ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 33, Number 3, Fall 2003

SUMS OF BIQUADRATES AND CUBES IN $\mathbf{F}_q[t]$

LUIS GALLARDO

ABSTRACT. Every polynomial $P \in \mathbf{F}_q[t]$ where $\gcd(q,6) = 1$ and $q \notin \{5,13,17,25,29\}$, is a strict mixed sum of 11 biquadrates and it is also a strict sum of 16 biquadrates. For the strict mixed sum representation, a supplementary biquadrate is required for $q \in \{13,17,25,29\}$ and four supplementary biquadrates for $q = 5$. Every polynomial $P \in \mathbf{F}_q[t]$ where $\gcd(q,6) = 1$ and $q \notin \{7,13\}$ is a strict sum of 7 cubes. One supplementary cube is required for $q = 13$ and two for $q = 7$.

1. Introduction. In order to study the analogue of the Waring problem, and of the "easy" Waring problem over the ring $F[t]$, where F is a field, we fix some notation.

Let k be an integer greater than 1. Let F be a field, and let $P \in F[t]$ be a polynomial such that

$$P = c_1^k + \cdots + c_s^k,$$

for some polynomials $c_1, \ldots, c_s \in F[t]$ such that $\deg(c_i^k) < \deg(P) + k$ for all $i = 1, \ldots, s$. Then we say that P is restricted (or strict) sum of s kth powers. We also say that a polynomial $Q \in F[t]$ is a strict sum of kth powers if, for some integer $s \geq 1$, Q is a strict sum of s kth powers.

If k is even, then we can also consider sums and differences instead of merely sums in the above representation of P. If this is the case, then we replace the word "sum" by the words, "mixed sum."

In this paper we are interested in the case $F = F_q$, a finite field with q elements. More precisely, we study the case $k = 4$ and $k = 3$, for q such that $\gcd(q,6) = 1$.

We establish the following results in this paper.

a) Every polynomial $P \in \mathbf{F}_q[t]$ where $\gcd(q,6) = 1$ and $q \notin \{5,13,17,25,29\}$, is a strict mixed sum of 11 biquadrates, and it is also

Key words and phrases. Waring's problem, polynomials, biquadrates, cubes, finite fields.
Received by the editors on August 11, 2000, and in revised form on May 29, 2001.

a strict sum of 16 biquadrates. For the strict mixed sum representation, a supplementary biquadrate is required for $q \in \{13, 17, 25, 29\}$ and four supplementary biquadrates for $q = 5$ (see Theorem 1).

b) Every polynomial $P \in \mathbf{F}_q[t]$ where $\gcd(q, 6) = 1$ and $q \notin \{7, 13\}$ is a strict sum of 7 cubes. One supplementary cube is required for $q = 13$ and two for $q = 7$ (see Theorem 2).

For any $k > 3$, it is not known whether every polynomial in $F_q[t]$ is a strict sum or a strict mixed sum of kth powers. Furthermore, even if one or other of these properties is known to hold, it is not known (for all $k \geq 3$) what is the exact value of the minimal number $g_s(k, F_q[t])$, respectively $v_s(k, F_q[t])$, of kth powers that are required.

On the other hand, for a similar problem without restrictions on the degrees there are comprehensive results in [**7**]–[**10**].

However, there are some results on $g_s(3, F_q[t])$ that we will describe below.

First of all, assuming that q is even, and assuming that the polynomials to be represented are of *sufficiently high degree* and that they are already sums of cubes (this is required only for $q < 8$), it is proved in [**1**] that 11 cubes suffice, by use of the circle method.

More generally, this method is naturally adapted to study the representation of polynomials of sufficiently high degree by sums of kth powers when $\gcd(q, k!) = 1$. In these cases, with the assumption $0 < k < p$ where p is the characteristic of F_q, there are known upper bounds on the quantity $G_s(k, F_q[t])$, that is the analogue of $g_s(k, F_q[t])$ for these polynomials (see [**3**]). Otherwise, much more technical work is involved. The method does not give an explicit representation of those polynomials.

Recently (see [**4**]), we proved by applying an elementary constructive procedure that, for any positive integer n such that $n \notin \{1, 2, 4\}$, every polynomial $P \in \mathbf{F}_{2^n}[t]$ is a restricted sum of 9 cubes, and that 10 cubes suffice when $n = 4$.

On the other hand, the latter method gives only some partial information about how many representations exist for a given polynomial.

Similar elementary methods are used here to establish our results.

2. Main lemmas.

2.1 Some identities. The following results are easily checked.

First of all, we have the identity of Norrie (see [**2**, p. 729]).

