ACTA ARITHMETICA
149.1 (2011)

Büchi's problem in any power for finite fields

by

HECTOR PASTEN (Concepción and Kingston)

1. Introduction. In an unpublished work of J. R. Büchi communicated by Lipshitz (see [11]), the following number-theoretical question was formulated:

QUESTION 1.1 ($\mathbf{BP}^2(\mathbb{Z})$). Does there exist an integer M such that, if a sequence of length M formed by integer squares has constant second differences equal to 2, then necessarily the squares are of the form $(\nu+1)^2, (\nu+2)^2, \ldots, (\nu+M)^2$ for some integer ν?

A positive answer to this problem would imply a very strong undecidability result for $\mathbb{Z}$ improving the known negative answer to Hilbert's Tenth Problem (see [11, 12]).

If σ is a sequence in a ring, we will denote by $\Delta^{(k)}\sigma$ the sequence of its kth differences. One can extend Büchi's problem in a natural way to other powers and (commutative unitary) rings (see [15] for implications in logic).

QUESTION 1.2 ($\mathbf{BP}^k(\mathbb{Z})$). Does there exist an integer M such that, if a sequence of integers $(x_i)_{i=1}^M$ satisfies $\Delta^{(k)}(x_i^k)_{i=1}^M = (k!, \ldots, k!)$ then there exists an integer ν such that $x_i^k = (\nu+i)^k$ for each i?

Over $\mathbb{Z}$, these are open problems for all $k \geq 2$. In the case $k = 2$ a lot of progress has been achieved. See for example [8, 19, 16, 17]. We also refer the reader to [14] for a survey on Büchi's problem.

On the other hand, the *only* known example of a positive answer to $\mathbf{BP}^k(A)$ with $k > 2$ is for $A = F[z]$ and $k = 3$ (see [18]). The aim of this paper is to provide, for any $k \geq 2$, examples of rings A where $\mathbf{BP}^k(A)$ has a positive answer. Unfortunately, the examples shown below do not give new results in logic (in an obvious way) since the rings considered are finite.

Before stating our results, let us introduce some notation.

2010 *Mathematics Subject Classification*: Primary 11T55; Secondary 11D85.
Key words and phrases: Büchi's problem, n squares problem.

DOI: 10.4064/aa149-1-4

Notation 1.3.

(1) If S is a set, $|S|$ denotes the cardinality of S.
(2) $P(K,k)$ is the set of kth powers in the field K.
(3) If F is a polynomial, $\mathbb{V}(F)$ is the zero locus of F.

Theorem 1.4. *Let $k \geq 2$ be an integer, c its least prime factor and p a prime of the form $kl+1$ such that $p > 4k^2$. Consider the constant*

$$M = \left\lfloor \frac{1}{c}p + (k-1)\sqrt{p} - k \right\rfloor$$

and let $f \in \mathbb{F}_p[x]$ be a monic polynomial of degree k. We have $M \leq p$ and, if $f(n)$ is a kth power for at least M values of $n \in \mathbb{F}_p$ then f is a kth power in $\mathbb{F}_p[x]$. Moreover, in the particular case $k = 2$ the result holds with $M = (p+3)/2$ and for any odd prime.

As a consequence of the above result, we solve the problem $\mathbf{BP}^k(\mathbb{F}_p)$ (see Section 2).

Corollary 1.5. *Let $k \geq 2$ be an integer. The problem $\mathbf{BP}^k(\mathbb{F}_p)$ has a positive answer for any prime $p > 4k^2$ of the form $kl+1$, taking*

$$M = \left\lfloor \frac{1}{c}p + (k-1)\sqrt{p} - k \right\rfloor$$

where c is the least prime divisor of k. Moreover, $\mathbf{BP}^2(\mathbb{F}_p)$ has a positive answer for any prime $p > 2$, with $M = (p+3)/2$.

