Bernoulli–Goss polynomial and class number of cyclotomic function fields

by

Keqin Feng and Wenyun Gao

Max–Planck–Institut
für Mathematik
Gottfried–Claren–Straße 26

D–5300 Bonn 3

Federal Republic of Germany

Dept. of Mathematics
China University of Science
and Technology
Hefei, Anhui

People's Republic of China

MPI/88–42

Bernoulli–Goss polynomial and class number of Cyclotomic function fields

Keqin Feng   Wenyun Gao

Abstract

Let $k = \mathbb{F}_q(T)$, $q = p^n$, $K = k(\Lambda_P)$ the cyclotomic function field with conductor $P = P(T)$, K^+ the maximal real subfield of K, $h_P(h_P^+)$ the class number of divisor group (of degree zero) of $K(K^+)$, $h_P^- = h_P/h_P^+ (\in \mathbb{Z})$. In the paper we prove that for any fixed $q \geq 3$, there exist infinite many of irreducible manic polynomial $P \in \mathbb{F}_q[T]$ such that $p \mid h_P^+$ and $p^{q-2} \mid h_P^-$. We also determine all regular quadratic irreducible polynomial in $\mathbb{F}_q[T]$ for $2 \leq p \leq 269$.

1. Introduction and state of results

The cyclotomic function field theory has been developed extensively in recent years (see survey articles Goss [3] and [4]). There are many analogies with cyclotomic number field case, but some situations are quite different. In number field case, for example, the well–known Kummer results says that

$$p \mid h_p^+ \Rightarrow p \mid h_p^- \Leftrightarrow p \mid h_p$$

where h_p (h_p^+) is the class number of $\mathbb{Q}(e^{\frac{2\pi i}{p}})$ ($\mathbb{Q}(e^{\frac{2\pi i}{p}} + e^{\frac{-2\pi i}{p}})$), $h_p^- = h_p/h_p^+$, p is prime number. And Vandiver conjecture says $p \nmid h_p^+$ for all odd prime number p . For function field case, the following calculated data by Ireland and Small [7] shows that each possibility can occure (p = q =3, P(T) is an irreducible polynomial in $\mathbb{F}_3[T]$. From now on, all irreducible polynomials are monic):

cases	P(T)	h_p^+	h_p^-
$3\nmid h_p^+, 3\nmid h_p^-$	$2+T^2+T^3$	$53\cdot 313$	$2^{12}\cdot 5\cdot 79$
$3\mid h_p^+, 3\mid h_p^-$	$1+2T+T^3$	3^9	$2^{12}\cdot 3^6$
$3\nmid h_p^+, 3\mid h_p^-$	$1+2T^2+T^3$	$53\cdot 313$	$2^{12}\cdot 3\cdot 131$
$3\mid h_p^+, 3\nmid h_p^-$	$2+T^2+T^4$	$2^7\cdot 3\cdot 11^2\cdot 17\cdot 29^2\cdot 421^2\cdot 191969^2$	$2^{39}\cdot 241\cdot 3329\cdot 65521\cdot 1322641$

As an analogy of number field case, we introduce the following

Definition. An irreducible $P = P(T)$ in $\mathbb{F}_q[T]$ is called regular (irregular) if $p \nmid h_p$ ($p \mid h_p = h_p^+ h_p^-$) . P is called irregular of first (second) class if $p \mid h_p^-$ ($p \mid h_p^+$) .

