WARING'S PROBLEM FOR POLYNOMIALS IN POSITIVE CHARACTERISTIC

JOSÉ FELIPE VOLOCH

ABSTRACT. Rough notes of talk at Silvermania.

Let R be a ring (or a semiring) and $n > 1$ a fixed integer. Waring's problem in this setting is to determine the least integer s for which every element of R is a sum of s n-th powers of elements of R, if such an integer exists. The classical Waring's problem is what we call Waring's problem for $\mathbf{N}$. For n odd, what we call Waring's problem for $\mathbf{Z}$ is usually referred to as the "easier" Waring's problem. In this note, we consider Waring's problem for $R = k[t]$, where k is an algebraically closed field of characteristic p and we denote the least s as above by $v(p, n)$. This problem has been extensively studied ([C, LW] and references therein). For $p = 0$, it's known that $\sqrt{n} < v(0, n) \leq n$ ([NS]). Our focus here is on $p > 0$. If $n = n_0 + n_1 p + \cdots + n_k p^k$ is the base p expansion of n (i.e. $0 \leq n_i < p$), then Vaserstein and also Liu and Wooley [Va, LW] showed that $v(p, n) \leq \prod(n_i + 1)$. We improve this bound for some values of n.

Note that, if s is the smallest integer for which there exists $x_1, \dots, x_s \in k[t]$ with $\sum x_i^n = t$, then $s = v(p, n)$, simply by replacing t by a polynomial in t. It is easy to see that $v(p, 2) = 2, p > 2$, that $v(p, n) > 2$ for all $n > 2$, that $v(p, d) \leq v(p, n)$ if $d|n$ and that $v(p, n)$ does not exist if $p|n$. i The following proposition for $n = p^m + 1$ is due to Car, [C], Prop. 3.2. We give a slightly different proof.

Proposition 1. *If $n|(p^m + 1)$ for some m, then $v(p, n) = 3$.*

Let us write $q = p^m$. An identity $\sum x_i^{q+1} = t$ gives $\sum (x_i^{(q+1)/n})^n = t$, so we need only consider $n = q+1$. Let $x, y \in k$ satisfy $x^{q+1} + y^{q+1} + 1 = 0$, then

$$(xt + x^{q^2})^{q+1} + (yt + y^{q^2})^{q+1} + (t + 1)^{q+1} = ct,$$

where $c = x^{q^3+1} + y^{q^3+1} + 1$ and can be chosen to be nonzero by an appropriate choice of x, y. Replacing t by t/c completes the proof.

We remark that the solutions to $x^{q^3+1} + y^{q^3+1} + 1 = x^{q+1} + y^{q+1} + 1 = 0$ are in $\mathbf{F}_{q^2}$.

We conjecture that $v(p,n) > 3$ in the cases not covered by the above proposition.

Theorem 1. *If $p > 3$ and $n|(2p^m+1)$ for some m, then $v(p,n) \le 4$.*

For the proof, see [V].

The next two results are easy.

Theorem 2. *(Lucas' theorem) For prime p and non-negative integers m and n such that*

$$\begin{aligned} m &= m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0, \\ n &= n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0, \\ 0 &\le m_i, n_i < p \end{aligned}$$

we have

$$\binom{n}{m} \equiv \prod_{i=0}^{k} \binom{n_i}{m_i} \pmod{p}.$$

In particular, $\binom{n}{m} \not\equiv 0 \pmod{p}$ if and only if $m_i \le n_i, i = 0, \ldots, k$.

Theorem 3.

$$\sum_{\zeta \in \mu_n} \zeta (t+\zeta)^n = n^2 t$$

More generally

$$\sum_{\zeta \in \mu_m} \zeta^{1-n} (t+\zeta)^n = nmt + \sum_{j=1}^{[(n-1)/m]} m \binom{n}{mj+1} t^{mj+1}$$

We analyze when the previous identity for $m = 4$ has degree one on the RHS.

