Plane curves and $p$-adic roots of unity

José Felipe Voloch

Let $\mathbb{C}_p$ be the completion of the algebraic closure of $\mathbb{Q}_p$ with its usual norm extending that of $\mathbb{Q}_p$. In [TV], J. Tate and the author proved a result which implies the following statement. If $f(x, y) \in \mathbb{C}_p[x, y]$ there exists a positive constant $c$ such that, for any roots of unity $\zeta_1, \zeta_2$, either $f(\zeta_1, \zeta_2) = 0$ or $|f(\zeta_1, \zeta_2)| \geq c$ (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 $\mathbb{Q}_p$, it was proved in [TV] that the inequality $|f(\zeta_1, \zeta_2)| \leq p^{-2}$ had at most $p$ solutions $\zeta_1, \zeta_2$ 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 coefficients are integers in an unramified extension of $\mathbb{Q}_p$. 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 $\zeta_1, \zeta_2$ roots of unity in $\overline{\mathbb{Q}}_p$ or zero, is at most $pd^2$.

**Proof:** We will 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 $\mathbb{Q}_p$ can be viewed as the ring of Witt vectors over the algebraic closure of $\mathbb{F}_p$ 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 $\mathbb{F}_p$. We are thus interested in the solutions of the equation $f((x, 0), (y, 0)) = (0, 0)$. 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 $(f^\sigma(x^p, y^p) - f(x, y)^p)/p$ and $\sigma$ 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 will derive a contradiction from the assumption that $g$ vanishes identically on $X$. If $g = 0$ on $X$ then, differentiating $g(x,y) = 0$ we obtain $g_x + g_y dy/dx = 0$ and, from the definition of $g$ we have $g_x = f_x^p(x^p,y^p)x^{p-1} - f(x,y)^{p-1}f_x = f_{0x}^p x^{p-1}$ 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 $f_0 x, f_0 y$ are non-zero. So we obtain, using that $dy/dx = -f_0 x/f_0 y$, the identity $f_p^{p-1} x^{p-1} - f_{0y}^{p-1} y^{p-1},$ on $X$. This gives $xf_0 x = cyf_0 y$ for some $c \in F_p$. 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 $\zeta_1, \zeta_2$ are arbitrary roots of unity satisfying the inequality $|f(\zeta_1, \zeta_2)| < p^{-1}$ we can write $\zeta_i = \lambda_i \eta_i, i = 1, 2$ where the $\lambda_i$ are of order prime to $p$ and the $\eta_i$ are of $p$-power order and are not both equal to one. We will 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 $|f(\zeta_1, \zeta_2)| < p^{-1}$ implies $f(1 + \pi, (1 + \pi)^r) \equiv 0(\text{mod } \pi^{p-1})$. On the other hand if $O$ is the ring of integer of the field $F(\eta_1)$, where $F$ is a unramified extension of $Q_p$ containing the coefficients of $f$, then $O/\pi^{p-1}$ is isomorphic to $k[t]/t^{p-1}$, where $k$ is the residue field of $F$. Therefore we obtain $f_0(1 + t, (1 + t)^r) \equiv 0(\text{mod } t^{p-1})$. This implies, with notation as above, that $y/x^r - 1$ has a zero of order at least $p - 1$ at some place of $X$ centered at $(1,1)$, so the differential $dy/y - rdx/x$ 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, $3d + 2g - 2 \leq 3d + d(d - 3) = d^2 < p - 2$, by hypothesis, so the differential is identically zero, which using that $dy/dx = -f_0 x/f_0 y$ 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 \( i'j' - ij = (i - cj)j' - (i' - cj')j = 0 \) in \( k \), which means that \( p \) divides \( i'j' - ij \), but under our assumption that \( p > d^2 \), this implies that \( i'j' = ij \) and this implies that the value of \( i/j \) is constant for all \( i, j \) with \( a_{ij} \neq 0 \). So \( f(x, y) = \sum r a_{rm, r'n}x^m y^n \) which can be written as a constant multiple of a product of terms of the form \( x^m y^n - \alpha \) 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 \( ij_1 + ji_1 \equiv i_1j_1 \pmod{p} \). But \( i_1, j_1 \leq d, i + j \leq d \), therefore \( 0 \leq ij_1 + ji_1, i_1j_1 \leq d^2 < p \) 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 \( f(x, y) = \sum_u a_{mu, vn(\delta - u)}x^{mu} y^{n(\delta - u)} \) 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 \( \mathbb{Q}_p \), then Raynaud [R] 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 [B] gave an explicit bound for the number of those points. Perhaps the techniques of Coleman [C] 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 [L], ch. 8, thm. 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 \( \zeta_1, \zeta_2 \) 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 coefficients of \( f \) embed in \( \mathbb{Q}_p \) and such that the hypotheses of the theorem hold.

**Acknowledgements:** The author would like to thank the TARP (grant #ARP-006) and the NSA (grant MDA904-97-1-0037) for financial support.

**References.**


Dept. of Mathematics, Univ. of Texas, Austin, TX 78712, USA

e-mail: voloch@math.utexas.edu