BULL. AUSTRAL. MATH. SOC. 11S05, 11J61
VOL. 60 (1999) [479–482]

PLANE CURVES AND p-ADIC ROOTS OF UNITY

JOSÉ FELIPE VOLOCH

We prove the following result: Let $f(x,y)$ be a polynomial of degree d in two variables whose coefficents are integers in an unramified extension of $\mathbf{Q}_p$. Assume that the reduction of f modulo p is irreducible of degree d and not a binomial. Assume also that $p > d^2 + 2$. Then the number of solutions of the inequality $|f(\zeta_1,\zeta_2)| < p^{-1}$, with ζ_1, ζ_2 roots of unity in $\overline{\mathbf{Q}}_p$ or zero, is at most pd^2.

Let $\mathbf{C}_p$ be the completion of the algebraic closure of $\mathbf{Q}_p$ with its usual norm extending that of $\mathbf{Q}_p$. In [**5**], a result which implies the following statement was proved. If $f(x,y) \in \mathbf{C}_p[x,y]$ there exists a positive constant c such that, for any roots of unity ζ_1, ζ_2, either $f(\zeta_1,\zeta_2) = 0$ or $\left|f(\zeta_1,\zeta_2)\right| \geqslant c$. (A similar result holds for polynomials with an arbitrary number of variables.) In general, however, there is little information about the value of c. In the case that f is linear and its coefficients are units in an unramified extension of $\mathbf{Q}_p$, it was proved in [**5**] that the inequality $\left|f(\zeta_1,\zeta_2)\right| \leqslant p^{-2}$ had at most p solutions ζ_1, ζ_2 roots of unity or zero. The purpose of this note is to obtain a similar result for more general polynomials in two variables. Recall that a binomial is a polynomial with (at most) two non-zero coefficients. Our main result is then:

THEOREM. *Let $f(x,y)$ be a polynomial of degree d in two variables whose coefficents are integers in an unramified extension of $\mathbf{Q}_p$. Assume that the reduction of f modulo p is irreducible of degree d and not a binomial. Assume also that $p > d^2 + 2$. Then the number of solutions of the inequality $\left|f(\zeta_1,\zeta_2)\right| < p^{-1}$, with ζ_1, ζ_2 roots of unity in $\overline{\mathbf{Q}}_p$ or zero, is at most pd^2.*

PROOF: We shall first prove the theorem under the additional condition that we are dealing with roots of unity of order prime to p. The inequality then translates into $f(\zeta_1,\zeta_2) \equiv 0 \pmod{p^2}$. The ring of integers of the completion of the maximal unramified extension of $\mathbf{Q}_p$ can be viewed as the ring of Witt vectors over the algebraic closure of $\mathbf{F}_p$ and, since we are interested only in the situation modulo p^2, we can work in the Witt vectors of length two over the algebraic closure of $\mathbf{F}_p$. We are thus interested

Received 3rd March, 1999
The author would like to thank the TARP (grant #ARP-0006) and the NSA (grant MDA904-97-1-0038) for financial support.

in the solutions of the equation $f\big((x,0),(y,0)\big) = (0,0)$. This equation translates into the system $f_0(x,y) = g(x,y) = 0$, where f_0 is the reduction of f modulo p and the polynomial g is the reduction modulo p of the polynomial $\big(f^\sigma(x^p,y^p) - f(x,y)^p\big)/p$ and σ is the Frobenius automorphism of the ring of Witt vectors. Clearly g has degree at most pd and, since f_0 is assumed irreducible of degree d, the result we want follows from Bézout's theorem unless f_0 divides g, which we proceed to show cannot happen.

Let X be the irreducible plane curve defined by $f_0(x,y) = 0$. We shall derive a contradiction from the assumption that g vanishes identically on X. If $g = 0$ on X then, by differentiating $g(x,y) = 0$ we obtain $g_x + g_y dy/dx = 0$ and, from the definition of g we have $g_x = f_x^\sigma(x^p,y^p)x^{p-1} - f(x,y)^{p-1}f_x = f_{0x}^p x^{p-1}$ on X. Likewise $g_y = f_{0y}^p y^{p-1}$ on X. Since f_0 is of degree less than p and is not a binomial, we have that f_{0x}, f_{0y} are non-zero. Using that $dy/dx = -f_{0x}/f_{0y}$, we obtain the identity $f_{0x}^{p-1}x^{p-1} = f_{0y}^{p-1}y^{p-1}$, on X. This gives $xf_{0x} = cyf_{0y}$ for some $c \in \mathbf{F}_p$. The lemma below ensures that this cannot hold under the assumptions that $p > d^2$ and f_0 is not a binomial and this will complete the proof in the case the roots of unity are of order prime to p.