Lemma 1 (Norrie). *Let F be a field of characteristic not equal to* 2. *Let $a, b, c \in F$ be such that $bc(b^8 - c^8) \neq 0$. Let $d = c^8 - b^8$.*

Then we have Norrie's identity:

(1)
$$t = \left(\frac{c^2(d+2t)}{2d}\right)^4 - \left(\frac{c^2(d-2t}{2d}\right)^4 + \left(\frac{2c^4t-b^4d}{2bcd}\right)^4 - \left(\frac{2c^4t+b^4d}{2bcd}\right)^4,$$

and two supplementary identities yielding biquadrates:

$$48t = (t+2)^4 - 2(t+1)^4 + 2(t-1)^4 - (t-2)^4, \tag{2}$$

$$8t^3 = (t+1)^4 - (t-1)^4 - 8t. \tag{3}$$

Remark. The lemma improves the result for the case $k = 4$ in [**7**, p. 295] when $A = F_q[t]$, provided $q > 5$. Norrie's identity (1) is vacuous for the field of 5 elements when (2) has to be used.

Next we have the identity of Serre, see [**9**] (slightly modified)

Lemma 2 (Serre). *Let F be a field of characteristic not equal to* 3, *in which there are two elements x, y such that $1 = x^3 + y^3$ and $xy \neq 0$. Let p be a nonzero element of F.*

Then we have Serre's identity:

$$t = \left(\frac{p^6(x^3+1)+t}{3xp^4}\right)^3 + \left(\frac{p^6(x^3-2)+t}{3yp^4}\right)^3 + \left(\frac{p^6(2x^3-1)-t}{3xyp^4}\right)^3, \tag{4}$$

and two supplementary identities yielding cubes:

$$6t^2 = (t+1)^3 - (t-1)^3 - 2, \tag{5}$$

$$90t = (t+4)^3 + (t-4)^3 - (t+1)^3 - (t-1)^3. \tag{6}$$

2.2 Sums of biquadrates and cubes in F_q.

Lemma 3. *Let F be a finite field of characteristic p with q elements. Suppose that $p > 3$. Then*

a) *Every element of F is a sum of 2 biquadrates if $q > 31$.*

b) *Every element of F is a sum of 3 biquadrates if $q \leq 31$ and $q \neq 5$.*

c) *Every element of F is a sum of 4 biquadrates if $q = 5$.*

d) *-1 is a sum of 2 biquadrates if $q \notin \{5, 29\}$.*

Proof. For $q > 41$, the first result follows from [**5**, p. 295] by specializing k to 4, while for $q \in \{37, 41\}$ it follows by direct computation. The other results are easily checked by direct computation.

Lemma 4. *Let F be a finite field of characteristic p with q elements. Suppose that $p > 3$. Then*

a) *Every element of F is a sum of 2 cubes if $q \neq 7$.*

b) *Every element of F is a sum of 3 cubes if $q = 7$.*

c) *1 is a sum of two nonzero cubes if $q \notin \{7, 13\}$.*

Proof. The first result follows from [**5**, p. 327] that refers to [**6**]. Another proof of (a) is obtained by specializing k to 3 in [**5**, p. 295]. The same specialization of k proves (c). The other result is easily checked by direct computation.

2.3 Descent. First we study the representation by sums of biquadrates.

Lemma 5. *Let F be a field of characteristic $p > 3$ in which every element is a sum of s biquadrates, where $4 \geq s \geq 1$. Let $n > 0$ be an integer and let $P \in F[t]$ be a polynomial of degree $m \in \{4n + 4, 4n + 3, 4n + 2, 4n + 1\}$.*

Then there exist polynomials $\{a, b, \ldots, g, R\} = \{A, B, A_1, B_1, C, D, E, R\}$ in $F[t]$ satisfying the conditions

1) A_1 *and* B_1 *are* 0 *if* $m \not\equiv 0 \pmod 4$,

2) $B = 0$ *if* $m \equiv 0 \pmod 4$ *and* $s = 3$,

3) B *and* B_1 *are* 0 *if* $m \equiv 0 \pmod 4$ *and* $s = 2$,

and such that

a) $P = a^4 + b^4 + c^4 + d^4 - e^4 + 8f^3 + 8g^3 + R$,

b) $\max(\deg(a, b, \ldots, g, R)) < m/4 + 1$.

Proof. Write

$$P = p_0 + \cdots + p_{4n+4}\, t^{4n+4}.$$

First of all, we study the case where P is monic and 4 divides m. We contend that $P = A^4 + Q$ where $\deg(A^4) = m$, $\deg(Q) = 3n + 3$ and the leading coefficient of Q is equal to 8. Write

$$A = \sum_{r=0}^{n} + a_r t^r + t^{n+1}.$$

By equating coefficients of t^k in the expansion of A^4 in powers of t with those of $P - 8t^{3n+3}$, for k descending from $4n + 3$ to $3n + 3$, we obtain $a_n, \ldots, a_0$ by solving the corresponding linear equations.

