On the number of points on a plane algebraic curve over $GF(q)[t]/t^n$

Dirk Keppens Wim Mielants

ABSTRACT. A general formula is obtained for the number of points lying on a plane algebraic curve over the finite local ring $GF(q)[t]/t^n (n > 1)$ whose equation has coefficients in $GF(q)$ and under the restriction that it has only simple and ordinary singular points.

1. Preliminaries

Let C be an algebraic curve in $PG(2, GF(q)((t))$, $GF(q)((t))$ being the field of Laurent series over $GF(q)$, with minimal equation $F(X_0, X_1, X_2) = 0$ whose coefficients are supposed to belong to $GF(q)$.

The finite local ring $GF(q)[t]/t^n$ is denoted as R_n and the "projective plane" over it (in fact a projective Hjelmslev plane) as $PG(2, R_n)$.

Then $C \bmod t^n = \{R_n^*(x_0, x_1, x_2) | R_n^*(x_0, x_1, x_2) \in PG(2, R_n)$ and $F(x_0, x_1, x_2) = 0 \pmod{t^n}\}$ is an algebraic curve in $PG(2, R_n)$. In particular $C \bmod t$ is an algebraic curve in $PG(2, q)$.

The canonical epimorphism from $PG(2, R_i)$ onto $PG(2, R_j) (i \geq j)$ is denoted as Π_j^i. It is clear that $\Pi_n^\infty(C)$ $(R_\infty = GF(q)((t)))$ is a subset of $C \bmod t^n$.

If p is a point of $C \bmod t^n$ then $\Delta_i^n(p) = (\Pi_i^n)^{-1}(\Pi_i^n(p))$ $(1 \leq i \leq n-1)$ is called the *ith neighbourhood of p*.

In this paper we shall calculate the number of points in the intersections $C \bmod t^n \cap \Delta_i^n(p)$ for $\Pi_i^n(p)$ a simple ordinary point of $C \bmod t$. As a consequence we obtain a general formula for the number of points on $C \bmod t^n$. It will turn out that $|C \bmod t^n|$ depends on $|C \bmod t|$ (the number of points on the canonical projection $\Pi_i^n(C \bmod t^n)$) and on the intersection numbers $|C \bmod t^n \cap \Delta_1^n(p)|$.

ARS COMBINATORIA 40(1995), pp. 121-128

2. The intersection numbers $|C \bmod t^n \cap \Delta_i^n(p)|$

Suppose C had degree m and write $F(X_0, X_1, X_2) = F_0(X_1, X_2)X_0^m + F_1(X_1, X_2)X_0^{m-1} + \ldots + F_m(X_1, X_2)$ where F_i is a homogenous form of degree i in X_1 and X_2. Without loss of generality we may assume that $p = R_\infty^*(1, 0, 0)$ is a point of C. Then $F_0 = 0$.

An arbitrary point of $\Delta_i^n(p)$ has coordinates of the form $R_n^*(1, t^iU, t^iV)$ with $U, V \in GF(q)[t]/t^{n-i}$.

Hence, the coordinates of the points of $C \bmod t^n \cap \Delta_i^n(p)$ satisfy

$$\begin{aligned} & F_1(t^iU, t^iV) + F_2(t^iU, t^iV) + \ldots + F_m(t^iU, t^iV) = 0 \bmod t^n \\ \iff \; & t^iF_1(U, V) + t^{2i}F_2(U, V) + \ldots + t^{mi}F_m(U, V) = 0 \bmod t^n \\ \iff \; & F_1(U, V) + t^iF_2(U, V) + \ldots + t^{(m-1)}F_m(U, V) = 0 \bmod t^{n-i} \end{aligned} \tag{1}$$

2.1. Case I: p a simple point

We write $U = u_0 + u_1t + \ldots + u_{n-i-1}t^{n-i-1}$ and $V = v_0 + v_1t + \ldots + v_{n-i-1}t^{n-i-1}$ with $u_j, v_j \in GF(q)$, $0 \leq j \leq n-i-1$

