On regularity of small primes in function fields

Ernst–Ulrich Gekeler

Max–Planck–Institut
für Mathematik
Gottfried–Claren–Straße 26
D–5300 Bonn 3

Federal Republic of Germany

MPI/89–7

On regularity of small primes in function fields

Ernst–Ulrich Gekeler

Abstract: Let $\mathfrak{p}$ be a finite prime of the rational function field $K = \mathbb{F}_q(T)$ and $K(\mathfrak{p}) : K$ the $\mathfrak{p}$–th cyclotomic extension. We study the p–component of various class groups associated with $K(\mathfrak{p})$, using criteria of Kummer–Herbrand–Ribet type and explicit formulas for Bernoulli–Goss and Bernoulli–Carlitz numbers. Results of computer calculations are given for $\mathfrak{p}$ of degree two and three and small constant fields $\mathbb{F}_q$.

1. Introduction

Let q be a power of the prime p, $\mathbb{F}_q$ the finite field with q elements, and $A = \mathbb{F}_q[T]$ the polynomial ring in an indeterminate T. Fix a prime ideal $\mathfrak{p}$ (always assumed non–zero) of A of degree $d \in \mathbb{N}$. By abuse of notation, we also write $\mathfrak{p}(T)$ for the monic irreducible polynomial that generates $\mathfrak{p}$. Let $K(\mathfrak{p})$ be the field extension of $K = \mathbb{F}_q(T)$, determined up to isomorphism by the following conditions:

(1.1) (i) $K(\mathfrak{p}) : K$ is abelian, unramified outside $\mathfrak{p}$ and ∞, and its conductor divides the divisor $\mathfrak{p} \cdot \infty$ of K;

(ii) T is a norm at ∞;

(iii) $\mathbb{F}_q$ is algebraically closed in $K(\mathfrak{p})$;

(iv) $K(\mathfrak{p})$ is maximal with (i), (ii), (iii).

Thus in terms of class field theory, the subgroup of norms in the units U_q of the q–adic completion K_q is U_q, if q is a place of K different from $\mathfrak{p}$, ∞, and is the 1–units in U_q, if q equals $\mathfrak{p}$ or ∞. Also, let $K_+(\mathfrak{p})$ be the maximal subfield of $K(\mathfrak{p})$ unramified at ∞. Then $\mathfrak{p}$ completely ramifies in $K(\mathfrak{p})$, the place ∞ splits completely in $K_+(\mathfrak{p})$, and ramifies completely in $K(\mathfrak{p}) : K_+(\mathfrak{p})$. We have canonically

$$(1.2) \quad \mathrm{Gal}(K(\mathfrak{p}) : K_+(\mathfrak{p})) \xleftarrow{\cong} \mathbb{F}_q^* \hookrightarrow (A/\mathfrak{p})^* \xrightarrow{\cong} \mathrm{Gal}(K(\mathfrak{p}) : K) = G \ .$$

An explicit construction of $K(\mathfrak{p})$ by means of "cyclotomic" polynomials may be found in [9]. By the far–reaching analogy of K with the rational number field $\mathbb{Q}$, $K(\mathfrak{p})$ and $K_+(\mathfrak{p})$ correspond to the p–th cyclotomic field extension $\mathbb{Q}(p)$, the maximal real subfield $\mathbb{Q}_+(p)$ of $\mathbb{Q}(p)$, respectively, see [9, 3, 7].

Let $C = C(\mathfrak{p})$ be the p–primary part of the group of degree zero divisor classes of $K(\mathfrak{p})$, and C_∞ the subgroup of classes supported by the infinite primes of $K(\mathfrak{p})$. Then we have an exact sequence of finite p–groups

$$0 \longrightarrow C_\infty \longrightarrow C \longrightarrow \tilde{C} \longrightarrow 0 \quad , \tag{1.3}$$

where $\tilde{C}$ is the p–part of the ideal class group Pic B, B = integral closure of A in $K(\mathfrak{p})$. Similarly, if $K \subset L \subset K(\mathfrak{p})$ is an intermediate field and B_L, $C_{\infty,L}$, C_L, $\tilde{C}_L$ are the objects associated with L,

$$0 \longrightarrow C_{\infty,L} \longrightarrow C_L \longrightarrow \tilde{C}_L \longrightarrow 0 \tag{1.3$_L$}$$

is also exact. If $L = K_+(\mathfrak{p})$, we write B_+, C_+..... for B_L, C_L .....

(1.4) Let now $K \subset L \subset M \subset K(\mathfrak{p})$ be two intermediate fields. The natural mapping $i : C_L \longrightarrow C_M$ composed with the norm $N : C_M \longrightarrow C_L$ is multiplication with $[M : L]$, which is prime to p. Hence i is injective and N is surjective, and corresponding statements hold for C replaced by C_∞ and $\tilde{C}$.

(1.5) Let W be the ring of Witt vectors of the finite field $A/\mathfrak{p}$, and $\mathfrak{m}$ its maximal ideal. All the W–valued characters of $G = (A/\mathfrak{p})^*$ are powers ω^k $(0 \leq k < q^d-1)$ of the Teichmüller character $\omega : G \longrightarrow W^*$, which satisfies $\omega(g) \equiv g \bmod \mathfrak{m}$, $g \in G$. Tensoring with W over $\mathbb{Z}_p$, we may decompose our class groups according to characters of G :

$$C \underset{\mathbb{Z}_p}{\otimes} W = \bigoplus_{0 \leq k < q^d-1} C(\omega^k) \quad ,$$

similarly for C_∞ and $\tilde{C}$. We write $C(k)$ for $C(\omega^k)$.

1.6 Lemma: For any intermediate field $K \subset L \subset K(\mathfrak{p})$,

$$C_L \otimes W = \oplus\, C(\chi) \ ,$$

where the sum on the right hand side is over those characters $\chi : G \longrightarrow W^*$ that factorize over $\mathrm{Gal}(L : K)$.

Proof: Let $H = \mathrm{Gal}(K(\mathfrak{p}) : L)$. By (1.4), it suffices to show that $C^H = C_L$. Since $\#(H)$ is prime to p, $H^2(H,C) = 0$. But H is cyclic, so $C^H/N(C) = \hat{H}^0(H,C) = 0$, where N is the norm of $K(\mathfrak{p}) : L$.

In particular, $C(\omega^0) = 0$, and

$$C_+ \otimes W = \bigoplus_{\substack{0<k<q^d-1 \\ k\equiv 0\,(q-1)}} C(k) \ . \tag{1.7}$$

Note also that for $k \equiv 0\ (q-1)$, $C_\infty(k) = 0$ and $C(k) \xrightarrow{\simeq} \tilde{C}(k)$, which follows from the ramification type of $K(\mathfrak{p}) : K_+(\mathfrak{p})$.

1.8 Definition: The prime $\mathfrak{p}$ is regular, if $C = 0$. Otherwise, it is called irregular; plus–irregular or minus–irregular, if there exists $k < q^d-1$, $k \equiv 0\ (q-1)$ or $k \not\equiv 0\ (q-1)$, respectively, with $C(k) \neq 0$.