For finding elementary criterion of regularity of irreducible polynomial in $\mathbb{F}_q[T]$, Goss [2] introduces a series of polynomial as an analogy of classical Bernoulli number. For $j,i \geq 0$, we define

$$S_j^i(T) = \sum_{\substack{A \in \mathbb{F}_q[T] \\ \text{monic} \\ \deg A = j}} A^i$$

$$\beta_i(T) = \begin{cases} \sum_{j\geq 0} S_j^i(T), & \text{if } (q-1)\nmid i \\ -\sum_{j\geq 0} j\, S_j^i(T), & \text{if } (q-1)\,|\,i\,. \end{cases}$$

It is easy to see that $S_j^i(T) = 0$ if $j(q-1) > i$. Thus $\beta_i(T)$ is a polynomial in $\mathbb{F}_q[T]$ wich is called the Bernoulli–Goss polynomial. Goss proved that

<u>Lemma 1</u> ([2]). Let P be an irreducible polynomial in $\mathbb{F}_q[T]$, $d = \deg P$. Then P is irregular of first (second) class iff there exists i, $1 \leq i \leq q^d-2$, $(q-1)\nmid i$ ($(q-1)\,|\,i$) such that $P\,|\,\beta_i$. (So P is regular iff $P\nmid\beta_i(T)$ for each i, $1 \leq i \leq q^d-2$.)

Goss [2] and Feng [1] proved that for each q, there exist infinite many of irregular irreducible polynomials of first class; for each $q \geq 3$ there exist infinite many of irregular irreducible polynomials of second class (for $q = 2$, $h_P^- = 1$, thus there is no irregular polynomial of first class in $\mathbb{F}_2[T]$). In this paper we improve this result by the following theorem (the proof of theorem 1 is in § 2)

<u>Theorem 1</u>. For each $q \geq 3$, there exist infinite many irreducible polynomials P in $\mathbb{F}_q[T]$ such that $p\,|\,h_P^+$ and $p^{q-2}\,|\,h_P^-$. Particularly, there exist infinite many irreducible polynomials in $\mathbb{F}_q[T]$ which are irregular both in first and second class.

On the other hand, concerning to regular irreducible polynomials, the result of [6] shows that regular irreducible polynomials are rare at least for the case of $q = p$ and $\deg P = 2$. Before we state the result of [6], we make following remark. It is easy to see from the definition of $\beta_i(T)$ that $\beta_i(T) = \beta_i(T+a)$ for any $a \in \mathbb{F}_q$. Thus $P(T)\,|\,\beta_i(T) \Leftrightarrow Q(T)\,|\,\beta_i(T)$ where $Q(T) = P(T+a)$. Therefore $P(T)$ and $Q(T)$ have the same regularity, and we can consider the regularity of equivalent class of irreducible polynomials by the action of group $\{\tau_a : P(T) \longmapsto P(T+a) \mid a \in \mathbb{F}_q\}$. Particularly, for the case of $2 \mid q$, we can consider only the polynomials $P(T) = T^2 - d$ where d is a non–square element in $\mathbb{F}_q$.

Lemma 2 (Ireland and Small [6]). If $3 \leq p \leq 269$, there exist regular quadratic polynomial in $\mathbb{F}_q[T]$ for only $p = 3,5,7,13$ and 31 . There are

$p = 3,$	$T^2 + 1$
$p = 5,$	$T^2 + 3$
$p = 7,$	$T^2 + 1$
$p = 13,$	$T^2 + 5$
$p = 31,$	$T^2 + 5$ and $T^2 + 25$.

In this paper the above result is generalized to the case $q = p^n$. At first we give several criterion for regularity of quadratic irreducible polynomial (lemma 6 and 7), then all regular quadratic irreducible polynomials in $\mathbb{F}_q[T]$ are determined for $2 \leq p \leq 269$. The result is (the proof of Theorem 2 is in § 3):

Theorem 2. Let $q = p^n$, $2 \leq p \leq 269$. The following list includes all (equivalence class of) regular quadratic irreducible polynomials in $\mathbb{F}_q[T]$.

(a) $q = 2^n$, $\varphi(q-1)$ classes: $T^2 + cT + c^2d$ where c takes $\varphi(q-1)$ primitive elements of $\mathbb{F}_q$ and d is any fixed element in the set $\mathbb{F}_q - \{\alpha^2 + \alpha \mid \alpha \in \mathbb{F}_q\}$.