Known results on incomplete character sums give the following improvement of Corollary 1.5 (see Section 3).

Corollary 1.6. *Let $k \geq 2$ be an integer and consider p ranging in the set of primes of the form $kl+1$. For p large enough, the problem $\mathbf{BP}^k(\mathbb{F}_p)$ has a positive answer with constant $M = M(p)$ where $M(p) = \mathcal{O}(p^{1/2}\log p)$.*

The approach to Büchi's Problem by means of Theorem 1.4 seems relevant because of its analogy with the following result in the case of fields of functions (see [13]).

Theorem 1.7. *Let A be the field of p-adic meromorphic functions over the field $\mathbb{C}_p$, the field of complex meromorphic functions, or the function field of a curve in characteristic zero. There exists a (computable) constant M depending on A such that the following holds: for any monic polynomial $P \in A[X]$ of degree two, if $P(a)$ is a square in A for at least M values of a in the constant field of A, then either P has constant coefficients or P is a square in $A[X]$.*

For some related results in the context of finite fields, see for example [3–7, 9]. In these works, the authors investigated the problem of showing that a polynomial (possibly in several variables) over a finite field with all its values being kth powers, must be a kth power. We improve these results for the class of polynomials $f \in \mathbb{F}_p[x]$ by effectively bounding the number of elements in $\mathbb{F}_p$ where it is enough to check whether the value of f is a kth power or not, in order to conclude that f is itself a kth power or not.

2. Representation of kth powers by a polynomial of degree k

NOTATION 2.1. Let $k \geq 2$ be an integer and let A be an integral domain such that the polynomial $x^k - 1 \in A[x]$ has all its zeros in A. We define μ_k as the multiplicative group formed by the zeros of $x^k - 1$. It is clear that μ_k is cyclic. Note that if d divides k then $x^d - 1$ has all its zeros in A and μ_d is a subgroup of μ_k.

LEMMA 2.2. *Let $k \geq 2$ be an integer, let A be an integrally closed domain containing μ_k, and let $a \in A$ be a non-zero element. Let $d \geq 1$ be the largest integer dividing k such that a is a dth power in A and fix a root $b = \sqrt[d]{a} \in A$. Write $e = k/d$. Consider the following factorization of $y^k - a$ in $A[y]$:*

$$y^k - a = \prod_{\epsilon^d = 1} (y^e - \epsilon b) \tag{2.1}$$

where the product takes into account the multiplicities of the zeros of $x^k - 1$. Then (2.1) *is the factorization of $y^k - a$ into irreducible elements of $A[y]$.*

Proof. We know that each irreducible factor in $A[y]$ is non-constant (that is, not in A), because $y^k - a$ is a monic polynomial. Write F for the field of fractions of A. Since A is integrally closed, d is the largest integer dividing k such that a is a dth power in F, and we reduce the factorization problem to $F[y]$ where we can conclude by applying standard results in Kummer theory. ■

LEMMA 2.3. *Let $k \geq 2$ be an integer, let K be a field of characteristic $p > 0$ and choose an algebraic closure Ω_p for K. If a polynomial $h \in K[x]$ is a kth power in $\Omega_p[x]$, then h can be written in the form $h = \alpha g^k u$ where $\alpha \in K$, $g \in K[x]$ is monic, and $u \in K[x^p]$ is a monic polynomial not divisible by a non-constant kth power in $K[x]$.*

Proof. Write h in the form $h = \alpha g^k u$ where $\alpha \in K$, $g \in K[x]$ is monic and has degree as large as possible, and $u \in K[x]$ is monic. If u is constant we are done, so we assume that u is non-constant. Since h is a kth power in $\Omega_p[x]$ it follows that u is a kth power in $\Omega_p[x]$, hence, each root of u in Ω_p has multiplicity at least k. On the other hand, each irreducible factor of u in $K[x]$ has multiplicity at most $k-1$ by definition of g, therefore the irreducible factors of u are not separable and $u \in K[x^p]$. ■

