ACTA ARITHMETICA
XC.1 (1999)

On the p-adic Waring's problem

by

José Felipe Voloch (Austin, TX)

Let R be a ring (commutative with unity, in what follows). For an integer $n > 1$ define $g_R(n)$ to be the least integer s for which every element of R is a sum of s nth powers of elements of R, if such an integer exists, or ∞ otherwise. *Waring's problem for* R is the problem of deciding whether $g_R(n)$ is finite and estimating it for all n. Note that what is usually called Waring's problem is not what we call Waring's problem for $\mathbb{Z}$. For n odd, what we call Waring's problem for $\mathbb{Z}$ is usually referred to as the "easier" Waring's problem, with Waring's problem proper referring only to positive integers. Nevertheless, the results we are discussing here have an impact on the usual Waring's problem because they have a bearing on the issue of local solvability. For Waring's problem for finite fields see [GV] and the references therein.

We wish to consider in this note Waring's problem for unramified extensions of the ring of p-adic integers $\mathbb{Z}_p$. For $\mathbb{Z}_p$ the problem has been considered extensively (see [B] and references therein) for its connection with the problem of non-vanishing of the singular series in the classical Waring's problem. We shall improve some of Bovey's results for $\mathbb{Z}_p$ and obtain new results for unramified extensions of $\mathbb{Z}_p$.

Let $W(k)$ be the (unique) complete unramified extension of $\mathbb{Z}_p$ with residue field k algebraic over $\mathbb{F}_p$; $W(k)$ is the ring of *Witt vectors* over k and we will recall some of its properties later. To begin with, note that it follows from Hensel's lemma that if $n = p^t d$, $(p, d) = 1$ and $a \equiv x_1^n + \ldots + x_s^n \pmod{p^{t+\varepsilon}}$, $x_1, \ldots, x_s \in W(k)$, where $\varepsilon = 1, p \neq 2$, $\varepsilon = 2$, $p = 2$ and some x_i is a unit, then there exist $y_1, \ldots, y_s \in W(k)$ with $a = y_1^n + \ldots + y_s^n$. This is easy and well known.

Assume for now on that $p \neq 2$ so $\varepsilon = 1$. Notice that if a, as above, is a unit then, for any representation $a \equiv x_1^n + \ldots + x_s^n \pmod{p^{t+\varepsilon}}$, some x_i will be a unit. So every unit of $W(k)$ is a sum of at most $g_{W_{t+1}(k)}(n)$ nth powers,

1991 *Mathematics Subject Classification*: 11D88, 11P05.

where $W_{t+1}(k) = W(k)/p^{t+1}$ is the ring of truncated Witt vectors. If a is not a unit then $a-1$ is a unit and is a sum of $g_{W_{t+1}(k)}(n)$ nth powers, and it follows that $g_{W(k)}(n) \le g_{W_{t+1}(k)}(n) + 1$. Obviously, $g_{W(k)}(n) \ge g_{W_{t+1}(k)}(n)$ and in [B] it is implicitly assumed that they are equal (for $k = \mathbb{F}_p$), however this is false already for $p = 3$, $n = 2$.

Bovey's nice idea was to relate $g_{W(k)}$ with the following function. Let v denote the p-adic valuation on $W(k)$ and define $g_{W(k)}(n, r)$ to be the smallest integer s for which there exist $x_1, \dots, x_s$ in $W(k)$ with $v(x_1^n + \dots + x_s^n) = r$. Of course $g_{W(k)}(n, 0) = 1$. If $n = p^t d, (p, d) = 1$, $r \le t$ and $v(x_1^n + \dots + x_s^n) = r$ then some x_i is a unit for, otherwise, $v(x_1^n + \dots + x_s^n) \ge n \ge p^t > t$. This observation will be useful in the following.

The following result was proved by Bovey [B] for $\mathbb{Z}_p$. We state and prove it in a more general form. The proof is essentially the same as Bovey's and is done here for the reader's convenience. Note however that Bovey actually claims a stronger result which is false (see above).

Lemma 1. *If $n = p^t d$ and $(p, d) = 1$ then*

$$g_{W_{t+1}(k)}(n) \le g_k(n) \sum_{r=0}^{t} g_{W(k)}(n, r).$$

Proof. By induction on t, the case $t = 0$ being clear. Assume $t > 0$. If $a \in W_{t+1}(k)$, then by induction there exist $x_1, \dots, x_s$ in $W_{t+1}(k)$, $s \le g_k(n) \sum_{r=0}^{t-1} g_{W(k)}(n, r)$ with $x_1^{n/p} + \dots + x_s^{n/p} = a$ and, as $x^{n/p} \equiv (\sigma x)^n \pmod{p^t}$, where σ is the inverse of the Frobenius automorphism of $W(k)$, we get $(\sigma x_1)^n + \dots + (\sigma x_s)^n = a - bp^t$ for some b. Also, there exist $y_1, \dots, y_u$ with $\sum y_i^n = cp^t$, $u \le g_{W(k)}(n, t)$ and c not divisible by p. Finally, there exist $z_1, \dots, z_v$ with $\sum z_i^n \equiv b/c \pmod{p}$ and $v \le g_k(n)$. It follows that