(b) $q = 3^n$, $\varphi(q-1)$ classes: $T^2 - d$ where d takes $\varphi(q-1)$ primitive elements of $\mathbb{F}_q$.

(c) $q = 5$, one class: $T^2 + 3$.

$q = 25$, four classes: $T^2 \pm (1 \pm 2\sqrt{2})$.

(d) $q = 7$, one class: $T^2 + 1$.

(e) $q = 13$, one class: $T^2 + 5$.

(f) $q = 31$, two classes: $T^2 + 5$ and $T^2 + 25$.

2. Proof of Theorem 1

Both proofs of Theorem 1 and Theorem 2 are based on a closed expression for Bernoulli–Goss polynomial $\beta_i(T)$ (Lemma 4). At first we list some fundamental properties of $\beta_i(T)$.

Lemma 3 (Goss [4]).

(a) (reccurence formula) $\beta_0(T) = 0$, $\beta_1(T) = 1$ and

$$\beta_i(T) = 1 - \sum_{\substack{j=1 \\ (q-1) \mid (i-j)}}^{i-1} \begin{bmatrix} i \\ j \end{bmatrix} T^j \beta_j(T) \qquad (i \geq 2) \tag{1}$$

(b) For $i \geq 1$, $\beta_i(T) \equiv 1 \pmod{T}$.

(c) $\beta_{pi}(T) = \beta_i(T)^p$ where p is the characteristic of $\mathbb{F}_q$.

(d) (congruence property) If $i_1, i_2 \geq 1$, $d \geq 1$, $i_1 \equiv i_2 \pmod{q^d-1}$, then $\beta_{i_1}(T) \equiv \beta_{i_2}(T) \pmod{T^{q^d} - T}$. Particularly, $\beta_{i_1}(T) \equiv \beta_{i_2}(T) \pmod{P}$ for any irreducible polynomial $P(T)$ in $\mathbb{F}_q[T]$ with degree d .

Let i be a positive integer, $i = c_0 + c_1 q + c_2 q^2 + \dots$ the q–adic expansion, $\ell(i) = c_0 + c_1 + c_2 + \dots$. Then $\ell(i) \equiv i \pmod{q-1}$.

Lemma 4. Suppose $i \geq 1$, $s = q-1$.

(a) $\beta_i(T) = 1$ for $\ell(i) \leq s$.

(b) If $i = a + bq^e$, $e \geq 1$, $1 \leq a, b \leq q-1$, $\ell(i) = a+b > s$, then

$$\beta_i(T) = 1 - \begin{bmatrix} b \\ r \end{bmatrix} (T^{q^e} - T)^r$$

where $r = a+b-s (s \geq 1)$.

Proof. (a) The recurrent formula (1) can be rewritten as following (let $ks = i-j$):

$$\beta_i(T) = 1 - \sum_{1 \leq ks < i} \begin{bmatrix} i \\ ks \end{bmatrix} T^{i-ks} \beta_{i-ks}(T) \tag{2}$$

We need to show that if $1 \leq ks < i$ then $\begin{bmatrix} i \\ ks \end{bmatrix} \equiv 0 \pmod p$. Suppose that $\begin{bmatrix} i \\ ks \end{bmatrix} \not\equiv 0 \pmod p$. From the Lucas formula we know that $\ell(i) > \ell(ks) \geq 1$. Since $\ell(ks) \equiv ks \equiv 0 \pmod s$ we know that $\ell(ks) \geq s$. Therefore $\ell(i) > s$ which is contradiction to the assumption $\ell(i) \leq s$.