The different components $C(k)$ are not quite independent. Define the equivalence relation

(1.9) $\quad k' \underset{p}{\sim} k \iff$ there exists a p–power p^n such that

$$k' \equiv p^n \cdot k \ (q^d - 1) \ .$$

Then from the action of the Frobenius automorphism on W, we derive

(1.10) $\quad k' \sim k$ implies $C(k') \cong C(k)$,

and the corresponding statements for C_m and $\tilde{C}$.

2. We give some numerical criteria, analogous with the Kummer–Herbrand–Ribet criterion, for the non–vanishing of $C(k)$. These involve two different series of Bernoulli – like numbers, corresponding to zeta values at positive and negative integers. First, define for non–negative i

$$(2.1) \qquad \begin{aligned} [i] &= T^{q^i} - T \\ L_i &= [i]\,[i-1]\,\ldots\,[1] \\ D_i &= [i]\,[i-1]^q \ldots\, [1]^{q^{i-1}} \quad . \end{aligned}$$

In particular, $[0] = 0$ and $L_0 = D_0 = 1$. Further, for k given in its q–adic expansion $k = \sum a_i q^i$, $0 \le a_i < q$, let

$$\Gamma_k = \prod D_i^{a_i} \quad \text{and}$$

$$\ell(k) = \sum a_i$$

the sum of its q–adic digits. Note that for $i > 0$, $[i]$ is the product of all the monic primes whose degree divides i. Γ_k is the substitute for the factorial $k! = \Gamma(k+1)$ in our context. Put

$$e(X) = \sum_{k \ge 0} X^{q^k} / D_k$$

as a formal power series, and define the Bernoulli–Carlitz numbers $B(k) \in K$ by

(2.2) $$\frac{X}{e(X)} = \sum_{k \geq 0} \frac{B(k)}{\Gamma_k} X^k \quad \text{(see [1,6])}.$$

Then $B(0) = 1$, $B(k) = 0$ unless $q \equiv 0\ (q-1)$, and e.g. $B(k) = (-1)^i (D_1 \ldots D_{i-1})^{q-1}/L_i$, if $k = q^i - 1$. There is a von Staudt–like result on the denominator of $B(k)$, which in particular implies that $B(k)$ is p–integral if $k < q^d - 1$. Besides the above and the mysterious identities of [5], nothing is known about the $B(k)$. Next, let

(2.3) $$s_i(k) = \sum a^k \ ,$$

summing over the monic polynomials of degree i in A . Then $s_i(k) = 0$ for $i > \ell(k)/(q-1)$ [4, 2.12]. Hence we may define the Bernoulli–Goss numbers $\beta(k)$ (see [7]) by

(2.4) $$\beta(k) = \sum_{i \geq 0} s_i(k) \qquad k \not\equiv 0\ (q-1)$$

$$= -\sum_{i \geq 0} i\, s_i(k) \qquad k \equiv 0\ (q-1)\ .$$

The $s_i(k)$ (and therefore the $\beta(k)$) satisfy

(2.5) $$s_i(pk) = s_i(k)^p$$

and the Kummer congruences

(2.6) $$s_i(k') \equiv s_i(k) \bmod p \ , \ \text{if} \ k' \equiv k \ (q^d-1) \ .$$

In particular,

(2.7) $$p \,|\, \beta(k) \Rightarrow p \,|\, \beta(k') \ , \ \text{if} \ k' \underset{p}{\sim} k \ .$$

Our interest in $B(k)$ and $\beta(k)$ results from the next two theorems.

2.8. Theorem [7, 6.2.2]: Let $0 < k < q^d-1$. Then

$$C(k) \not\equiv 0 \iff p \,|\, \beta(q^d-1-k) \ .$$

2.9. Theorem [12, 2.18]: Let $0 < k < q^d-1$, k divisible by $q-1$. Then

$$\tilde{C}(k) \not\equiv 0 \Rightarrow p \,|\, B(k)$$

(i.e., p divides the numerator of $B(k)$) .

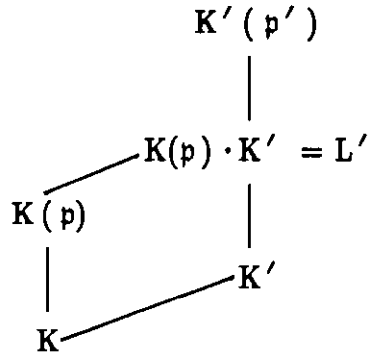
2.10. Remark: In view of (1.10), an equivalence above would imply a statement like (2.7) for $B(k)$. In fact, it is easy to see that if $pk < q^d-1$, $p \,|\, B(k)$ implies $p \,|\, B(pk)$. But in general, (2.7) doesn't hold for $B(k)$. A counterexample is given by $q = 3$ and $p(T) = T^3-T-1$, which divides $B(10)$, but not $B(4)$ $(4 + 3^3-1 = 3 \cdot 10)$.

From 2.8, we may derive the stability of divisibility properties of $\beta(k)$ under constant field extensions. Let $r > 1$ be a natural number and $K' = \mathbb{F}_{q^r}(T)$. We denote with a

prime $(\ )'$ all the objects related to K' instead of K. Suppose the degree d of $\mathfrak{p}$ is relatively prime with r. Then $\mathfrak{p}$ is inert in K'. Let $\mathfrak{p}'$ be the corresponding prime in K', $n = q^d - 1$, $n' = q^{rd} - 1$.

2.11. Theorem: If p divides $\beta(k)$, then p' divides the Bernoulli–Goss number $\beta'(k')$ associated with K', where $k' = k \cdot n'/n$.

Proof: By (2.6), we may assume that $k < n$, so $k' < n'$. Consider the field extensions



Then $G' = \mathrm{Gal}(K'(\mathfrak{p}') : K') = (A'/\mathfrak{p}')^*$ acts on L' via the norm $N : (A'/\mathfrak{p}')^* \longrightarrow (A/\mathfrak{p})^* = \mathrm{Gal}(L' : K') = \mathrm{Gal}(K(\mathfrak{p}) : K) = G$. If we think of W imbedded in W', we have $\omega \circ N = \omega'^{n'/n}$ for the Teichmüller character ω' of G'. Combined with (1.6) and the injectivity of $C \longrightarrow C'_{L'}$, we get "$C(n-k) \neq 0 \Rightarrow C'((n-k)n'/n) \neq 0$", which by (2.8) is equivalent with the assertion.

