x^4 - \frac{648t^4}{(6t+1)(6t-1)}x^2 + \frac{104976t^8}{(6t+1)^2(6t-1)^2} - \frac{324t^4}{(6t+1)(6t-1)} \\ &= \frac{1}{(6t+1)^2(6t-1)^2}[(36t^2-1)x^2 + (6t - 216t^3)x + (324t^4 - 18t^2)] \\ &\quad \cdot[(36t^2-1)x^2 - (6t - 216t^3)x + (324t^4 - 18t^2)]. \end{aligned}$$

Not only this, we construct lots of polynomials which is irreducible but its second iteration is reducible.

Corollary 18. *The set $S(2,1)$ is infinite.*

Proof. Let $b = \frac{b_1}{b_2} \in S(2,1)$. Consider an irreducible polynomial $f(x) = x^2 - b$ with reducible f_2. By taking $p = 2$, Eq(1) forms $d^2 - z^2 = ub_2$. Due to Remark 1 (iii), equations of the form $x^2 - y^2 = z^r$ (any $r \geq 1$) has infinitely many solutions, for $\chi = \frac{1}{2} + \frac{1}{2} + \frac{1}{r} > 1$, and its parametric solutions are obtained by

$$(\alpha^r + 2^{r-2}\beta^r)^2 - (\alpha^r - 2^{r-2}\beta^r)^2 = (2\alpha\beta)^r.$$

Moreover the solution is primitive if β is even and $(\alpha, \beta) = 1$. Thus Eq(1): $d^2 - z^2 = ub_2$ shows that

$$d = 2\alpha + \beta, \ z = 2\alpha - \beta, \ \text{ and } \ b_2 = 8\alpha\beta u$$

with even integer α and $(\alpha, \beta) = 1$. Since $b_1 = ud^2 = u(2\alpha + \beta)^2$, we get

$$b = \frac{b_1}{b_2} = \frac{(2\alpha + \beta)^2}{8\alpha\beta}.$$

By running Maple program for some small $1 \leq \alpha, \beta \leq 50$, we have the following table for b and $f(x) = x^2 - b$ which is irreducible but $f_2(x)$ is reducible.

(α, β)	$f(x)$	(α, β)	$f(x)$
$(2,5), (14,35)$	$f(x) = x^2 - 81/80$	$(2,21)$	$f(x) = x^2 - 625/336$
$(2,45)$	$f(x) = x^2 - 2401/720$	$(4,1)$	$f(x) = x^2 - 81/32$
$(8,33)$	$f(x) = x^2 - 2401/2112$	$(12,1)$	$f(x) = x^2 - 625/96$
$(12,25)$	$f(x) = x^2 - 2401/2400$	$(16,49)$	$f(x) = x^2 - 6561/6272$
$(18,13)$	$f(x) = x^2 - 2401/1872$	$(20,9)$	$f(x) = x^2 - 2401/1440$
$(24,1)$	$f(x) = x^2 - 2401/192$	$(28,25)$	$f(x) = x^2 - 6561/5600$
$(32,17)$	$f(x) = x^2 - 6561/4352$	$(36,49)$	$f(x) = x^2 - 14641/14112$
$(40,1)$	$f(x) = x^2 - 6561/320$	$(48,25)$	$f(x) = x^2 - 14641/9600$

For instance, irreducible polynomials $f(x) = x^2 - \frac{6561}{320}$ and $g(x) = x^2 - \frac{14641}{9600}$ yield reducible polynomials $f_2(x)$ and $g_2(x)$ that

$$f_2(x) = \frac{1}{102400}(320x^2 + 2880x + 6399)(320x^2 - 2880x + 6399)$$

$$g_2(x) = \frac{1}{92160000}(9600x^2 + 21120x + 8591)(9600x^2 - 21120x + 8591).$$

By taking various α and β, we have series of examples for $f(x)$. □

References

[1] F. Beukers, *The Diophantine equation* $Ax^p + By^q = Cz^r$, Duke Math. J. **91** (1998), 61–88.

[2] N. Bruin, *The Diophantine equations* $x^2 \pm y^4 = \pm z^6$ *and* $x^2 + y^8 = z^3$, Compositio Math. **118** (1999), 305–321.

[3] ———, *On powers as sums of two cubes, in Algorithmic Number theory*, Prod. 4th International Symp. Lecture Notes in Computer Science 1838, Springer, New York, (2000), 169–184.

[4] L. Danielson and B. Fein, *On the irreducibility of the iterates of* $x^n - b$, Proc. Amer. Math. Soc. **130** (2001), 1589–1597.

[5] H. Darmon, *The equation* $x^4 - y^4 = z^p$, C.R.Math. Rep. Acad. Sci. Canada **15** (1993), 286–290.
[6] ———, *The equation* $x^n + y^n = z^2$ *and* $x^n + y^n = z^3$, Int. Math. Res. Notices **10** (1993), 236–274.
[7] 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.
[8] H. Darmon and L. Merel, *Widning quotients and some variants of Fermat's Last Theorem*, J. Reine Angew. Math. **490** (1997), 81–100.
[9] B. Fein and M. Schacker, *Properties of iterates and composites of polynomials*, J. London Math. Soc. **54** (1996), 489–497.
[10] A. Kraus, *Sur l'equation* $a^3 + b^3 = c^p$, Experiment Math. **7** (1998), 1–13.
[11] ———, *On the equation* $x^p + y^p = z^r$, A survey, Ramanujan **3** (1999), 315–333.
[12] R. W. K. Odoni, *The Galois theory of iterates and composites of polynomials*, Proc. London Math. Soc. **51** (1985), 385–414.
[13] ———, *Realising wreath products of cyclic groups as Galois groups*, Mathematika **35** (1988), 101–113.
[14] B. Poonen, *Some Diophantine equations of the form* $x^n + y^n = z^m$, Acta Arith. LXXXVI **3** (1998), 193–205.
[15] M. Stoll, *Galois groups over* $\mathbb{Q}$ *of some iterated polynomials*, Arch. Math. **59** (1992), 239–244.

Department of Mathematics
Han Nam University
Daejon 306-791, Korea
E-mail address: emc@hannam.ac.kr