Then we obtain from (1) the system (2):

$$\left\{ \begin{array}{l} F_1(u_0, v_0) = 0 \\ F_1(u_1, v_1) = 0 \quad \text{(coefficient of } t) \\ \vdots \\ F_1(u_{i-1}, v_{i-1} = 0 \quad \text{(coefficient of } t^{i-1}) \\ F_1(u_i, v_i) + F_2(u_0, v_0) = 0 \quad \text{(coefficient of } t^i) \\ \vdots \\ F_1(u_{2i-1}, v_{2i-1}) + f(u_0, \ldots, u_{i-1}, v_0, \ldots, v_{i-1}) = 0 \\ \quad \text{(coefficient of } t^{2i-1}) \\ \vdots \\ F_1(u_{n-i-1}, v_{n-i-1}) + f'(u_0, \ldots, u_{n-2i-1}, v_0, \ldots, v_{n-2i-1}) = 0 \\ \quad \text{(coefficient of } t^{n-i-1}) \end{array} \right.$$

It is clear that this system has q^{n-i} solutions $(u_0, \ldots, u_{n-i-1}, v_0, \ldots, v_{n-i-1})$. So: $|C \bmod t^n \cap \Delta_i^n(p)| = q^{n-i}$ if p is a simple point.

2.2. Case II: p an ordinary singular point

Let $p = R_\infty^*(1, 0, 0)$ be an r-fold singular piont $(2 \leq r \leq m-1)$ of C. Then $F_1 = F_2 = \ldots = F_{r-1} = 0 \neq F_r$.

The equation (1) becomes:

$$t^{(r-1)i}F_r(U,V)+\ldots+t^{(m-1)i}F_m(U,V)=0 \bmod t^{n-i}$$
$$(U,V\in GF(q)[t]/t^{n-i}). \tag{3}$$

1. $\boxed{i\geq n/r}$

Then (3) becomes: $0=0 \bmod t^{n-i}$.
Hence, $|C \bmod t^n \cap \Delta_i^n(p)|=q^{2(n-i)}$ in this case.

2. $\boxed{i<n/r}$

Then (3) becomes: $F_r(U,V)+t^iF_{r+1}+\ldots+t^{(m-r)i}F_m(U,V)=0 \bmod t^{n-ri}$ $(U,V\in GF(q)[t]/t^{n-i})$.

Put $U=\tilde{U}+U'$ and $V=\tilde{V}+V'$ with $\tilde{U},\tilde{V}\in GF(q)[t]/t^{n-ri}$ and $U'=u_{n-ri}t^{n-ri}+\ldots+u_{n-i-1}t^{n-i-1}$ and $V'=v_{n-ri}t^{n-ri}+\ldots+v_{n-i-1}t^{n-i-1}$.

Then $|C \bmod t^n\cap\Delta_i^n(p)|=q^{2(r-1)i}$ times the number of solutions of

$$F_r(\tilde{U},\tilde{V})+t^iF_{r+1}(\tilde{U},\tilde{V})+\ldots+t^{(m-r)i}F_m(\tilde{U},\tilde{V})=0 \bmod t^{n-ri} \tag{4}$$

One can see that the original problem is reduced to the problem of finding the numbers of points $(\tilde{U},\tilde{V})\in GF(q)[t]/t^{n-ri}\times GF(q)[t]/t^{n-ri}$ on the curve over $GF(q)[t]/t^{n-ri}$ with equation (4).

CASE (i) $\dfrac{n}{r+1}\leq i<\dfrac{n}{r}$

(4) becomes:

$$F_r(\tilde{U},\tilde{V})=0 \bmod t^{n-ri} \tag{5}$$

or equivalently (6):

$$\begin{cases} F_r(u_0,v_0)=0\\ u_1\dfrac{\partial F_r}{\partial u_0}+v_1\dfrac{\partial F_r}{\partial v_0}=0\\ u_2\dfrac{\partial F_r}{\partial u_0}+v_2\dfrac{\partial F_r}{\partial v_0}+f_2(u_0,u_1,v_0,v_1)=0\\ \vdots\\ u_{n-ri-1}\dfrac{\partial F_r}{\partial u_0}+v_{n-ri-1}\dfrac{\partial F_r}{\partial v_0}\\ \qquad +f_{n-ri-1}(u_0,\ldots,u_{n-ri-2},v_0,\ldots,v_{n-ri-2})=0\end{cases}$$

From now on we assume that the r-fold singular point p is an *ordinary* singular point (i.e. all tangents in p are distinct) with *real index* r'' (i.e. there are r'' distinct "real" tangents (with coefficients of their equation in $GF(q)$) (cfr. [1])).