3. Next, we show how to calculate $B(k)$ and $\beta(k)$ effectively. Directly from definitions, we get the recursion formula for $B(k)$

$$B(k) = -\sum_{i>0} \frac{\Gamma_k}{D_i \Gamma_{k+1-q^i}} B(k+1-q^i) \qquad (k > 0) \ . \tag{3.1}$$

Also, $\beta(k)$ might be calculated via the recursion described in [7]. Instead, we will use the generating function for $s_i(k)$, derived in [4], which is computationally simpler:

$$\sum_{k\geq 0} s_i(k)\, X^k = (-1)^i \frac{D_i}{L_i} \frac{X^{q^i}-1}{e_i(X^{-1})X^{q^i} - D_i X^{q^i}} \ , \tag{3.2}$$

where

$$e_i(X) = \sum_{0\leq j\leq i} (-1)^{i-j} \frac{D_i}{D_j L_{i-j}^{q^j}} X^{q^j} \ .$$

The resulting $B(k)$ and $\beta(k)$ are rational functions or polynomials in T of very large degrees, but, using invariance properties, we can drastically reduce the degrees. Let V (resp. U) be the group of affine transformations $T \mapsto aT + b$ $(a,b \in \mathbb{F}_q)$, where $a \neq 0$ (resp. $a = 1$), and put $S = [1] = T^q - T$, $R = S^{q-1}$. Then V acts on $A = \mathbb{F}_q[T]$, and the invariants are

$$A^U = \mathbb{F}_q[S] =: A_0 \ , \quad A^V = \mathbb{F}_q[R] =: A_1 \ . \tag{3.3}$$

Since the coordinate change $T \mapsto T + b$ affects neither $[i]$ nor $s_i(k)$, $B(k)$ and

$\beta(k)$ may be expressed through S.

3.4. Lemma: Let $k \equiv 0 \ (q-1)$. Then $B(k)$, considered as a rational function in T, satisfies

$$B(k)(aT) = a^{-\ell(k)/(q-1)}B(k)(T) \qquad (0 \neq a \in \mathbb{F}_q) \ .$$

Proof: For $k = \sum a_i q^i$ given in its q–adic expansion, let $\vartheta(k) = \sum i\, a_i$. Then the assertion follows by induction from (3.1) and the following easily proved facts:

$$\begin{aligned} [k](aT) &= a[k](T) \\ D_k(aT) &= a^k D_k(T) \\ \Gamma_k(aT) &= a^{\vartheta(k)}\Gamma_k(T) \\ \vartheta(k) &\equiv \frac{k-\ell(k)}{q-1} \bmod(q-1) \ . \end{aligned}$$

In view of the lemma, it is convenient to somewhat modify the definition of $B(k)$. Let $m = q-1$, and define

$$B^*(k) = S^{\ell(k)/m}B(k) \ , \tag{3.5}$$

which by (3.3) and (3.4) is a rational function in R. Since $S = [1] = \prod (T-b)$ $(b \in \mathbb{F}_q)$, $B(k)$ and $B^*(k)$ have the same prime divisors $\mathfrak{p}(T)$ of degree > 1. Let further $L_k^* = S^{-k}L_k \in \mathbb{F}_q[R]$, and, for $0 < k \equiv 0 \ (q-1)$ given q–adically

$$k = \sum_{0 \le j \le N} a_j q^j, \text{ and } \ 0 < i \le N \ ,$$

$r(i,k) = \inf(\{j \mid a_j < m\}, i)$,

$s(i,k) = \inf\{j \geq i \mid a_j > 0\}$, if $r(i,k) < i$, and $s(i,k) = i$ otherwise.

3.6. Lemma: $B^*(k) = -\sum_{i>0} \frac{L^*_{s(i,k)}}{L^*_{r(i,k)} L^*_i} B^*(k+1-q^i)$.

Proof: Let $0 < i \leq N$ be given, $r = r(i,k)$, $s = s(i,k)$. The q–adic expansion of $k+1-q^i$ is given by

$$k+1-q^i = a_i q^i + \dots a_N q^N \qquad (r = i)$$

$$= (a_r+1)q^r + a_{r+1}q^{r+1} + \dots a_{i-1}q^{i-1} + m\,q^i + \dots m\,q^{s-1}$$

$$+ (a_s-1)q^s + a_{s+1}\,q^{s+1} + \dots a_N q^N \qquad (r < i) \ .$$

Therefore, in both cases, $\frac{\Gamma_k}{D_i\,\Gamma_{k+1-q^i}} = \frac{(D_1 \dots D_{r-1})^m D_s}{D_i\,D_r (D_i \dots D_{s-1})^m}$.

But for all i , $D_i = (D_i \dots D_{i-1})^m L_i$, hence $\frac{\Gamma_k}{D_i \Gamma_{k+1-q^i}} = \frac{L_s}{L_r\,L_i}$. Since $\ell(k+1-q^j) = \ell(k) + (s-i-r)m$, the assertion follows from (3.1).

For the $s_i(k)$, we have by definition

(3.7) $$s_i(k)(aT) = a^{ik} s_i(k)(T) \ .$$

Thus if $\beta(k) = \sum b_{k,j} S^j$, $b_{kj} \neq 0$ implies $j \equiv k$, $2k \ldots (m)$. In particular:

(3.8) If $k \equiv 0(m)$, $s_i(k)$ and $\beta(k)$ are polynomials in $R = S^{q-1}$.

4. We now derive explicit expressions for $B^*(k)$ and $\beta(k)$, in case $0 < k < q^3-1$. First, note that each $k < q^3-1$ divisible by $m = q-1$ has a unique representation $k = s(q^2-1) + t(q-1)$, where either $(0 \le s < q,\ 0 \le t < q)$ or $(s = q,\ t = 0)$.

4.1. Theorem: Let $k = s(q^2-1) + t(q-1)$ as above. Then

$$B^*(k) = \frac{R^s}{R+1} \qquad (t = 0)$$

$$= (-1)^t \sum_{0 \le i \le s} (-1)^i \begin{bmatrix} t+i-1 \\ i \end{bmatrix} R^{s-i} \qquad (t > 0)\ .$$

Proof: Since $k < q^3-1$, the sum in (3.6) contains only two terms. For $k = a + bq + cq^2$, $0 \le a,b,c \le m = q-1$, we get $B^*(k) = -\alpha B^*(k+1-q) - \beta B^*(k+1-q^2)$, where $\alpha = R+1$ $(a < m,\ b = 0,\ c > 0)$, $\alpha = 1$ otherwise, $\beta = (R+1)^{-1}$ $(a = b = m,\ c = 0)$, and $\beta = 1$ otherwise. The result now follows by double induction on s and t, which involves some case considerations on the q–adic expansion of $k = s(q^2-1) + t(q-1)$. We omit the details.

4.2. Corollary: If $k = s(q^2-1)$ $(1 \le s \le q)$ or $k = s(q^2-1) + q(q-1)$ $(1 \le s < q)$, each prime divisor $p(T)$ of (the numerator of) $B^*(k)$ has degree one.

Proof: The first case is clear. In the second case, all the binomial coefficients $\begin{bmatrix} q+i-1 \\ i \end{bmatrix}$ vanish except for $i = 0$, hence $B^*(k) = -R^s$.

4.3. Corollary: Let $k = (q-1)(q^2-1) + t(q-1)$ $(1 \le t \le q)$. Then $B^*(k) = (-1)^t R^{t-1}(R+1)^{q-t}$, and is not divisible by primes $p(T)$ of degree > 2.