COROLLARY 2.4. *Let $k \geq 2$ be an integer, let K be a field of characteristic $p > k$ containing all the kth roots of* 1, *and let $f \in K[x]$ be a monic* *polynomial of degree k. Write d for the largest integer dividing k such that f is a dth power in $K[x]$, fix $g \in K[x]$ satisfying $f = g^d$ and define $e = k/d$. The polynomial g can be chosen monic and the factorization of the polynomial $y^k - f \in K[x,y]$ into irreducible elements of $K[x,y]$ is*

$$y^k - f = \prod_{\epsilon \in \mu_d} (y^e - \epsilon g)$$

where each factor is absolutely irreducible.

Proof. Since f is monic, its dth roots have as leading coefficients the elements of μ_d, hence we can take g monic.

Write $F = y^k - f$. Since the total degree of F is the same as the degree in x and in y, each non-constant factor of F must depend on both x and y. Hence, instead of considering the factorization of F in $K[x,y]$ we will rather consider the factorization of F in $K[x][y]$. By Lemma 2.2, the only remaining part is to show that the factors $y^e - \epsilon g$ are absolutely irreducible.

Assume that $y^e - \epsilon g$ is reducible in $\Omega_p[x,y]$ where Ω_p is an algebraic closure of K. Since the total degree of $y^e - \epsilon g$ is the same as the degree in x and in y, each non-constant factor of it must depend on both x and y. Hence $y^e - \epsilon g$ is reducible in $\Omega_p(x)[y]$ and Lemma 2.2 implies that ϵg is a rth power in $\Omega_p(x)$ for some $r > 1$ dividing e, hence in $\Omega_p[x]$. Note that ϵg has no non-constant factor in $K[x^p]$ because $k < p$; moreover, g is monic and the only s dividing e such that g is an sth power in $K[x]$ is $s = 1$, by maximality of d. This contradicts Lemma 2.3. ∎

Definition 2.5. If K is a field, k an integer and $f \in K[x]$ a polynomial, then we define the set

$$S(K,k,f) = \{x \in K \colon f(x) \in P(K,k)\}.$$

Proposition 2.6. *Let $k \geq 2$ be an integer and p be a prime of the form $kl + 1$. Let $f \in \mathbb{F}_p[x]$ be a monic polynomial of degree k and let d be the largest divisor of k such that f is a dth power in $\mathbb{F}_p[x]$. If we write $e = k/d$ then*

$$|S(\mathbb{F}_p,k,f)| \leq \frac{1}{e}(p+1) + \frac{(e-1)(e-2)}{e}\sqrt{p} + k - 2.$$

Proof. Since $p = kl + 1$, $\mathbb{F}_p$ contains k different kth roots of 1. Define $F = y^k - f(x) \in \mathbb{F}_p[x,y]$ and let $Z = \mathbb{V}(F) \subseteq \mathbb{A}^2$ be the zero locus of F. By Corollary 2.4, Z has d reduced absolutely irreducible components $X_1, \ldots, X_d$ each one of degree e. By the Riemann Hypothesis for curves (see [1] for the case of singular curves) we conclude that the number of $\mathbb{F}_p$-rational points of the projective closure of each X_i is at most

$$p + 1 + (e-1)(e-2)\sqrt{p}.$$

The projective closure of Z meets the line at infinity at the points $[1:\epsilon:0]$ where ϵ ranges in μ_k, therefore we get

$$|Z(\mathbb{F}_p)| \leq d(p+1) + d(e-1)(e-2)\sqrt{p} - k. \tag{2.2}$$

A similar bound would be obtained from Exercise 6.67 in [10] applied to this case:

$$|Z(\mathbb{F}_p)| \leq d(p+1) + d(e-1)(e-1)\sqrt{p} - d. \tag{2.3}$$

Let us now estimate $|Z(\mathbb{F}_p)|$ in a different way. We write $P = P(\mathbb{F}_p, k)$ and $S = S(\mathbb{F}_p, k, f)$. Note that a point $(x, y) \in Z(\mathbb{F}_p)$ is a solution of the system

$$\begin{cases} f(x) = r, \\ y^k = r, \end{cases}$$

where $r \in P$. Let us write

$$S_r = \{x \colon f(x) = r\}.$$

It is clear that the sets S_r are disjoint. Indeed they form a partition of S because by hypothesis we have $f(x) \in P$ if and only if $x \in S$. Since $\deg f = k$, for each $r \in P$ we have $|S_r| \leq k$. Also, since $p = kl + 1$, the second equation has k solutions for each non-zero $r \in P$ and just one solution for $r = 0$. Hence the total number of solutions of the system is

$$\begin{aligned} |Z(\mathbb{F}_p)| &\geq |S_0| + \sum_{r \in P \smallsetminus \{0\}} k|S_r| = (1-k)|S_0| + \sum_{r \in P} k|S_r| \\ &\geq (1-k)k + k|S|, \end{aligned}$$

therefore we have

$$k|S| - k(k-1) \leq |Z(\mathbb{F}_p)| \leq d(p+1) + d(e-1)(e-2)\sqrt{p} - k,$$

which gives the desired bound. ∎

Proof of Theorem 1.4. Under the definitions and the hypotheses of Theorem 1.4 we will prove that, if f is not a kth power in $\mathbb{F}_p[x]$ then $|S(\mathbb{F}_p, k, f)| < M$. We write $S = S(\mathbb{F}_p, k, f)$. From the previous proposition we have

$$|S| \leq \frac{1}{e}(p+1) + \frac{(e-1)(e-2)}{e}\sqrt{p} + k - 2$$

where e is a divisor of k depending on f. Note that $e \geq 2$ because f is not a kth power. When $k = 2$ the conclusion follows, so we consider the general case with $p > 4k^2$. We have

$$\begin{aligned}|S| &\le \frac{1}{e}(p+1)+\frac{(e-1)(e-2)}{e}\sqrt{p}+k-2\\ &\le \frac{1}{c}(p+1)+(k-2)\sqrt{p}+k-2\\ &\le \frac{1}{c}p+(k-1)\sqrt{p}+k+\frac{1}{c}-2-2k \quad \text{because } \sqrt{p}>2k\\ &< \frac{1}{c}p+(k-1)\sqrt{p}-(k+1)<M.\end{aligned}$$

Moreover, one can check that $M < p$ for $\sqrt{p} > 2k$, thus the bound is nontrivial. ∎

Proof of Corollary 1.5. Let $(x_n)_{n=1}^M$ be a sequence in $\mathbb{F}_p$ satisfying

$$\Delta^{(k)}(x_n^k)_{n=1}^M = (k!,\dots,k!),$$

with M as in the hypothesis. Solving the recurrence for the x_i^k in terms of the index i and the first initial values $x_1^k,\dots,x_k^k$, we get $x_n^k = f(n)$ where $f \in \mathbb{F}_p[x]$ is a monic polynomial of degree k. Hence Theorem 1.4 implies that there exists $\nu \in \mathbb{F}_p$ such that $x_n^k = (\nu+n)^k$. ∎

3. A refinement. Here we prove Corollary 1.6. Let ϵ be a primitive kth root of 1 in $\mathbb{C}$ and let g be a primitive root in $\mathbb{F}_p$. Define the character χ by setting $\chi(g)=\epsilon$, so that n is a kth power in $\mathbb{F}_p$ if and only if $\chi(n)=1$ or $\chi(n)=0$. Note that χ is a k-order character. Let $f \in \mathbb{F}_p[x]$ be a monic polynomial of degree k which is not a kth power. It is known (see for example [2]) that under these hypotheses, for $0 < V \le p$ we have

$$\Big|\sum_{x=U+1}^{U+V}\chi(f(x))\Big| = \mathcal{O}(p^{1/2}\log p)$$

where the implicit constant depends only on the degree of f, in this case k. Since $\chi(f(x))=0$ can happen at most k times, the result follows.