- If $(u_0, v_0) \neq (0,0)$ is a solution of $F_r(u_0, v_0) = 0$ then $(\frac{\partial F_r}{\partial u_0}, \frac{\partial F_r}{\partial v_0}) \neq (0,0)$ since p is ordinary and singular. Hence, in (6) we have for each solution $(u_0, v_0) \neq (0,0)$ of $F_r(u_0, v_0) = 0$, q solutions (u_1, v_1), q solutions $(u_2, v_2), \dots$, q solutions (u_{n-ri-1}, v_{n-ri-1}) so that the number of solutions $(\tilde{U}, \tilde{V})$ of (5) with $(u_0, v_0) \neq (0,0)$ equals $q^{n-ri-1}.r''(q-1)$.
- Consider the solution $(u_0, v_0) = (0,0)$ of $F_r(u_0, v_0) = 0$. The first r equations in (6) become: $0 = 0$.
  a) If $n - ri \leq r$, then *all* equations in (6) become trivial $(0 = 0)$ and consequently the number of solutions $(\tilde{U}, \tilde{V})$ of (5) with $(u_0, v_0) = (0,0)$ equals $q^{2(n-ri-1)}$.

  b) If $n - ri > r$ then the system (6) reduces to (7):
$$\begin{cases} F_r(u_1, v_1) = 0 \\ u_2 \dfrac{\partial F_r}{\partial u_1} + v_2 \dfrac{\partial F_r}{\partial v_1} = 0 \\ u_3 \dfrac{\partial F_r}{\partial u_2} + v_3 \dfrac{\partial F_r}{\partial v_2} + f_3'(u_0, u_1, u_2, v_0, v_1, v_2) = 0 \\ \vdots \\ u_{n-ri-r} \dfrac{\partial F_r}{\partial u_1} + v_{n-ri-r} \dfrac{\partial F_r}{\partial v_1} \\ \qquad + f_{n-ri-r}'(u_0, \dots, u_{n-ri-3}, v_0, \dots, v_{n-ri-3}) = 0 \end{cases}$$

  - If $(u_1, v_1) \neq (0,0)$ is a solution of $F_r(u_1, v_1) = 0$ then we obtain $q^{n-ri-r-1}.q^{2(r-1)}.r''(q-1)$ solutions $(\tilde{U}, \tilde{V})$ of (5) with $(u_0, v_0) = (0,0) \neq (u_1, v_1)$
  - For the solution $(u_1, v_1) = (0,0)$ of $F_r(u_1, v_1) = 0$ the first r equations in (7) are $0 = 0$.
    (a) If $n - ri \leq 2r$ then *all* equations become trivial and the number of solutions $(\tilde{U}, \tilde{V})$ of (5) with $(u_0, v_0) = (u_1, v_1) = (0,0)$ is $q^{2(n-ri-2)}$.

    (b) If $n - ri > 2r$ the system reduces to (8):
$$\begin{cases} F_r(u_2, v_2) = 0 \\ u_3 \dfrac{\partial F_r}{\partial u_2} + v_3 \dfrac{\partial F_r}{\partial v_2} = 0 \\ \vdots \\ u_{n-ri-(2r-1)} \dfrac{\partial F_r}{\partial u_2} + v_{n-ri-(2r-1)} \dfrac{\partial F_r}{\partial v_2} \\ \qquad + f_{n-ri-(2r-1)}''(u_0, \dots, u_{n-ri-4}, v_0, \dots, v_{n-ri-4}) = 0 \end{cases}$$
    As above we obtain that (5) has $q^{n-ri-2r-1}.q^{2(2r-2)}.r''(q-1)$ solutions $(\tilde{U}, \tilde{V})$ with $(u_0, v_0) = (u_1, v_1) = (0,0) \neq (u_2, v_2)$

and $q^{2(n-ri-3)}$ solutions $(\tilde{U}, \tilde{V})$ with $(u_0, v_0) = (u_1, v_1) = (u_2, v_2) = (0,0)$ in the case where $n - ri \leq 3r$ and another system (with first equation $F_r(u_3, v_3) = 0$) for the solution $(u_2, v_2) = (0,0)$ in the case where $n - ri > 3r$.