Proof: As above, $\begin{bmatrix} t+i-1 \\ i \end{bmatrix}$ vanishes for $i > q-t$. Hence

$$B^*(k) = (-1)^t \sum_{0 \le i \le q-t} (-1)^i \begin{bmatrix} t+i-1 \\ i \end{bmatrix} R^{q-1-i}$$

$$= (-1)^t \sum \begin{bmatrix} q-t \\ i \end{bmatrix} R^{q-1-i}$$

$$= (-1)^t R^{t-1} \sum \begin{bmatrix} q-t \\ i \end{bmatrix} R^{q-t-i}$$

$$= (-1)^t R^{t-1} (R+1)^{q-t} \ .$$

Further $R+1 = S^{q-1}+1 = [2]/[1]$, which is the product of all monic irreducible quadratic polynomials $\mathfrak{p}(T)$.

The corollaries give vanishing results for p–class groups $\tilde{C}(k)$ for primes $\mathfrak{p}(T)$ of degree > 2 . Other special cases of (4.1) are

(4.4)
$$k = s(q^2-1) + q-1 \qquad (1 \le s < q)$$
$$B^*(k) = -(R^{s+1} + (-1)^s)/(R+1)$$

and

(4.5)
$$k = q^2-1 + t(q-1) \qquad (1 \le t \le q)$$
$$B^*(k) = (-1)^t(R-t) \ .$$

Next, let us consider $\beta(k)$, where k has the q–adic expansion $a + bq + cq^2$,

$\ell = \ell(k) = a+b+c$, $m = q-1$. Since $k < q^3-1$, $s_i(k) = 0$ if $i > 2$, and we have to calculate $s_2(k)$, $s_1(k)$, and $s_0(k) = 1$. From (3.2), one may derive the following expression for $s_2(k)$ (see [4, 3.13]):

$$(4.6) \qquad s_2(k) = (-1)^a \begin{bmatrix} a \\ m-a \end{bmatrix} \begin{bmatrix} a+c-m \\ m-b \end{bmatrix} S^{\ell(q+1)+1-q^2-(a+1)m}(1+S^m)^{a+c-m} \ ,$$

which vanishes if $\ell = a+b+c < 2m$.

For $i = 1$, the generating function (3.2) becomes

$$\sum s_1(k)X^k = -X^m/(1-X^m-SX^q) \ , \ m = q-1 \ , \ S = [1] = T^q-T \ .$$

We read off

$$s_1(k) = -\sum \begin{bmatrix} \alpha+\beta \\ \beta \end{bmatrix} S^\beta \ ,$$

summing over pairs (α,β) of non–negative integers that satisfy

$$(*) \qquad \alpha m + \beta q = k-m \ .$$

Let (α_0, β_0) be the solution with α_0 maximal. All the other solutions are given by (α_i, β_i) , $\alpha_i = \alpha_0 - iq$, $\beta_i = \beta_0 + im$, $i \leq \alpha_0/q$. We have to separate the cases A) $\ell < m$, B) $m \leq \ell < 2m$, and C) $2m \leq \ell$. In case A , $s_1(k) = 0$. In case B , $\alpha_0 = m-a+cq$, $\beta_0 = \ell-m$. Looking at the q–adic expansions of $\alpha_i + \beta_i$ and of β_i , and using Lucas' congruence on binomial coefficients, one sees that $\begin{bmatrix} \alpha_i+\beta_i \\ \beta_i \end{bmatrix} = 0$ unless $b+c-q < i \leq \ell-m$, in which case one has

$$\begin{bmatrix} \alpha_i+\beta_i \\ \beta_i \end{bmatrix} = \begin{bmatrix} b+c-i \\ \ell-m-i \end{bmatrix} \begin{bmatrix} c \\ i \end{bmatrix} .$$

Now suppose C , i.e., $\ell \geq 2m$. Then $\alpha_0 = m-a+(c+1)q$, $\beta_0 = \ell-2m$. Again determining q–adic expansions yields

$$\begin{aligned} \begin{bmatrix} \alpha_i+\beta_i \\ \beta_i \end{bmatrix} &= \begin{bmatrix} b+c-m-i \\ m-a \end{bmatrix} \begin{bmatrix} c+1 \\ i \end{bmatrix} && (i \leq \ell-2m) \\ &= 0 && (\ell-2m < i \leq b+c-m) \\ &= \begin{bmatrix} b+c+1-i \\ m-a \end{bmatrix} \begin{bmatrix} c \\ i-1 \end{bmatrix} && (b+c-m < i \leq c+1) \\ &= 0 && (c+1 < i) \ . \end{aligned}$$

With the usual conventions $\begin{bmatrix} n \\ k \end{bmatrix} = 0$ if $k < 0$ or $k > n$, all these cases are included in

(4.7)

$$s_1(k) = \sum_{0 \leq i \leq \ell-2m} \begin{bmatrix} b+c-m-i \\ m-a \end{bmatrix} \begin{bmatrix} c+1 \\ i \end{bmatrix} S^{\ell+(i-2)m} \quad - \sum_{b+c-m \leq i \leq c} \begin{bmatrix} b+c-i \\ m-a \end{bmatrix} \begin{bmatrix} c \\ i \end{bmatrix} S^{\ell+(i-1)m} .$$

Summarizing:

4.8. Theorem: Let $0 < k = a+bq+cq^2 < q^3-1$ with $0 \leq a,b,c < q$, $\ell = a+b+c$, $m = q-1$. Then

$$\begin{aligned} \beta(k) &= 1 + s_1(k) + s_2(k) && (k \not\equiv 0(m)) \\ &= -s_1(k) - 2s_2(k) && (k \equiv 0(m)) \ , \end{aligned}$$

the $s_i(k)$ being given by (4.6) and (4.7).

Note that since $k \equiv \ell(m)$, $k \equiv 0(m)$ means $\ell = m$ or $2m$. For the binomial coefficients $\begin{bmatrix} n \\ r \end{bmatrix}$ in (4.6) and (4.7), always $r,n \in \{0,\ldots,q-1\}$, with the exception of $n = c+1 = q$ in (4.7). But $\begin{bmatrix} q \\ i \end{bmatrix} \equiv 0(p)$ if $0 < i < q$. Hence (4.8) may directly be implemented for computer calculations.

4.9. Example: Let $k = a+bq$. Then

$$\begin{aligned} \beta(k) &= 1 && (\ell \leq m) \\ &= 1 - \begin{bmatrix} b \\ m-a \end{bmatrix} S^{\ell-m} && (m < \ell \leq 2m) \ . \end{aligned}$$

(A special case of this has been shown in [10].)