Acknowledgements. This work is part of the MS Thesis of the author at the Universidad de Concepción, Chile. I thank the professors of the Mathematics Department for their useful comments, especially Antonio Laface and Xavier Vidaux. I would also like to express my gratitude to Thanases Pheidas and Bjorn Poonen for their valuable suggestions. Finally, I would like to thank the referee for useful suggestions and comments.

References

[1] Y. Aubry and M. Perret, *A Weil theorem for singular curves*, in: Proceedings of Arithmetic, Geometry and Coding Theory IV, R. Pellikaan et al. (eds.), de Gruyter, 1995, 1–7.

[2] D. A. Burgess, *On Dirichlet characters of polynomials*, Proc. London Math. Soc. 13 (1963), 537–548.

[3] L. Carlitz, *A problem of Dickson's*, Duke Math. J. 14 (1947), 1139–1140.

[4] —, *A problem of Dickson*, ibid. 19 (1952), 471–474.

[5] —, *Note on a problem of Dickson*, Proc. Amer. Math. Soc. 14 (1963), 98–100.

[6] L. E. Dickson, *Definite forms in a finite field*, Trans. Amer. Math. Soc. 10 (1909), 109–122.

[7] E. M. Hanine, *Polynômes singuliers à plusieurs variables sur un corps fini et congruences modulo p^2*, Acta Arith. 68 (1994), 1–10.

[8] D. Hensley, *Sequences of squares with second difference of two and a problem of logic*, unpublished (1980–1983).

[9] D. J. Lewis, *Singular quartic forms*, Duke Math. J. 21 (1954), 39–44.

[10] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia Math. Appl. 20, Cambridge Univ. Press, Cambridge, 1997.

[11] L. Lipshitz, *Quadratic forms, the five square problem, and diophantine equations*, in: The Collected Works of J. Richard Büchi (S. MacLane and Dirk Siefkes, eds.), Springer, 1990, 677–680.

[12] Y. Matiyasevich, *Enumerable sets are diophantine*, Dokl. Akad. Nauk SSSR 191 (1970), 279–282 (in Russian); English transl.: Soviet Math. Dokl. 11 (1970), 354–358.

[13] H. Pasten, *Representation of squares by monic second degree polynomials in the field of p-adic meromorphic functions*, Trans. Amer. Math. Soc., to appear; arXiv: 1003.1969.

[14] H. Pasten, T. Pheidas and X. Vidaux, *A survey on Büchi's problem: new presentations and open problems*, Zap. Nauchn. Sem. POMI 377 (2010), 111–140, 243.

[15] T. Pheidas and X. Vidaux, *Extensions of Büchi's problem: Questions of decidability for addition and kth powers*, Fund. Math. 185 (2005), 171–194.

[16] —, —, *The analogue of Büchi's problem for rational functions*, J. London Math. Soc. 74 (2006), 545–565.

[17] —, —, *Corrigendum: The analogue of Büchi's problem for rational functions*, ibid. 82 (2010), 273–278.

[18] —, —, *The analogue of Büchi's problem for cubes in rings of polynomials*, Pacific J. Math. 238 (2008), 349–366.

[19] P. Vojta, *Diagonal quadratic forms and Hilbert's Tenth Problem*, in: Contemp. Math. 270, Amer. Math. Soc., 2000, 261–274.

Hector Pasten
Departamento de Matemáticas
Universidad de Concepción
Concepción, Chile

Current address:
Department of Mathematics and Statistics
Queen's University
Kingston, Canada
E-mail: hpasten@gmail.com

Received on 31.3.2010
and in revised form on 7.10.2010 (6348)