Since $P = -t^{4n+4} + (P + t^{4n+4})$, the cases where $m \not\equiv 0 \pmod 4$, reduce to the above one.

We can then suppose that 4 divides m and that P is not monic. Since the leading coefficient of P is a sum of s biquadrates, the same procedure as above yields $P = A^4 - B^4 + A_1^4 + B_1^4 + Q$ where A, B, A_1, B_1 are polynomials satisfying the conditions 2) and 3). Furthermore, we have

$$\max(\deg(A^4), \deg(B^4), \deg(A_1^4), \deg(B_1^4)) < m + 4,$$

$\deg(Q) = 3n + 3$ and the leading coefficient of Q is equal to 8.

Now, to represent Q in the desired form, by a similar argument we obtain

$$Q = 8C^3 + Q_1,$$

where $\deg(C) = n + 1$, $\deg(Q_1) = r$, where r is the closest multiple of 4 that is greater than or equal to $2n + 2$ and the leading coefficient of Q_1 is equal to 1.

Next, to represent Q_1 in the desired form, by a similar argument we obtain

$$Q_1 = D^4 + Q_2,$$

where $\deg(D) = r/4$, $\deg(Q_2) = s$, where s is the closest multiple of 3 that is greater than or equal to $3(n+1)/2$ and the leading coefficient of Q_2 is equal to 8.

Finally, to represent Q_2 in the desired form, by a similar argument we obtain

$$Q_2 = 8E^3 + R,$$

where $\deg(E) = s/3$ and $\deg(R) < m/4 + 1$.

This finishes the proof of the lemma.

We study now the representation of polynomials of degree less than or equal to 4.

Lemma 6. *Let F be a field of characteristic $p > 3$ in which every element is a sum of s biquadrates, where $4 \geq s \geq 1$. Let $P \in F[t]$ be a polynomial of degree $m \leq 4$. Then P is a strict mixed sum of $s+6$ biquadrates if $\operatorname{card}(F) > 5$, and of $s+8$ biquadrates if $\operatorname{card}(F) = 5$.*

Proof. For $m \leq 3$, we have for some $a \in F$, $P = -t^4 + (t+a)^4 + Q$, and for $m = 4$ we have $P = a_1^4 t^4 + \cdots + (a_s t + a)^4 + Q$, where $Q \in F[t]$ has $\deg(Q) = 3$, and the leading coefficient of Q is equal to 8. For some $b, c, d \in F$, we have $Q = 8(t+b)^3 + ct + d$. The result follows from identities (3) and (1) in Lemma 1 if $\operatorname{card}(F) > 5$ and, from the identities (3) and (2) in Lemma 1 if $\operatorname{card}(F) = 5$.

Next we study the representation by cubes.

Lemma 7. *Let F be a field of characteristic $p > 3$ in which every element is a sum of s cubes where $3 \geq s \geq 1$. Let $n \geq 0$ be an integer and let $P \in F[t]$ be a polynomial of degree $m \in \{3n+3,\ 3n+2,\ 3n+1\}$.*

Then there exist polynomials $\{a, b, \ldots, e, R\} = \{A, B, A_1, B_1, C, R\}$ in $F[t]$ satisfying the conditions

1) *A_1 and B_1 are 0 if $m \not\equiv 0 \pmod 3$,*

2) $B = 0$ *if* $m \equiv 0 \pmod 3$ *and* $s = 3$,

3) A_1 *and* B_1 *are* 0 *if* $s = 2$,

and such that

a) $P = a^3 + b^3 + c^3 + d^3 + 6e^2 + R$,

b) $\max(\deg(a, b, \ldots, e, R)) < m/3 + 1$.

Proof. Suppose that $n > 0$. The proof is similar to the first two steps (*mutatis mutandis*) of the proof of Lemma 5. For $n = 0$, the proof is similar to those of Lemma 6.

3. Representation by biquadrates. In this section and the next one, we specialize F to a finite field with q elements.

Theorem 1. *Every polynomial* $P \in \mathbf{F}_q[t]$, *where* $\gcd(q, 6) = 1$ *and* $q \notin \{5, 13, 17, 25, 29\}$, *is a strict mixed sum of* 11 *biquadrates, and it is also a strict sum of* 16 *biquadrates. For the strict mixed sum representation, a supplementary biquadrate is required for* $q \in \{13, 17, 25, 29\}$ *and four supplementary biquadrates for* $q = 5$.