4.10. Example: Let $k = a + mq + cq^2$, $0 < a+c \leq m$. Then

$$\beta(k) = 1 + (-1)^{a+1} S^{a+cq} \ .$$

4.11. Example: Let $k = a + bq + cq^2$, $\ell = a+b+c = 2m$. Then

$$\beta(k) = 1 + \sum_{b+c-m \leq i \leq c} \begin{bmatrix} b+c-i \\ m-a \end{bmatrix} \begin{bmatrix} c \\ i \end{bmatrix} R^{i+1} + 2(-1)^{a+1} \begin{bmatrix} c \\ m-a \end{bmatrix} \sum_{0 \leq i \leq a+c-m} \begin{bmatrix} a+c-m \\ i \end{bmatrix} R^{q-a+i} \ ,$$

where $R = S^{q-1}$. Specializing b yields e.g.

$$\begin{aligned} \beta(k) &= 1 + (-1)^{c+1} R^{c+1} && (k = m-c + mq + cq^2) \ , \text{ or} \\ \beta(k) &= 1 + (-1)^c c \, R^c (R+1) && (k = m-c+1+(m-1)q+cq^2, \ c > 0) \ . \end{aligned}$$

5. By the results of the last section, we are given $B(k)$ and $\beta(k)$ as rational functions (or polynomials) in $S = T^q - T$ or even in $R = S^{q-1}$. Therefore, we examine the behavior of prime ideals in the ring extensions

$$\begin{array}{l} A = \mathbb{F}_q[T] \\ | \\ A_0 = \mathbb{F}_q[S] \\ | \\ A_1 = \mathbb{F}_q[R] \end{array} .$$

More precisely, given a prime ideal $\mathfrak{p}$ of A of degree ≤ 3 and $f \in A_0$ or A_1, we want to decide whether $\mathfrak{p} | f$. Let K_0 and K_1 be the quotient fields of A_0, A_1, respectively. The following is obvious:

(5.1) $K : K_0$ is galois with group $\mathbb{F}_q$, $b \in \mathbb{F}_q$ acting via $T \mapsto T+b$. It is unramified at finite places and completely ramified at ∞. The $T+b$ are the zeroes of the minimal polynomial $\phi(X)-S = X^q - X - S \in A_0[X]$. A prime $\mathfrak{p}_0$ of A_0 splits into q or q/p primes $\mathfrak{p}$ of A (since the residual extension must be cyclic).

5.2. Lemma: The following statements are equivalent:

(i) $\mathfrak{p}_0$ splits completely, i.e., into q factors;

(ii) $\phi(X)-S \bmod \mathfrak{p}_0$ has one, thus all its zeroes in $A_0/\mathfrak{p}_0$;

(iii) $\mathrm{Tr}(s) = 0$, where s is the class of $S \bmod \mathfrak{p}_0$ and $\mathrm{Tr} : A_0/\mathfrak{p}_0 \longrightarrow \mathbb{F}_q$ is the trace map.

Proof: (i) $\Leftrightarrow$ (ii) is obvious. Let F be the Frobenius automorphism of $A_0/\mathfrak{p}_0 : \mathbb{F}_q$. Then $\phi(A_0/\mathfrak{p}_0) = \mathrm{im}(F-1) \subset \mathrm{Ker}(\mathrm{Tr})$. By dimension reasons, $\mathrm{im}(F-1) = \mathrm{Ker}(\mathrm{Tr})$, hence

(ii) $\Leftrightarrow$ (iii) .

5.3. Corollary: The primes $\mathfrak{p}(T)$ of degree $d = 2$ in A are those lying over primes $\mathfrak{p}_0(S)$ of A_0 that satisfy a) $\deg \mathfrak{p}_0 = 2$, $Tr(s) = 0$, or b) $\mathfrak{p}_0(S) = S-a$, $0 \neq a \in \mathbb{F}_q$, case b) occurring in char 2 only. Similarly, the primes $\mathfrak{p}(T)$ of degree $d = 3$ in A are those over $\mathfrak{p}_0(S)$ that satisfy a) $\deg \mathfrak{p}_0 = 3$, $Tr(s) = 0$, or b) $\mathfrak{p}_0(S) = S-a$, $0 \neq a \in \mathbb{F}_q$, where b) occurs in char 3 only.

Next, which primes $\mathfrak{p}_1$ in A_1 lie below the $\mathfrak{p}_0$ described above ? Note that $\prod_{0 \neq a \in \mathbb{F}_q} (S-a) = S^{q-1}-1 = R-1$, hence we may restrict to cases a).

Let first $d = 2$. If $p = 2$, no $\mathfrak{p}_0$ as required exists. If $p > 2$, the product over the monic irreducible S^2-b gives $S^{q-1}+1 = R+1$.
Let now $d = 3$. In any case, the product $\prod \mathfrak{p}(T)$ over the primes of degree 3 equals

$$[3]/[1] = ([1]^{q^2} + [1]^q + [1])/[1] = S^{q^2-1} + S^{q-1} + 1 = R^{q+1} + R + 1 \ ,$$

which is divisible by $(R-1)$, if $q \equiv 0(3)$, and by $(R-\rho)(R-\rho^2)$, if $q \equiv 1(3)$ and ρ is a primitive third root of unity. Besides these linear factors, $R^{q+1} + R + 1$ is divisible by $q/3$, $(q-1)/3$, $(q+1)/3$ different cubic irreducible factors, if $q \equiv 0,1,2(3)$, respectively. Summing up, the following primes $\mathfrak{p}_1(R)$ of $A_1 = \mathbb{F}_q[R]$ decompose into primes $\mathfrak{p}(T)$ of degree $d = 2$ or 3 of $A = \mathbb{F}_q[T]$:

(5.4) $d = 2$: $\mathfrak{p}_1(R) = R+1$

$d = 3$: $\mathfrak{p}_1(R)$ = irreducible cubic divisor of $R^{q+1} + R + 1$, or $R-1$ ($q \equiv 0(3)$ only), or $R-\rho$, $R-\rho^2$ ($q \equiv 1(3)$ only, ρ = prim. third root of unity).

Playing around with Newton's formulas, one can show that the cubic divisors of $R^{q+1} + R + 1$ have necessarily the form $R^3 + aR^2 + (a-3)R - 1$. The special primes $\mathfrak{p}(T)$ dividing $R-1$, $R-\rho$, $R-\rho^2$ respectively are those having a non–trivial stabilizer group under $T \longmapsto aT+b$, i.e., $\mathfrak{p}(T) = T^3 - bT - c$, b a square ($q \equiv 0(3)$) , and $\mathfrak{p}(T) = T^3 - c$ ($q \equiv 1(3)$, c a non–cube). Combined with Theorems 4.1 and 4.8, the considerations above enormously simplify the verification of $\mathfrak{p} \mid \beta(k)$ or $B(k)$.

6. Applications

Let now $\mathfrak{p}$ be a prime of A of degree ≤ 3. If $d = 1$, $K(\mathfrak{p})$ is rational and has trivial class group, so we exclude that case. If $d = 2$, $K_+(\mathfrak{p})$ is rational, so all of the $C(k)$ with $k \equiv 0\ (q-1)$ are trivial (which corresponds to the fact that all the associated $\beta(k)$ and $B(k)$ are never divisible by primes of degree 2). Hence only $\beta(k)$ with $0 < k < q^2-1$, $k \not\equiv 0\ (q-1)$ is interesting. Recall that $m = q-1$.

6.1. Theorem: Let $q \equiv 3(4)$, $q \geq 7$, and let $\mathfrak{p}(T)$ be a prime divisor of $\mathfrak{p}_0(S) = S^2+1$. Then $\mathfrak{p}$ is irregular. (The prime divisors of S^2+1 are the shifts under $T \mapsto T+b$ of $T^2+1/4$.)