$$\sum (\sigma x_i)^n + \sum y_i^n \sum z_i^n \equiv a - bp^t + cp^t b/c \equiv a \pmod{p^{t+1}}$$

and this means that a is a sum of at most $s + uv$ nth powers in $W_{t+1}(k)$, as desired.

The main results of this paper are sharpened estimates for $g_{W(k)}(n, r)$ with the consequences for Waring's problem following from Lemma 1.

The simplest result is when k is algebraically closed.

Lemma 2. *If $n = p^t d$, $(p, d) = 1$ and k is an algebraically closed field then $g_{W(k)}(n, r) \le 2r + 1$ for $1 \le r \le t$.*

Proof. It follows from [TV] that the residue classes of $x_1, \dots, x_s$ with $v(\sum x_i^{p^t}) \ge r$ form an algebraic variety V_r for $r \le t + 1$, since x^{p^t} is a Teichmüller representative modulo p^{t+1}. Also from [TV], Proposition 1, V_r has dimension $s - 1 - r$ for $r \le (s+1)/2$. The subset of V_r where the residue class of some x_i is zero corresponds to a similar variety with s replaced by

$s-1$. Again by [TV], Proposition 1, we know its dimension to be $s-2-r$ for $r \le s/2$. It follows that there exists a point in $V_r \setminus V_{r+1}$ with $x_1, \dots, x_s$ non-zero, for $r \le (s-1)/2$. The Teichmüller representatives of $x_1, \dots, x_s$ are dth powers since k is algebraically closed, and are p^tth powers modulo p^{t+1}. We thus obtain $y_1, \dots, y_s \in W(k)$ with $v(\sum y_i^n) = r$ if $s \ge 2r+1$. Thus $g_{W(k)}(n, r) \le 2r+1$.

COROLLARY. *Under the assumptions of Lemma* 2, $g_{W(k)}(n) \le (t+1)^2+1$.

Proof. Since $g_k(n) = 1$, this follows from Lemmas 1 and 2.

LEMMA 3. *If* $n = pd$, $(p, d) = 1$ *and* $q \ge 4d^4$, $q \ne p$, *or* $q = p \ge \max\{27d^6, 13\}$, *then* $g_{W(\mathbb{F}_q)}(n, 1) \le 3$.

Proof. Retaining the notation of the previous lemma and of [TV], we have to consider the $\mathbb{F}_q$-rational points of $V_1 \setminus V_2$, that is, the set of $a \in \mathbb{F}_q$ with $f(a) \ne 0$, where $f(x) = ((-x-1)^p + x^p + 1)/p$. Any such a will give rise to a triple of pth powers modulo p^2 whose sum has valuation 1, by taking the Teichmüller representatives of $a, (-1-a), 1$. To ensure that these lifts are pdth powers and prove the lemma, we need to be able to choose $a \in \mathbb{F}_q$ such that both a and $-1-a$ are dth powers. The set of $a \in \mathbb{F}_q$ with both a and $-1-a$ dth powers has at least $q/d^2 - q^{1/2}$ elements by the Riemann hypothesis for function fields (although the relevant case of Fermat equations can be proved directly), whereas $f(x)$ has at most $p-1$ zeros, so we are done unless $q = p$. In this case Mit'kin [M] (see also Heath-Brown [HB]) has shown that $f(x)$ has at most $2p^{2/3} + 2$ zeros in $\mathbb{F}_p$ and again we are done.

COROLLARY. *Under the assumptions of Lemma* 3, $g_{W(\mathbb{F}_q)}(n) \le 9$. *If* n *is odd then* $g_{W(\mathbb{F}_q)}(n) \le 8$.

Proof. The first statement follows from Lemma 1 and $g_{\mathbb{F}_q}(n) = g_{\mathbb{F}_q}(d) \le 2$, for d in the given range. For the second statement, note that $0 = 1^n + (-1)^n$, so it is easy to see that $g_{W(\mathbb{F}_q)}(n) = g_{W_2(\mathbb{F}_q)}(n)$ in this case. So, again, the statement follows from Lemma 1 and $g_{\mathbb{F}_q}(n) = g_{\mathbb{F}_q}(d) \le 2$.