Proof. Assume that $q > 5$. The result follows from Lemmas 5, 6 and 3, and from identities (3) and (1) in Lemma 1.

For example, if $m = \deg(P) \not\equiv 0 \pmod 4$ and $q > 31$, then in Lemma 5 a) there are three nonzero biquadrates ($A_1 = B_1 = 0$), so that $P = a^4 + b^4 - e^4 + 8f^3 + 8g^3 + R$. Apply (3) with $t = f$ and g to yield 4 more, and finally apply (1) with t replaced by what remains (a polynomial of degree $< m/4 + 1$). This yields the claimed 11 biquadrates for the strict mixed representation of P (6 of them with sign + and the remaining 5 with negative signs −.)

Now, with the help of Lemma 3 d) we convert the latter 5 biquadrates into 10 biquadrates with positive sign +. This yields the 16 claimed biquadrates for the strict sum representation of P, and so on for the other cases.

For $q = 5$ the proof is similar. We apply identity (2) in Lemma 1 instead of Norrie's identity (1) in Lemma 1.

Remark 1. The upper bounds for $g_s(4, F_q[t])$ when $q \in \{5, 13, 17, 25, 29\}$ can be easily deduced from Theorem 1 and from Lemma 3.

Remark 2. We do not know whether our bounds are best possible. Indeed it seems to be a difficult problem to establish nontrivial lower bounds for $v_s(4, F_q[t])$ or for $g_s(4, F_q[t])$.

4. Representation by cubes.

Theorem 2. *Every polynomial* $P \in \mathbf{F}_q[t]$ *where* $\gcd(q, 6) = 1$ *and* $q \notin \{7, 13\}$ *is a strict sum of* 7 *cubes. One supplementary cube is required for* $q = 13$ *and two for* $q = 7$.

Proof. Assume that $q \notin \{7, 13\}$. The result follows from Lemmas 7 and 4, from identity (5) in Lemma 2 and from Serre's identity (4) in Lemma 2.

For example, since $q \neq 7$, Lemma 4 a) tells us that in Lemma 7 a) there are 2 nonzero cubes ($A_1 = B_1 = 0$), so that $P = a^3 + b^3 + 6c^2 + R$. Apply (5) with $t = c$ to yield 2 more, and finally apply (4) with t replaced by what remains (a polynomial of degree $< m/3 + 1$). This yields the claimed 7 cubes for the strict representation of P.

For $q \in \{7, 13\}$ the proof is similar. We apply identity (6) instead of identity (4) in Lemma 2.

Remark 3. We do not know whether our bounds are best possible. Indeed it seems to be a difficult problem to establish nontrivial lower bounds for $g_s(3, F_q[t]) = v_s(3, F_q[t])$.

5. Acknowledgments. The author thanks the two anonymous referees for their useful comments that improved the presentation of the paper. He especially thanks the anonymous referee that pointed out the special case when $q \in \{37, 41\}$ that resulted in an improved Lemma 3.

REFERENCES

1. M. Car and J. Cherly, *Sommes de cubes dans l'anneau* $F_{2^h}[X]$, Acta Arith. **65** No. 3 (1993), 227–241.

2. L.E. Dickson, *History of the theory of numbers*, Volume II, *Diophantine analysis*, Chelsea Publ. Co., New York, 1992.

3. G. Effinger and D. Hayes, *Additive number theory of polynomials over a finite field*, Oxford Math. Monographs, Clarendon Press, Oxford, 1991.

4. L. Gallardo, *On the restricted Waring problem over* $F_{2^n}[t]$, Acta Arith. **XCII.2** (2000), 109–113.

5. R. Lidl and H. Niederreiter, *Finite fields*, Encylopedia Math. Appl., Vol. 20, Cambridge Univ. Press, Cambridge, 1984, reprinted 1987.

6. S. Singh, *Analysis of each integer as sum of two cubes in a finite integral domain*, Indian J. Pure Appl. Math. **6** (1975), 29–35.

7. L.N. Vaserstein, *Waring's problem for algebras over fields*, J. Number Theory **26** (1987), 286–298.

8. ———, *Waring's problem for commutative rings*, J. Number Theory **26** (1987), 299–307.

9. ———, *Sums of cubes in polynomial rings*, Math. Comp. **56** (1991), 349–357.

10. ———, *Ramsey's theorem and the Waring's problem for algebras over fields*, Proc. of Workshop on the Arithmetic of Function Fields (Ohio State Univ., 1991), de Gruyter Verlag, Berlin, 1992, pp. 435–442.

Department of Mathematics, University of Brest, 6, Avenue Le Gorgeu, 29285 Brest Cedex, France
E-mail address: Luis.Gallardo@univ-brest.fr