This procedure stops after a finite number of steps. Indeed, there is a non-negative integer k such that $n - ri > kr$ and $n - ri \leq (k+1)r$.

If $r|n$ then $k = \dfrac{n-ri}{r} - 1$ and if $r \not| n$ then $k = \left[\dfrac{n-ri}{r}\right]$.

So after a finite number of steps we obtain the system (9):

$$\begin{cases} F_r(u_k, v_k) = 0 \\ u_{k+1}\dfrac{\partial F_r}{\partial u_k} + v_{k+1}\dfrac{\partial F_r}{\partial v_k} = 0 \\ \vdots \\ u_{n-ri-(kr-k+1)}\dfrac{\partial F_r}{\partial u_k} + v_{n-ri-(kr-k+1)}\dfrac{\partial F_r}{\partial v_k} + g(\ldots) = 0 \end{cases}$$

- If $(u_k, v_k) \neq (0,0)$ is a solution of $F_r(u_k, v_k) = 0$ then the number of solutions $(\tilde{U}, \tilde{V})$ with $(u_0, v_0) = (u_1, v_1) = \ldots = (u_{k-1}, v_{k-1}) = (0,0) \neq (u_k, v_k)$ equals $q^{n-ri-kr-1}.q^{2(kr-k)}.r''(q-1)$.
- For $(u_k, v_k) = (0,0)$ all equations in (9) become $0 = 0$ (since $n - ri - kr \leq r$). Hence, there are $q^{2(n-ri-k-1)}$ solutions $(\tilde{U}, \tilde{V})$ of (5) with $(u_0, v_0) = \ldots = (u_k, v_k) = (0,0)$.

  We conclude that $F_r(\tilde{U}, \tilde{V}) = 0 \bmod t^{n-ri}$ with $\tilde{U}, \tilde{V} \in GF(q)[t]/t^{n-ri}$ has $r''(q-1)q^{n-ri-1} + r''(q-1)q^{n-ri}\,(\sum_{j=1}^{k} q^{jr-2j-1}) + q^{2(n-ri-k-1)}$ solutions (the second term does not occur if $k = 0$).

  Since we had the number of solutions (U, V) of (3) is $q^{2(r-1)i}$ times the number of solutions $(\tilde{U}, \tilde{V})$ of (5) we finally get: $|C \bmod t^n \cap \Delta_i^n(p)| = r''(q-1)q^{n+(r-2)i-1}.(1+q(\sum_{j=1}^{k} q^{(r-2)j-1})) + q^{(n-i-k-1)}$ if p is an ordinary r-fold singular point with real index r'' and if $\dfrac{n}{r+1} \leq i \leq \dfrac{n}{r}$

CASE (ii) $\dfrac{n}{r+h+1} \leq i < \dfrac{n}{r+h}$ $(h \in \{1, \ldots, n-r-1\})$

The case $h = 0$ has already been treated in Case (i).

(4) becomes: $F_r(\tilde{U}, \tilde{V}) + t^i F_{r+1}(\tilde{U}, \tilde{V}) + \ldots + t^{(s-r)i} F_s(\tilde{U}, \tilde{V}) = 0 \bmod t^{n-ri}$ with $s = r + h$ if $h \leq m - r$ and $s = m$ if $h > m - r$, or equivalently:

$$
\begin{cases}
F_r(u_0, v_0) = 0 \\
u_1 \dfrac{\partial F_r}{\partial u_0} + v_1 \dfrac{\partial F_r}{\partial v_0} = 0 \\
\vdots \\
u_{i-1} \dfrac{\partial F_r}{\partial u_0} + v_{i-1} \dfrac{\partial F_r}{\partial v_0} + f_{i-1}(u_0, \dots, u_{i-2}, v_0, v_{i-2}) = 0 \\
u_i \dfrac{\partial F_r}{\partial u_0} + v_i \dfrac{\partial F_r}{\partial v_0} + f_i(u_0, \dots, u_{i-1}, v_0, \dots, v_{i-1}) \\
\quad + F_{r+1}(u_0, v_0) = 0 \\
u_{i+1} \dfrac{\partial F_r}{\partial u_0} + v_{i+1} \dfrac{\partial F_r}{\partial v_0} + f_{i+1}(u_0, \dots, u_i, v_0, \dots, v_i) + u_1 \dfrac{\partial F_{r+1}}{\partial u_0} \\
\quad + v_1 \dfrac{\partial F_{r+1}}{\partial v_0} = 0 \\
\vdots \\
u_{2i-1} \dfrac{\partial F_r}{\partial u_0} + v_{2i-1} \dfrac{\partial F_r}{\partial v_0} + f_{2i-1}(\dots) + u_{i-1} \dfrac{\partial F_{r+1}}{\partial u_0} \\
\quad + v_{i-1} \dfrac{\partial F_{r+1}}{\partial v_0} + f'_{i-1}(\dots) = 0 \\
\vdots \\
u_{(s-r)i} \dfrac{\partial F_r}{\partial u_0} + v_{(s-r)i} \dfrac{\partial F_r}{\partial v_0} + f_{hi}(\dots) + u_{(s-r-1)i} \dfrac{\partial F_{r+1}}{\partial u_0} \\
\quad + v_{(s-r-1)i} \dfrac{\partial F_{r+1}}{\partial v_0} + f'_{(s-r-1)i}(\dots) + \dots + F_s(u_0, v_0) = 0 \\
\vdots \\
u_{n-ri-1} \dfrac{\partial F_r}{\partial u_0} + v_{n-ri-1} \dfrac{\partial F_r}{\partial v_0} + \dots + u_{n-si-1} \dfrac{\partial F_s}{\partial u_0} + v_{n-si-1} \dfrac{\partial F_s}{\partial v_0} \\
\quad + g(\dots) = 0
\end{cases}
$$

It is clear that this system has the same number of solutions as the corresponding system for the case $h = 0$.

Hence, the formula obtained in case (i) is valid for $1 \leq i < \frac{n}{r}$.

3. The number of points on C mod t^n

By using the previous section we obtain a formula for the number of points on C mod t^n. Let n_1 be the number of simple points and n_r the number of r-fold singular points on C mod t.

We then have that $|C \bmod t^n| = n_1 q^{n-1} + \sum_r n_r \delta_1$ where $\delta_1(r, q, n) = |C \bmod t^n \cap \Delta_1^n|$.

In particular, if C has only simple points, then $|C \bmod t^n| = q^{n-1} |C \bmod t|$.

If moreover C mod t is absolutely irreduceble over $GF(q)$ then we have by the Hasse-Weil bound: $q^{n-1}.(q + 1 - 2g\sqrt{q}) \leq |C \bmod t^n| \leq q^{n-1}(q +$

$1 + 2g\sqrt{q})$ where g is the genus of C mod t.

EXAMPLE: Cubic curves over $GF(q)[t]/t^n$

Assume that C mod t^n is a cubic curve over $GF(q)[t]/t^n$ such that C mod t is absolutely irreducible. There are four possibilities for C mod t:

1. C mod t is a non-singular cubic. By the Hasse-Weil bound one has $(\sqrt{q}-1)^2 \leq |C \text{ mod } t| \leq (\sqrt{q}+1)^2$

2. C mod t is a cubic with a node (i.e. a double point with two distinct "real" tangents). Such a cubic has q points.

3. C mod t is a cubic with an isolated double point (i.e. a double point with two distinct "complex conjugated" tangents). Such a cubic has $q+2$ points.

4. C mod t is a cubic with a cusp (i.e. a double point with coinciding tangents). Such a cubic has $q+1$ points.

We now calculate the number of points on the cubic curve C mod t^n.

1. If C mod t is non-singular then we have $|C \text{ mod } t^n| = q^{n-1}.|C \text{ mod } t|$ and consequently $(\sqrt{q}-1)^2.q^{n-1} \leq |C \text{ mod } t^n| \leq (\sqrt{q}+1)^2.q^{n-1}$.