Proof: Let $k = m + bq$, where $0 < b < m$, $b \equiv 0(4)$. Then from (4.9), $\beta(k) = 1-S^b$, which is divisible by S^2+1. The result now follows from Thm. 2.8.

But the most interesting case is where $d = 3$.

6.2. Theorem: Let $\mathfrak{p}(T)$ be a special prime of degree 3 (see (5.4)). Then $\mathfrak{p}$ is plus–irregular.

Proof: Let $k = m-c + mq + cq^2$, where $0 < c \leq m$, $c \equiv 2(6)$. From (4.11), we have $\beta(k) = 1 + (-1)^{c+1}R^{c+1}$, which is divisible by $R-1$ in char 3, and by $(R-\rho)(R-\rho^2)$, if $q \equiv 1(3)$.

Recall that in the number field case, the class number of $\mathbb{Q}_+(p)$ should not be divisible by p by Vandiver's conjecture. Actually, it occurs very rarely that a non–special prime $\mathfrak{p}$ is plus–irregular.

6.3. Example: For $q \leq 64$, there are only 4 examples of non–special plus–irregular primes of degree 3, involving $\mathbb{F}_q$ with $q = 16, 32, 47, 49$. The examples with the non–prime fields are complicated to be written down. For $q = 47$, let $\mathfrak{p}(T)$ be the prime $T^3 + 5T + 20$, which divides $\mathfrak{p}_1(R) = R^3 + 41\,R^2 + 38\,R + 46$. For $k = 81\,696 = 10 + 46 \cdot 47 + 36 \cdot 47^2$, (4.11) gives $\beta(k) = 1 - R^{37}$, which is divisible by $\mathfrak{p}_1$! Hence $\mathbb{F}_{47}(T)_+(\mathfrak{p})$ has a class number divisible by 47.

Let now $\mathfrak{p}$ have degree 3, n a divisor of q^3-1, and let $K \subset L \subset K(\mathfrak{p})$ be the unique intermediate field of degree n over K. Then $\mathrm{Gal}(K(\mathfrak{p}) : L) = \{n\text{–th powers in } (A/\mathfrak{p})^*\} =: H$, and the ramification group of $L : K$ at ∞ is $\mathbb{F}_q^*/\mathbb{F}_q^* \cap H$.

6.4. Example: Let $p > 2$ and $n = 2$. Then L is ramified at ∞, and the Hurwitz formula shows L to be elliptic. Since T is a norm at ∞, the elliptic curve E associated with L is given by the equation $-Y^2 = \mathfrak{p}(T)$. The relevant Bernoulli–Goss number is

$$\beta((q^3-1)/2) = 1 - \sum_{0 \leq i \leq m/2} \binom{m-i}{m/2} \binom{m/2}{i} S^{m/2+im},$$

whose divisibility by $\mathfrak{p}$ is equivalent with E having non–trivial p–division points over $\mathbb{F}_q$.

6.5. Example: Let $q \equiv 1(3)$ and $n = 3$. Then L is unramified at ∞, and Hurwitz again gives L elliptic. The relevant B.–G. numbers are $\beta(k)$ for $k = k_i = i(q^3-1)/3$, $i = 1,2$. We have $\beta(k_1) = 1$, and $\beta(k_2)$ is a polynomial in R given by (4.11). In the range $q \leq 64$, $\beta(k_2)$ has cubic prime divisors only for $q = 49$.

In the next examples, we let $\mathfrak{p}(T)$ have degree 2 and, assuming $n \mid q^2-1$, we consider the unique subfield L of $K(\mathfrak{p})$ of degree n over K. Let $k_i = i(q^2-1)/n$, $0 < i < n$.

6.6. Example: Let $q \equiv 1(3)$ and $n = 3$. L is ramified at ∞, and elliptic with equation $X^3 = \mathfrak{p}(T)$, from which we see that the corresponding elliptic curve has j–invariant 0. We have $\beta(k_1) = 1$ and

$$\beta(k_2) = 1 - \begin{bmatrix} 2m/3 \\ m/3 \end{bmatrix} S^{m/3} .$$

One easily shows $\prod_{b \in \mathbb{F}_q} ((T+b)^2-c) = S^2-4c$, provided that c is a non–square in $\mathbb{F}_q$.
Therefore, the elliptic curve

$$T^2 = X^3 + c$$

has p–division points over $\mathbb{F}_q \Leftrightarrow \mathfrak{p}(T) = T^2-c \mid \beta(k_2) \Leftrightarrow 1 = \begin{bmatrix} 2m/3 \\ m/3 \end{bmatrix} (4c)^{m/6}$ in $\mathbb{F}_q$.

6.7. Example: Let $q \equiv 2(3)$ and $n = 3$. L splits at ∞ and is rational. Therefore, the $\beta(k_i)$ have no quadratic prime divisors.

6.8. Example: Let $q \equiv 1(4)$ and $n = 4$. L ramifies at ∞ with index 2, so by Hurwitz is elliptic. Any contribution to $C(k)$ comes from $k = k_3 = 3(q^2-1)/4$,
$\beta(k) = 1 - \begin{bmatrix} 3m/4 \\ m/4 \end{bmatrix} S^{m/2}$.

Let us now consider the "affine" class group $\tilde{C}(k)$ and the divisibility properties of $B(k)$, assuming $\deg \mathfrak{p} = 3$. Recall that if $\tilde{C}(k) \neq 0$, then for all $k' < q^3-1$ that satisfy

$k' \sim k$, $\mathfrak{p}$ divides $B(k')$ and also $\beta(q^3-1-k')$. Here "$\sim$" = "$\sim_{\mathfrak{p}}$" is the equivalence relation (1.9). Cases were $\mathfrak{p} | B(k')$ for all $k' \sim k$ are rare. For $q \leq 32$, they exist for $q = 9, 16, 27$. Also, we found some examples for $q = 43$ and 49. In all these cases, we also found $\mathfrak{p} | \beta(q^3-1-k)$, and in some of them (see (6.10)), we could verify $\tilde{C}(k) \neq 0$. This leads to the following conjecture, that states a converse of Theorem 2.9:

6.9. Conjecture: Let $\mathfrak{p}$ be a prime of A of arbitrary degree d. Suppose that for all $k' \sim k$ (i.e., such that there exists a power p^n of p with $k' \equiv p^n k \ (q^d-1)$), $\mathfrak{p}$ divides (the numerator of) $B(k)$. Then $\tilde{C}(k) \neq 0$.

6.10. Example: Consider the follwing data, where $\mathfrak{p}(T)$ is a divisor of $\mathfrak{p}_1(R)$:

		q	k	$\mathfrak{p}_1(R)$	$\mathfrak{p}(T)$
a)		9	112	$R-1$	T^3-T-1
b)	(ρ a root of X^2+X+1)	16	585	$R-\rho$	$T^3-\rho^2$
c)		49	39216	R^3+4R^2+R+6	T^3-T-2
d)		49	12384	$R-2$	T^3-2
				$R-4$	T^3-3.