REMARK. For $p = 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37$, we have $g_{\mathbb{Z}_p}(2p) = 9, 12, 7, 6, 7, 5, 5, 5, 5, 5, 5$ respectively. It appears at first glance that $g_{\mathbb{Z}_p}(2p) = 5$ for $p \ge 17$. However, $g_{\mathbb{Z}_{59}}(118) = 7$.

EXAMPLES. Some cases where one knows the value of $g_{\mathbb{Z}_p}$ are:

$$g_{\mathbb{Z}_p}((p-1)p^t) = p^{t+1},\ p \ne 2, \qquad g_{\mathbb{Z}_p}((p-1)p^t/2) = (p^{t+1}-1)/2,\ p \ne 2.$$

Bovey has shown (it appears that the proof can be fixed) that, if $(p-1)/2$ does not divide n, $g_{\mathbb{Z}_p}(n) \ll n^{1/2+\varepsilon}$ for all $\varepsilon > 0$.

It is not hard to show, using the above methods, that $g_{\mathbb{Z}_p}(p) \le 4$ for all p. But $g_{\mathbb{Z}_p}(p) = 3$ for all $p \le 211$, except $p = 3, 7, 11, 17, 59$ when it is 4.

LEMMA 4. $g_{W(k)}(n,r) \leq g_{W(k)}(n,1)^r$.

Proof. If $\sum_{i=1}^s x_i^n$ has valuation 1, then $(\sum_{i=1}^s x_i^n)^r$ has valuation r, which gives what we want upon expansion.

Lemma 4 is well known but is included here for completeness. Since $g_{W(k)}(n,1) = g_{W(k)}(n/p^{t-1},1)$, $n = p^t d$, $(p,d) = 1$, the above lemma can be used together with the previous results to give bounds on $g_{W(k)}(n)$, for arbitrary n. Of course, these bounds are not always the best. For instance, $g_{W(\mathbb{F}_q)}(p^2,2) \leq 3^2 = 9$, $q \neq p$, as follows from Lemmas 3 and 4. However, we have

LEMMA 5. $g_{W(\mathbb{F}_q)}(p^2,2) \leq 5$ *if* $q = p^a, a \geq 7$ *and* p *is sufficiently large.*

Proof. As in Lemma 2, we use the notation and results of [TV]. The variety V_2 is, in this case, a surface of degree p in $V_1 \cong \mathbb{P}^3$, with isolated singularities, and V_3 is a curve of degree p^3. It follows from [K] that $|\#V_2(\mathbb{F}_q) - q^2 - q - 1| \leq 2(4p+10)^3 q^{3/2}$. Also $\#V_3(\mathbb{F}_q) \leq p^3(q+1)$, trivially. So $V_2 \setminus V_3$ has $\mathbb{F}_q$ rational points as soon as p is sufficiently large.

Acknowledgements. I would like to thank J. Tate for pertinent comments, F. Rodríguez Villegas for help with the numerical calculations and the NSA (grant MDA904-97-1-0037) for financial support.

My interest in the subject was started by reading a post by N. Benschop on the Usenet newsgroup sci.math where he claimed, in effect, that $g_{\mathbb{Z}_p}(p) \leq 4$ for all p. After overcoming my initial disbelief of the statement, through numerical experimentation, I looked at Benschop's paper [Be], but the proof there is unfortunately incorrect, although he does rediscover part of Bovey's argument. A search through MathSciNet then unearthed Bovey's paper, which sparked the present work.

References

[Be] N. Benschop, *Powersums representing residues mod* p^k, *from Fermat to Waring*, preprint, available at http://www.IAE.nl/users/benschop/.

[B] J. D. Bovey, *A note on Waring's problem in p-adic fields*, Acta Arith. 29 (1976), 343–351.

[GV] A. Garcia and J. F. Voloch, *Fermat curves over finite fields*, J. Number Theory 30 (1988), 345–356.

[HB] R. Heath-Brown, *An estimate for Heilbronn's exponential sum*, in: *Analytic Number Theory*, Vol. 2 (Allerton Park, Ill., 1995), Progr. Math. 139, Birkhäuser Boston, Boston, Mass., 1996, 451–463.

[K] N. M. Katz, *Number of points on singular complete intersections*, appendix to: C. Hooley, *On the number of points on a complete intersection over a finite field*, J. Number Theory 38 (1991), 338–358.

[M] D. A. Mit'kin, *An estimate for the number of roots of some comparisons by the Stepanov method*, Mat. Zametki 51 (1992), 52–58, 157 (in Russian); English transl.: Math. Notes 51 (1992), 565–570.

[TV] J. Tate and J. F. Voloch, *Linear forms in p-adic roots of unity*, Internat. Math. Res. Notices 12 (1996), 589–601.

Department of Mathematics
University of Texas
Austin, Texas 78712
U.S.A.
E-mail: voloch@math.utexas.edu

Received on 13.10.1998 (3479)