(b) Now we suppose that $s < \ell(i) = a+b \leq 2s$. If $1 \leq ks < i$ and $\begin{bmatrix} i \\ ks \end{bmatrix} \not\equiv 0 \pmod p$, then $s \leq \ell(ks) < 2s$ by Lucas formula, and $\ell(i-ks) = \ell(i) - \ell(ks) \leq 2s-s = s$. From the part (a) we know that $\beta_{i-ks}(T) = 1$ and formula (2) becomes

$$\beta_i(T) = 1 - \sum_{1 \leq ks < i} \begin{bmatrix} i \\ ks \end{bmatrix} T^{i-ks}$$

From $\ell(ks) = s$, $ks < i = a + bq^e$, $\begin{bmatrix} i \\ ks \end{bmatrix} \not\equiv 0 \pmod p$ we know

$$ks = (s-m) + mq^e\ , \ s-a \leq m \leq b\ .$$

Thus

$$\beta_i(T) = 1 - \sum_{m=s-a}^{b} \begin{bmatrix} a \\ s\text{-}m \end{bmatrix} \begin{bmatrix} b \\ m \end{bmatrix} T^{(b-m)q^e + a + m - s}$$

$$= 1 - \sum_{\lambda=0}^{r} \begin{bmatrix} a \\ \lambda \end{bmatrix} \begin{bmatrix} b \\ b+\lambda-r \end{bmatrix} T^{(r-\lambda)q^e + \lambda}$$

$$(\text{let } \lambda = m - (s-a) = m - (b-r))$$

$$= 1 - \sum_{\lambda=0}^{r} \begin{bmatrix} a \\ \lambda \end{bmatrix} \begin{bmatrix} b \\ r-\lambda \end{bmatrix} T^{(r-\lambda)q^e + \lambda}\ .$$

But

$$\begin{bmatrix} a \\ \lambda \end{bmatrix} \begin{bmatrix} b \\ r-\lambda \end{bmatrix} = \frac{a(a-1)\ldots(a-\lambda+1)b(b\text{-}1)\ldots(b-r+\lambda+1)}{\lambda!\ \ (r-\lambda)!}$$

$$= \frac{(s-b+r)(s-b+r-1)\ldots(s\text{-}b+r-\lambda+1)b(b-1)\ldots(b-r+\lambda+1)}{\lambda!\ (r\text{-}\lambda)\ !}$$

$$\equiv (-1)^\lambda \begin{bmatrix} r \\ \lambda \end{bmatrix} \frac{(b-r+1)(b-r+2)\ldots(b\text{-}r+\lambda)b(b-1)\ldots(b-r+\lambda+1)}{r!}$$

$$= (-1)^\lambda \begin{bmatrix} r \\ \lambda \end{bmatrix} \begin{bmatrix} b \\ r \end{bmatrix} \pmod p\ .$$

Therefore

$$\beta_i(T) = 1 - \begin{bmatrix} b \\ r \end{bmatrix} \sum_{\lambda=0}^{r} \begin{bmatrix} r \\ \lambda \end{bmatrix} T^{(r-\lambda)q^e}(-T)^\lambda = 1 - \begin{bmatrix} b \\ r \end{bmatrix} (T^{q^e} - T)^r .$$

Corollary. Suppose $i = aq^e + bq^f$, $f > e \geq 0$, $1 \leq a, b \leq q-1$, $r = a+b-(q-1) \geq 1$. Then $\beta_i(T) = 1 - \begin{bmatrix} b \\ r \end{bmatrix} (T^{q^f} - T^{q^e})^r$.

This is a direct conclusion of lemma 4 and lemma 3, (c).

Lemma 5. There exist infinite many of irreducible polynomial P in $\mathbb{F}_q[T]$ satisfying the following property:

There exist a positive integer $t < \deg P$ such that $P \mid \beta_i(T)$ for all i, $1 + (q-1)q^t \leq i \leq (q-1) + (q-1)q^t$.