2. If C mod t has a node then we can use the formula obtained in this paper. So with $r = r'' = 2$ we obtain:

   $|C \text{ mod } t^n| = q^{n-1}(q-1) + 2(q-1)q^{n-1}(1+k) + q^{2(n-k-2)}$ with $k = \frac{n}{2} - 2$ if n is even and $k = \frac{n-3}{2}$ if n is odd.

   Hence, $|C \text{ mod } t^n| = q^{n-1}(nq - n + 1)$ for all n.

3. If C mod t has an isolated double point, then the formula in this paper remains valid. With $r = 2, r'' = 0$ and k as in the previous case, we obtain that $|C \text{ mod } t^n| = (q+2)q^n$ if n is even and that $|C \text{ mod } t^n| = (q+2)q^{n-1}$ if n is odd.

4. Finally, let C mod t be a cubic curve with a cusp. In [1] it is shown that there are one or two projectively distinct curves of this type in $PG(2,q)$ according as $(q,3) = 1$ or 3 and they have the following canonical forms:

   - $(q,3) = 1 : F(X_0, X_1, X_2) = X_0X_1^2 + X_2^3$
   - $(q,3) = 3 : F(X_0, X_1, X_2) = X_0X_1^2 + X_2^3$ and $F'(X_0, X_1, X_2) = X_0X_1^2 + X_1X_2^2 + X_2^3$

The number of points on C mod t^n equals $q^{n-1}(|C \bmod t|-1)+\delta_1 = q^n+\delta_1$. First assume that $(q,3)=1$. Then δ_1 is equal to q^2 if $n=2$ and to q^2 times the number of solutions $(\tilde{U},\tilde{V})$ of $\tilde{U}^2+t\tilde{V}^3=0$ mod t^{n-2} $(\tilde{U},\tilde{V}\in GF(q)[t]/t^{n-2})$ if $n\geq 3$. One can easily check that $\tilde{U}^2+t\tilde{V}^3=0$ mod t^{n-2} has q solutions for $n=3$ (resp. q^2,q^3 and q^5 solutions for $n=4,5$ and 6).

For $n=7$ the equation $\tilde{U}^2+t\tilde{V}^3=0$ mod t^{n-2} is equivalent to the system:

$$\begin{cases} u_0^2=0 \\ 2u_0u_1+v_0^3=0 \\ 2u_0u_2+u_1^2+3v_1v_0^2=0 \\ 2u_0u_3+2u_1u_2+3v_0^2v_2+3v_0v_1^2=0 \\ 2u_0u_4+2u_1u_3+u_2^2+v_1^3+3v_0^2v_3=0 \end{cases}$$

We get $u_0=v_0=u_1=0$ and $u_2^2=-v_1^3$ while v_1,v_2,u_3,v_3,u_4 and v_4 are arbitrary in $GF(q)$. Hence, the number of solutions $(\tilde{U},\tilde{V})$ is equal to q^6 times the number of solutions $u_2\in GF(q)$ of $u_2^2=-v_1^3$ with v_1 running in $GF(q)$. The number of non-zero values $-v_1^3$ which are a square in $GF(q)$ equals $\frac{q-1}{d}$ with $d=(6,q-1)$. There correspond two values of u_2 with each of them. Consequently there are $2(\frac{q-1}{d})+1$ values for u_2. We conclude that there are $q^6(\frac{2(q-1)}{d})$ solutions $(\tilde{U},\tilde{V})$, so $\delta_1=q^8(\frac{2(q-1)}{d})$.

Next assume that $(q,3)=3$. For both $F(X_0,X_1,X_2)=0$ and $F'(X_0,X_1,X_2)=0$ one obtains the same value for δ_1.

In the situation above ($n=7$) the number of sixth powers in $GF(q)$ is needed to be known in order to calculate the number of points on C mod t^7. For higher values of n higher powers in $GF(q)$ come in.

References

[1] J.W.P. Hirschfeld, *Projective geometries over finite fields*, Clarendon Press, Oxford (1979)

[2] D. Keppens, *Polarities in n-uniform projective Hjelmslev planes*, Geom. Dedicata, 26 (1988), p. 185–214.

[3] D. Keppens, *Polarities in 2-uniform projective Hjelmslev planes*, Geom. Dedicata, 24 (1987), p. 51–76.