Theorem 4. *If p is odd, $n \ge 5$ and $(p,n) = 1$ then $\binom{n}{4j+1} \equiv 0 \pmod{p}, j = 1, \ldots, [(n-1)/4]$ if and only if $p \equiv 3 \pmod 4$ and $n = 1 + p^i + p^k, 1 + p^k, 1 + 2p^k$ and i, k odd. For these values of n, $v(p,n) \le 4$.*

If $p \equiv 1 \pmod 4$ and, for some $i > 0, n_i \ne 0$, then $p^i \equiv 1 \pmod 4$ so $p^i = 4j+1$ contradicts the hypothesis. This shows that $p \equiv 3 \pmod 4$. The same argument shows that $n_i = 0$ for $i > 0$, even. If, for some $i > 0, n_i > 2$, then $3p^i = 4j+1$ contradicts the hypothesis. Also $n_0 = 1$, since $n_0 \ne 0$ by hypothesis and, otherwise, $p^k + 2 = 4j+1$ contradicts the hypothesis. If $n_k = 2$, then $n_i = 0, 0 < i < k$ for otherwise, $2p^k + p^i = 4j+1$ contradicts the hypothesis. So, if $n_k = 2$ then $n = 2p^k + 1$. Assume now that $n_k = 1$. If $n_i = 0, 0 < i < k$, then $n = p^k + 1$. There is at most one $i, 0 < i < k$ with $n_i > 0$ for otherwise,

$p^k + p^i + p^{i'} = 4j + 1$ contradicts the hypothesis. So we can assume there is exactly one such i and $n_i = 1$, for otherwise, $p^k + 2p^i = 4j + 1$ contradicts the hypothesis. So, $n = 1 + p^i + p^k$.

We note that, if $n = 1 + p^i + p^k, i, k$ odd then the representation of t as a sum of 4 n-th powers is realized by polynomials with coefficients in $\mathbf{F}_{p^2}$.

Corollary 1. *Under GRH, for any prime $p \equiv 3 \pmod 4$, the set of primes ℓ with $v(p, \ell) \leq 4$ has density one.*

See [Sk] for an argument, given for $p = 2$ which readily generalizes for all p, that shows, under a conjecture of Erdös, that the set of primes diving some $1 + p^i + p^k$ is of density one. It can be modified so one can only look at i, k odd. Finally, the aforementioned conjecture of Erdös is shown to follow from GRH in [FM].

It is likely that the set of integers dividing some $1 + p^i + p^k$ has positive density. For $p = 2$, numerically, the density is about 0.38.

Here is a list of open questions. I have formulated them in such a way that my guess is that they all have positive answers but I am not confident enough to make any of them a conjecture.

(1) Is $v(0, n) = n/2 + O(1)$?
(2) Is $v(p, n) \leq (\prod(n_i + 1))/2 + O(1)$?
(3) Is $\limsup_n v(p, n) = \infty$?
(4) Is $v(p, p^k - 1) = p^k/2 + O(1)$?

References

[C] M. Car, *Sums of (p^r+1)-th powers in the polynomial ring $\mathbf{F}_{p^m}[T]$*, J. Korean Math. Soc. **49** (2012) 1139–1161.

[FM] A. M. Felix and M. R. Murty, On a conjecture of Erdös. Mathematika 58 (2012), no. 2, 275–289.

[LW] Y.-R. Liu and T. Wooley, *The unrestricted variant of Waring's problem in function fields*, Funct. Approx. Comment. Math., **37** (2007) 285–291.

[NS] D. J. Newman and M. Slater, *Waring's problem for the ring of polynomials*, J. Number Theory **11** (1979) 477–487.

[Sk] M. Skalba, Two conjectures on primes dividing $2^a + 2^b + 1$, Elemente der Mathematik **59**, (2004) 171–173.

[Va] L. Vaserstein, *Ramsey's theorem and the Waring's Problem for algebras over fields*, Proceedings of the workshop on the arithmetic of function fields, Ohio State University, Walter de Gruyter, 1992, pp 435–442.

[V] J. F. Voloch, *Planar surfaces in positive characteristic*, São Paulo J. of Math. Sciences, to appear.

Department of Mathematics, The University of Texas at Austin, Austin, TX 78712 USA

E-mail address: `voloch@math.utexas.edu`