Then always $\mathfrak{p}$ divides $B(k')$ for all $k' \sim k$, and, furthermore, all the $\tilde{C}(k)$ are non–zero. In particular, the class numbers of the corresponding rings B_+ are divisible by p.

The facts on divisibility result from explicit calculation. We will prove the non–vanishing of $\tilde{C}(k)$ in case a. Modifications of the argument used work in the other cases b,c,d, but not in the cases mentioned earlier where $q = 27$ and 43.

6.11. Proposition: Let $q = 9$ and $k = 112$. Then $\tilde{C}(k) \neq 0$.

Proof: The equivalence class of 112 is $M = \{112, 280, 336\}$. We have $\mathfrak{p} | B(k')$ and $\mathfrak{p} | \beta(q^3-1-k')$, $k' \in M$, therefore $C(k') \neq 0$. We must show that actually the "affine" part $\tilde{C}(k)$ is non–zero. The characters $\omega^{k'}$, where $k' \in M$, generate a subgroup of order 13 in the character group of $(A/\mathfrak{p})^*$, thus $\bigoplus_{k' \in M} C(k')$ belongs to the subfield $L : K$ of $K_+(\mathfrak{p})$ of degree 13. Let $L_3 = K_{3,+}(\mathfrak{p}_3)$ be the abelian extension of $K_3 = \mathbb{F}_3(T)$ constructed from $\mathfrak{p}_3$. Here, $\mathfrak{p}_3 = \mathfrak{p} \cap K_3$, so L_3 is the maximal abelian extension of K_3 unramified outside of $\mathfrak{p}_3$ and completely split at ∞, which has degree $(3^3-1)/2 = 13$ over K_3. From the ramification conditions, $L = L_3 \cdot K = L_3 \otimes_{\mathbb{F}_3} \mathbb{F}_9$. All the infinite places of L_3 are $\mathbb{F}_3$–rational, hence the canonical map $C_{\infty,L_3} \longrightarrow C_{\infty,L}$ is bijective. The action of $\mathrm{Gal}(K(\mathfrak{p}) : K) = (A/\mathfrak{p})^*$ on $K_3(\mathfrak{p}_3)$ is via the norm $N : (A/\mathfrak{p})^* \longrightarrow (A_3/\mathfrak{p}_3)^* = \mathrm{Gal}(K_3(\mathfrak{p}_3) : K_3)$, thus the component $C_{\infty,L_3}(k_3)$ corresponds to $C_{\infty,L}(k)$, $k = k_3 \cdot n$, where $n = \#(\mathrm{Ker}(N)) = 28$. From the calculation of $\beta_3(k_3)$ (i.e., the B.–G. numbers in the $\mathbb{F}_3$–situation), we see that $C_{L_3}(k_3)$ is non–zero for $k_3 = 2, 6, 18$ only. Hence $C_{\infty,L}(112) = C_{\infty,L_3}(4) = 0$ and $\tilde{C}(112) \xleftarrow{\cong} C(112) \neq 0$.

7. Numerical results

By the computations of Johnson [11] and Wagstaff [14], the numerators of classical Bernoulli numbers B_k seem to be equidistributed mod p , for any prime $p > 2$. In particular, the hypothesis "probability of $p \mid B_k = p^{-1}$" very well "explains" the frequency of irregular primes p and their indices of irregularity for $p < 125\,000$ (see also [13]).

In our situation, the validity of $p \mid \beta(k)$ depends on

a) the equivalence class of k relative to p (see (1.9)), and

b) the orbit of p under the translation group U , or possibly a larger subgroup of V , which depends on k (see (3.3)).

But there are equivalence classes of different lengths, and also U–orbits of different lengths, which complicates the situation. Let p have degree d , and consider indices $0 < k < q^d - 1$. Call the pair (k,p) regular if $p \nmid \beta(k)$, and irregular otherwise. In certain cases, fixing (k,p) , we are given a priori information of whether p divides $\beta(k)$, e.g. (6.1), or (6.2). The general pattern seems to be that, leaving aside the above mentioned pairs (k,p) , irregular pairs are equidistributed among all pairs, where the probability depends on the type a), b) of (k,p) . In the following, we give some heuristic considerations about the expected number of irregular pairs of a given type, based on the equidistribution assumption, and the actual numbers determined by machine calculations.
Instead of the condition $\mathfrak{p}(T) \mid \beta(k)$, we use the equivalent condition $\mathfrak{p}_0(S) \mid \beta(k)$ or even $\mathfrak{p}_1(R) \mid \beta(k)$, whenever $\beta(k)$ is a polynomial in $S = T^q - T$, or $R = S^{q-1}$, and $\mathfrak{p}_1 \mid \mathfrak{p}_0 \mid \mathfrak{p}$ (see section 5). For simplicity, we assume from now on that $q = p > 3$. (For non–prime constant fields $\mathbb{F}_q$, similar, but more complicated arguments apply.)

(7.1) Let $d = \deg \mathfrak{p} = 2$, $k = a+bq < q^2-1$, $0 \leq a,b \leq m = q-1$, $\ell = a+b$. If $\beta(k) \neq 1$, then

(i) $m < \ell < 2m$.

In that case, if $\mathfrak{p}_0(S) = S^2-c$ is a prime, the residue class of $\beta(k)$ mod $\mathfrak{p}$ is some element $\neq 1$ of $\mathbb{F}_q$, if ℓ is even, and non–zero, if ℓ is odd, as we see from (4.9). If $q \equiv 3(4)$, we get precisely $(p-3)/4$ irregular pairs $(k,\mathfrak{p}_0)$ from $\mathfrak{p}_0 = S^2+1$ (see proof of (6.1)). Since there are $m/2$ primes $\mathfrak{p}_0(S) = S^2-c$ and $m^2/4-1$ numbers k that satisfy (i) and

(ii) $\ell \equiv 0(2)$,

we expect

$$\begin{aligned} EV &= m^2/8 - 1/2 && (p \equiv 1(4)) \\ &= m^2/8 - m/4 - 1/2 - 1/m && (p \equiv 3(4)) \end{aligned}$$

irregular pairs $(k,\mathfrak{p}_0)$ with $\mathfrak{p}_0(S) \neq S^2+1$. (The assumption used is that $\beta(k)$ mod $\mathfrak{p}_0$ is equidistributed in $\mathbb{F}_q \setminus \{1\}$ for k that satisfy (i) and (ii).) In the next table, OV is the observed value of irregular pairs as above. We also give the sums of expected and observed values for the first 5, 10, ..., 25 primes $q \geq 5$.