Proof. We need to show that for any $d_1 \geq 1$, there exists an irreducible polynomial P with degree $> d_1$ satisfying above–mentioned property. Let $e = d_1!$. From lemma 4 we know that for $1 \leq i \leq q-1$,

$$\beta_{i+(q-1)q^e}(T) = 1 - \begin{bmatrix} q-1 \\ i \end{bmatrix} (T^{q^e} - T)^i = 1 + (-1)^{i+1}(T^{q^e} - T)^i . \tag{3}$$

Thus for any irreducible polynomial Q with degree $\leq d_1$,

$$\beta_{1+(q-1)q^e}(T) \equiv 1 \pmod{Q} \tag{4}$$

From (3) we know that $\deg \beta_{1+(q-1)q^e}(T) \geq 1$, so $\beta_{1+(q-1)q^e}$ have an irreducible factor $P = P(T)$. From (4) we know that $d = \deg P > d_1$. Let t be the least non–negative residue of $e(\mathrm{mod}\ d)$. From lemma 3(d) we know that $P \mid \beta_{1+(q-1)q^t}$. But we have from (3) that

$$\beta_{1+(q-1)q^t} = 1 + (t^{q^t} - T) \Big| 1 + (-1)^{i+1}(T^{q^t} - T)^i = \beta_{i(q-1)q^t} .$$

Therefore $P \mid \beta_{i+(q-1)^t}$ $(1 \leq i \leq q-1)$. At last, from $P \mid \beta_q(T) = 1$ we know that $t \geq 1$. This completes the proof of lemma 5.

Now we are ready to prove Theorem 1. We know that the Galois group of the cyclotomic extension $k(\Lambda_P)/k$ is naturally isomorphic to $G = (\mathbb{F}_q[T]/P)^{\times}$ which is cyclic group with order q^d-1, $d = \deg P$. Let C and C^+ be the p–part of the divisor class group of $k(\Lambda_P)$ and its maximal real subfield respectively. Then C and C^+ are $\mathbb{Z}_p[G]$–module and have direct decomposition

$$C = \prod_{i=0}^{q^d-2} C(\chi^i) \,, \quad C^+ = \prod_{\substack{i=0 \\ q-1 \mid i}}^{q^d-2} C(\chi^i)$$

where $\{\chi^i \mid 0 \leq i \leq q^d-2\}$ is the character group of G. Goss and Sinnott [7] proved that

$$C(\chi^i) \neq 1 \Leftrightarrow P \mid \beta_{q^d-1-i}(T) . \qquad (5)$$

Theorem 1 is a direct conclusion of (5) and lemma 5.

3. Proof of Theorem 2

At first we give several criterion for regularity of quadratic irreducible polynomial in $\mathbb{F}_q[T]$ by considering two cases $2 \mid q$ and $2 \nmid q$ separately.

Lemma 6. Suppose $2 \mid q$, $P = T^2 + cT + d$ is an irreducible polynomial in $\mathbb{F}_q[T]$. Then

$$P \text{ is regular} \Leftrightarrow c \text{ is a primitive element of } \mathbb{F}_q .$$

Proof. From the definition of regularity we know that P is regular $\Leftrightarrow P \mid \beta_i(T)$ $(1 \leq i \leq q^2-2)$

$$\Leftrightarrow P \nmid \beta_i(T) \text{ (for all } i = a+bq,\ 1 \leq a,b \leq q-1,\ 2q-2 \geq a+b \geq q)$$
(by lemma 4 (a))

$$\Leftrightarrow \begin{bmatrix} b \\ r \end{bmatrix} (T^q + T)^r \not\equiv 1 \pmod P \text{ (for all } 1 \leq r \leq b \leq q-1,\ r < q-1)$$
(by lemma 4 (b)).