If ζ_1, ζ_2 are arbitrary roots of unity satisfying the inequality $\big|f(\zeta_1,\zeta_2)\big| < p^{-1}$ we can write $\zeta_i = \lambda_i\eta_i$, $i = 1,2$ where the λ_i are of order prime to p and the η_i are of p-power order and are not both equal to one. We shall show that this inequality has no such solution. By a harmless change of coordinates we may assume that $\lambda_i = 1$, $i = 1,2$. Further, perhaps after switching x and y if necessary, we may assume that $\eta_2 = \eta_1^r$ for some integer r. We write $\eta_1 = 1 + \pi$ and notice that the inequality $\big|f(\zeta_1,\zeta_2)\big| < p^{-1}$ implies $f\big(1+\pi,(1+\pi)^r\big) \equiv 0\big(\mathrm{mod}\,\pi^{p-1}\big)$. On the other hand if $\mathcal{O}$ is the ring of integers of the field $F(\eta_1)$, where F is a unramified extension of $\mathbf{Q}_p$ containing the coefficients of f, then $\mathcal{O}/\pi^{p-1}$ is isomorphic to $k[t]/t^{p-1}$, where k is the residue field of F. Therefore we obtain $f_0\big(1+t,(1+t)^r\big) \equiv 0\big(\mathrm{mod}\,t^{p-1}\big)$. This implies, with notation as above, that $y/x^r - 1$ has a zero of order at least $p-1$ at some place of X centred at $(1,1)$, so the differential $dy/y - r\,dx/x$ has a zero of order at least $p-2$ at that same place. However, this differential has at most $3d$ poles counted with multiplicity, so at most $3d + 2g - 2$ zeros, where g is the genus of X unless it is identically zero. Now, $3d + 2g - 2 \leqslant 3d + d(d-3) = d^2 < p-2$, by hypothesis, so the differential is identically zero, which, using that $dy/dx = -f_{0x}/f_{0y}$, leads to a contradiction with the lemma below. ∎

It remains only to prove:

Lemma. *Let $f(x,y) = 0$ define an irreducible plane curve X of degree d over an algebraically closed field k of characteristic p satisfying $p > d^2$. If $xf_x = cyf_y$ on X for some c in k then f is a binomial.*

Proof: The hypothesis means an identity $xf_x - cyf_y = bf$ for some b in k. If

$f(x,y) = \sum a_{ij}x^iy^j$ we get $a_{ij}(i - cj - b) = 0$ for all i, j. Suppose first that $b = 0$. For any i, j, i', j' with both $a_{ij}, a_{i'j'}$ non-zero, we get $i - cj = i' - cj' = 0$ which implies that $ij' - i'j = (i - cj)j' - (i' - cj')j = 0$ in k, which means that p divides $ij' - i'j$, but under our assuption that $p > d^2$, this implies that $ij' = i'j$ and this implies that the value of i/j is constant for all i, j with $a_{ij} \neq 0$. So $f(x,y) = \sum_r a_{rm,rn}x^{rm}y^{rn}$ which can be written as a constant multiple of a product of terms of the form $x^my^n - \alpha$ and, since f is irreducible, we conclude that f is a binomial.

Assume now that b is not zero. First of all, if f is a polynomial in just one variable and is irreducible, then it is a binomial and we are done. Therefore, we may assume that there exists i_1, j_1 with a_{0j_1}, a_{i_10} both non-zero and we get that $i_1 = b$ and $cj_1 = -b$, so c is not zero and $c = -i_1/j_1$. If i, j are such that $a_{ij} \neq 0$ then $i + ji_1/j_1 - i_1 = 0$ in k so $ij_1 + ji_1 \equiv i_1j_1 (\operatorname{mod} p)$. But $i_1, j_1 \leqslant d$, $i + j \leqslant d$, therefore $0 \leqslant ij_1 + ji_1$, $i_1j_1 \leqslant d^2 < p$ so $ij_1 + ji_1 = i_1j_1$. Let $\delta = (i_1, j_1)$, $i_1 = m\delta$, $j_1 = n\delta$, $(m,n) = 1$. We get $in + jm = mn\delta$, so $m|i$, $n|j$ and writing $i = mu$, $j = mv$ we get $u + v = \delta$. Thus $f(x,y) = \sum_u a_{mu,n(\delta-u)}x^{mu}y^{n(\delta-u)}$ which can be written as a constant multiple of a product of terms of the form $x^m - \alpha y^n$ and, since f is irreducible, we conclude that f is a binomial. ∎

REMARKS. (i) If X is a projective curve of genus bigger than one embedded in an Abelian variety A, all defined over an unramified extension of $\mathbf{Q}_p$, then Raynaud [**4**] proved that there are only finitely many torsion points of A of order prime to p which are in X modulo p^2 and Buium [**1**] gave an explicit bound for the number of those points. Perhaps the techniques of Coleman [**2**] could be used to extend this result to the full torsion and obtain an Abelian analogue of the above result.

(ii) A special case of Lang's extension of the Manin-Mumford conjecture, proved by Ihara, Serre and Tate (see [**3**, Chapter 8, Theorem 6.1]) states that if $f(x,y)$ is an irreducible polynomial, not a binomial, over a field of characteristic zero, then there are only finitely many roots of unity ζ_1, ζ_2 with $f(\zeta_1, \zeta_2) = 0$. This follows from the above theorem by choosing p large enough such that the field generated by the coefficents of f embeds in $\mathbf{Q}_p$ and such that the hypotheses of the theorem hold.

REFERENCES

[1] A. Buium, 'Geometry of p-jets', *Duke Math. J.* **82** (1996), 349–367.

[2] R.F. Coleman, 'Ramified torsion points on curves', *Duke Math. J.* **54** (1987), 615–640.

[3] S. Lang, *Fundamentals of diophantine geometry* (Springer-Verlag, Berlin, Heidelberg, New York, 1983).

[4] M. Raynaud, 'Courbes sur une variété abélienne et points de torsion', *Invent. Math.* **71** (1983), 207–233.

[5] 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 TX 78712
United States of America
e-mail: voloch@math.utexas.edu