Since

$$T^{2q} \equiv (cT + d)^q = cT^q + d \equiv cT^q + T^2 + cT \pmod P$$

we know that $(T^q + T + c)(T^q + T) \equiv 0 \pmod P$. But $P \mid T^q + T$, so $T^q + T \equiv c \pmod P$. Therefore

$$P \text{ is regular} \Leftrightarrow \begin{bmatrix} b \\ r \end{bmatrix} c^r \not\equiv 1 \pmod{P} \ (\text{for all } 1 \le r \le b \le q-1, r < q-1)$$

$$\Leftrightarrow c^r \not\equiv 1 \pmod{P} \ (\text{for } 1 \le r < q-1)$$

$$\Leftrightarrow c^r \ne 1 \in \mathbb{F}_q \ (\text{for } 1 \le r < q-1)$$

$$\Leftrightarrow c \text{ is a primitive element of } \mathbb{F}_q .$$

For the case of $2 \mid q$, as we said in § 1, each equivalence class has exact one quadratic irreducible polynomial T^2-d where d is a non–square element of $\mathbb{F}_q$.

Lemma 7 Suppose $q = p^n$, $p \ge 3$, d is a non–square element of $\mathbb{F}_q$. Then following statements are equivalent to each other.

(A) T^2-d is regular;

(B) $\begin{bmatrix} b \\ r \end{bmatrix} (4d)^{r/2} \ne 1 \in \mathbb{F}_q$ (for all $2 \le r \le b \le q-1, 2 \mid r$)

(C) $4d$ is a primitive element of $\mathbb{F}_q$, and

$$g^{k/2} \prod_{j=0}^{n-1} \begin{bmatrix} b_j \\ k \end{bmatrix} \ne 1 \in \mathbb{F}_p \ (\text{for all } 2 \le k \le b_j \le p-1 , 2 \mid k)$$

where $g = (4d)^{\frac{q-1}{p-1}} \in \mathbb{F}_p$.

Proof As the same as the case $2 \mid q$, from lemma 4 we know that

$$(A) \Leftrightarrow \begin{bmatrix} b \\ r \end{bmatrix} (T^q-T)^r \not\equiv 1 \pmod{T^2-d} \ (\text{for all } 1 \le r \le b \le q-1 , r < q-1).$$

Since $T^{2q-2} \equiv d^{q-1} \equiv 1 \pmod{T^2-d}$, $T^{q-1} \equiv d^{\frac{q-1}{2}} \not\equiv 1 \pmod{T^2-d}$ (d is non–sqare element of $\mathbb{F}_q$), thus $T^{q-1} \equiv -1 \pmod{T^2-d}$ and $T^q \equiv -T \pmod{T^2-d}$. Therefore

$$(A) \quad \Leftrightarrow \begin{bmatrix} b \\ r \end{bmatrix}(-2T)^r \not\equiv 1 \pmod{T^2-d} \ (1 \le r \le b \le q-1,\ r < q-1)$$

$$\Leftrightarrow \begin{bmatrix} b \\ r \end{bmatrix}(4T^2)^{r/2} \not\equiv 1 \pmod{T^2-d} \ (2 \le r \le b \le q-1,\ 2|r < q-1)$$

$$\Leftrightarrow \begin{bmatrix} b \\ r \end{bmatrix}(4d)^{r/2} \not\equiv 1 \in \mathbb{F}_q \ \ (2 \le r \le b \le q-1,\ 2|r)$$

$$\Leftrightarrow (B)$$

(B) ⇒ (C): Taking $r = b$ in (B), we get $(4d)^{r/2} \neq 1$ for all $2 \le r \le q-1,\ 2|r$. So 4d is a primitive element of $\mathbb{F}_q$ and g is a primitive element of $\mathbb{F}_q$. For $2 \le k \le b_j \le p-1$ $(0 \le j \le n-1)$ we take $r = k\frac{q-1}{p-1} = k + kp + \dots + kp^{n-1}$ and let $b = \sum_{j=0}^{n-1} b_j p^j$. From (B) and Lucas formula we know that

$$g^{k/2} \prod_{j=0}^{n-1} \begin{bmatrix} b_j \\ k \end{bmatrix} \equiv \begin{bmatrix} b \\ r \end{bmatrix}(4d)^{r/2} \neq 1 \in \mathbb{F}_p \ .$$

(C) ⇒ (B): Suppose that $\begin{bmatrix} b \\ r \end{bmatrix}(4d)^{r/2} = 1$ for some r and b , $1 \le r \le b \le q-1$, $2|r$. Then $(4d)^{r/2} \in \mathbb{F}_p$. Since 4d is a primitive element of $\mathbb{F}_p$, we get $\frac{q-1}{p-1}\Big|\frac{r}{2}$ and $r = \sum_{j=0}^{n-1} kp^j$ for some k , $2|k$, $2 \le k \le p-1$. Let $b = \sum_{j=0}^{n-1} b_j p^j$ be the p–adic expansion. Then

$$g^{k/2}\prod_{j=0}^{n-1}\begin{bmatrix} b_j \\ k \end{bmatrix} = (4d)^{r/2}\begin{bmatrix} b \\ r \end{bmatrix} = 1$$

which is contradict to (C). This completes the proof of lemma 7.

Remark. Ireland and Small [6] proved the equivalence (A) $\Leftrightarrow$ (B) for $q = p \geq 3$. The statement (C) of lemma 7 is only concerned on the basic field $\mathbb{F}_p$ so that it can be used to prove the following remarkable result.

Lemma 8. Suppose $q = p^n$, $q' = p^m$, $p \geq 3$, $n > m$. If there exists a regular quadratic irreducible polynomial in $\mathbb{F}_q[T]$, then there exists such polynomial in $\mathbb{F}_{q'}[T]$.

Proof. Suppose that $T^2 - \frac{d}{4}$ is a regular quadratic irreducible polynomial in $\mathbb{F}_q[T]$. From lemma 7 we know that d is a primitive element of $\mathbb{F}_q$, thus $g = d^{\frac{q-1}{p-1}}$ is a primitive element of $\mathbb{F}_q$. Therefore there exists a primitive element d' in $\mathbb{F}_q$, such that $g = (d')^{\frac{q'-1}{p-1}}$. From lemma 7 (c) we know that

$$T^2 - \frac{d}{4} \in \mathbb{F}_q[T] \text{ is regular}$$

$$\Rightarrow g^{k/2}\prod_{j=0}^{n-1}\begin{bmatrix} b_j \\ k \end{bmatrix} \not\equiv 1 \pmod{p}$$

$$(\text{for all } 1 \leq k \leq b_j \leq p-1,\ 0 \leq j \leq n-1,\ 2 \mid k)$$

$$\Rightarrow g^{k/2} \prod_{j=1}^{m-1} \begin{bmatrix} b_j \\ k \end{bmatrix} \not\equiv 1 \pmod p$$

$$(\text{for all } 1 \leq k \leq b_j \leq p-1,\ 0 \leq j \leq m-1,\ 2 \mid k)$$

$$\Rightarrow T^2 - \frac{d'}{4} \in \mathbb{F}_{q'}[T] \text{ is regular.}$$

Now we are ready to prove Theorem 2. The lemma 2 says that there are no regular quadratic irreducible polynomial in $\mathbb{F}_p[T]$ for $37 \leq p \leq 269$, so there are no such polynomial in $\mathbb{F}_q[T]$ for $p \mid q$, $37 \leq p \leq 269$ by lemma 8.

For $p = 2$, the lemma 6 says that a polynomial $T^2 + cT + d$ in $\mathbb{F}_q[T]$ is regular iff c is a primitive element of $\mathbb{F}_q$. Let $A_c = \{ a^2 + ca \mid a \in \mathbb{F}_q \}$ which is an additive subgroup of $\mathbb{F}_q$ and isomorphic to $\mathbb{F}_q/_{\{0,c\}}$, thus $|A_c| = q/_2$. It is easy to see that $T^2 + cT + d$ is irreducible iff $d \notin A_c$. Therefore there exist exactly $\varphi(q-1)$ classes of regular quadratic irreducible polynomials as shown in theorem 2.

For $p = 3$, from lemma 7 (C) we know that if $T^2 - d \in \mathbb{F}_q[T]$ is regular, then d is a primitive element of $\mathbb{F}_q$ and the condition (C) is trivially satisfied. Therefore $T^2 - d$ is regular if and only if d is a primitive element of $\mathbb{F}_q$.

For $p = 5$, the lemma 2 showed that there is only one regular quadratic polynomial $T^2 + 3$ in $\mathbb{F}_5[T]$. Let $\mathbb{F}_{25} = \mathbb{F}_5[\sqrt{2}]$. If $T^2 - d$ is a regular irreducible polynomial in $\mathbb{F}_{25}[T]$, then $(-d)^{\frac{25-1}{5-1}} = 3$ from the proof of lemma 8. Thus $d = \pm 1 \pm 2\sqrt{2}$. We can varify easily that the condition (C) of lemma 7 is hold for such d. Therefore there exist exactly four regular quadratic irreducible $T^2 \pm (1 \pm 2\sqrt{2})$ in $\mathbb{F}_{25}[T]$. For $q = 125$ we have

$$3\begin{bmatrix}3\\2\end{bmatrix}\begin{bmatrix}4\\2\end{bmatrix}\begin{bmatrix}4\\2\end{bmatrix} \equiv 1 \pmod 5 .$$

From lemma 7 (C) we know that there is no such polynomial in $\mathbb{F}_{125}[T]$. By lemma 8, there is no such polynomial in $\mathbb{F}_{5^n}[T]$ for all $n \geq 3$.

For $p = 7,13$ and 31 , we have

$$(-4)^2\begin{bmatrix}5\\4\end{bmatrix}\begin{bmatrix}5\\4\end{bmatrix} \equiv 1 \pmod 7$$

$$6\begin{bmatrix}3\\2\end{bmatrix}\begin{bmatrix}7\\2\end{bmatrix} \equiv 1 \pmod{13}$$

$$11\begin{bmatrix}3\\2\end{bmatrix}\begin{bmatrix}13\\2\end{bmatrix} \equiv 24\begin{bmatrix}3\\2\end{bmatrix}\begin{bmatrix}8\\2\end{bmatrix} \equiv 1 \pmod{31} .$$

From lemma 7 (C) and lemma 8 we know that there is no regular quadratic irreducible polynomial in $\mathbb{F}_{p^n}[T]$ for $P = 7, 13, 31$ and $n \geq 2$. This completes the proof of theorem 2.

To end this paper we raise the following problem of elementary number theory:

For each prime number $p \geq 37$ and each primitive element of $\mathbb{F}_p$, are there exist integers r,b , $2 \leq 2r \leq b \leq p-1$ such that $g^r\begin{bmatrix}b\\2r\end{bmatrix} \equiv 1 \pmod p$? (The calculating result of Ireland and Small (lemma 2) says that is true for $37 \leq p \leq 269$.)

References

[1] Keqin Feng, A note on irregular prime polynomials in cyclotomic function field theory, Jour. of Number Theory, 22 (1986), 31–37.

[2] D. Goss, Kummer and Herbrand criterion in the theory of function field, Duke, Math. J. 49 (1982), 377–384.

[3] ————, The arithmetic of function fields 2: The 'cyclotomic' theory, Jour. of Algebra, 81 (1983), 107–149.

[4] ————, Analogies between global fields, Canad. Math. Soc. Conference Proceedings, Amer. Math. Soc. 7 (1987), 83–114.

[5] D. Goss and W. Sinnott, Class Group of Function Fields, Duke Math. J. 52 (1985), 507–516.

[6] K.F. Ireland and R.D. Small, A note on Bernoilli–Goss polynomials, Canad. Math. Bull., 27 (1984), 178–184.

[7] ————————————, Class Numbers of Cyclotomic Function Fields, Math. Comp. 46 (1986), 337–340.