7.2. Table (irregular pairs (k,p_0) , $p_0 \neq S^2+1$, $d = 2$)

q	EV	OV
5	1.50	1
7	2.67	2
11	9.60	10
13	17.50	14
17	31.50	26

N	$\sum$ EV(q)	$\sum$ OV(q) $5 \leq q \leq N$
17	62.77	53
37	516.40	497
59	1920.97	1868
79	4880.51	5013
103	10343.03	10201

(7.3) The number of regular p_0 we expect is $(1-1/m)^e m/2$, if $q \equiv 1(4)$, and $(1-1/m)^e(m/2-1)$, if $q \equiv 3(4)$, where $e = (q^2-9)/8$ is the number of equivalence classes of k with (i) and (ii). The sum of these values for all primes $q \geq 5$ converges to a finite limit ≈ 6.8866 . This raises the question of whether there exist only a finite number of regular quadratic primes $p_0(S) = S^2-c$. Ireland and Small [10] found there exist precisely 5 of them with $q \leq 269$, given in our S–coordinates by S^2-3 $(q = 5)$, S^2-3 $(q = 7)$, S^2-6 $(q = 13)$, S^2-11 , and S^2-24 $(q = 31)$. In [2], some consequences for non–prime q are derived.

(7.4) Next, let $d = \deg \mathfrak{p} = 3$, $k = a + bq + cq^2 < q^3-1$, $0 \leq a,b,c \leq m = q-1$, $\ell = a+b+c$. If $q \equiv 1(3)$, let ρ be a primitive third root of unity in $\mathbb{F}_q$. If $\beta(k) \neq 1$, then

(i) $m < \ell < 3m$.

Among all the k with (i), there are $(5q^3 - 6q^2 - 5q - 6)/6$ that also satisfy

(ii) $\ell \neq 2m$, i.e., $k \equiv 0(m)$,

and $q(q+1)/2$ with $\ell = 2m$.

(7.5) Let us first consider the "minus"–part where $k \equiv 0(m)$. From (4.8), $\beta(k) = 1 + S^i f(S^m) + S^j g(S^m)$ with polynomials f,g and $i \equiv \ell(m)$, $j \equiv 2\ell(m)$. Therefore, if $\mathfrak{p}_0 = S^3-c$ is special (which implies that $3 \mid m$), the values $f(S^m)$ and $g(S^m)$ mod $\mathfrak{p}_0$ lie in $\mathbb{F}_q$, and $\beta(k) \equiv 0$ mod $\mathfrak{p}_0$ is possible for those k only, for which also

(iii) $\ell \equiv 0(3)$

holds. Hence we expect

$$EV_s = \#\{k \mid \text{(i), (ii), (iii) holds}\} \times \#\{\text{special } \mathfrak{p}_0\} \times q^{-1}$$

minus–irregular pairs $(k,\mathfrak{p}_0)$ with $\mathfrak{p}_0$ special, and

$$EV_n = \#\{k \mid \text{(i), (ii) holds}\} \times \#\{\text{non–special } p_0\} \times q^{-3}$$

minus–irregular pairs (k,p_0) with p_0 non–special. This yields

$$EV_s = (10q^3-40q^2-6q+20+16q^{-1})/54 \ , \qquad 0$$
$$EV_n = (5q^2-16q+12+2q^{-1}+7q^{-2}-6q^{-3})/18 \ , \ (5q^2-6q-10+5q^{-2}+6q^{-3})/18$$

in the cases $q \equiv 1(3)$, $q \equiv 2(3)$, respectively.

7.6. Table (minus–irregular pairs (k,p_0) , $d = 3$)

q	EV_s	OV_s	EV_n	OV_n
5			4.75	2
7	26.86	29	8.05	15
11			29.39	31
13	280.62	262	36.05	53
17			74.06	117

(7.7) The number of minus–regular p_0 we would expect from the equidistribution hypothesis is

$$EV_s = \#\{\text{special } p_0\} \times (1-1/q)^{e_s} \qquad (p_0 \text{ special})$$
$$EV_n = \#\{\text{non–special } p_0\} \times (1-1/q)^{e} \qquad (p_0 \text{ non–special}) \ ,$$

where e_s , e is the number of equivalence classes of numbers k that satisfy (i), (ii), (iii)

or (i), (ii), respectively.

7.8. Table (minus–regular primes $\mathfrak{p}_0(S)$, $d = 3$)

q	EV_s	OV_s	EV_n	OV_n
5			6.49	6
7	0.29	0	9.56	6
11			31.21	20
13	3.0×10^{-5}	0	37.30	22
17			74.13	45

The discrepancy between expected and observed values in (7.6) and (7.8) results from the unexpectedly high divisibility by non–special cubic primes $\mathfrak{p}_0(S)$ of those $\beta(k)$ where k has the form $i(q^2 + q + 1)$. For this fact, I presently have no explication. Note that, besides probability arguments, there is no reason for a special prime $\mathfrak{p}_0(S)$ to be minus–irregular. For example, for the non–prime constant field $\mathbb{F}_4$, $\mathfrak{p}_0(S) = S^3 - \rho$ is minus–regular.

(7.9) Let us finally consider the "plus"–part, i.e., $\ell = 2m$ in (7.4). Here, $\beta(k)$ is a polynomial in R . From those k equivalent with $k' = m - c + mq + cq^2$ (their number is $3q-3$), we get precisely $q-1$ plus–irregular pairs $(k,\mathfrak{p}_1)$ with $\mathfrak{p}_1 = R - \rho$ or $R - \rho^2$ special. Hence we expect

$$EV_s = (q(q+1)/2 - 3q + 3) \times 2 \times q^{-1} = q - 5 + 6/q$$

plus–irregular pairs $(k,\mathfrak{p}_1)$ with $k \sim m - c + mq + cq^2$, $\mathfrak{p}_1$ special, and

$$EV_n = q(q+1)/2 \times (q-1)/3 \times q^{-3} = (1-q^{-2})/6 \qquad (q \equiv 1(3))$$
$$= q(q+1)/2 \times (q+1)/3 \times q^{-3} = (1+q^{-1})^2/6 \qquad (q \equiv 2(3))$$

plus–irregular pairs (k,p_1) with p_1 non–special.

7.10. Table (plus–irregular pairs (k,p_1), p_1 special)

$q \equiv 1(3)$	EV_s	OV_s
7	2.86	6
13	8.62	3
19	14.32	18
31	26.19	18
37	32.16	39
43	38.14	36
61	56.10	42
$\sum$	178.38	162

For plus–irregular pairs with p_1 non–special, the expected value is $\approx 1/6$ for each q. The observed values are 0 for the 15 primes q with $5 \leq q \leq 61$, $q \neq 47$, and 3 for $q = 47$.

Note that, in order to perform a χ^2–test on goodness of fit of our data, we had to divide expected and observed values by d to get meaningful results, since for each equivalence class of length d of elements k, there is only one independent event "$p \mid \beta(k)$".

Also, instead of considering primes of fixed degree over varying fields $\mathbb{F}_q$, it is a natural

question to ask for the behavior of primes p of degree $\leq d$, where $d \longrightarrow \infty$, and q is fixed.

References

[1] L. Carlitz: An analogue of the von Staudt–Clausen theorem. Duke Math. J. 3, 503–517, 1937, and 7, 62–67, 1940

[2] K. Feng and W. Gao: Bernoulli–Goss polynomials and class numbers of cyclotomic function fields. To appear (MPI–Preprint Bonn 1988).

[3] S. Galovich and M. Rosen: The class number of cyclotomic function fields. J. Number Theory 13, 363–375, 1981

[4] E.–U. Gekeler: On power sums of polynomials over finite fields. J. Number Theory 30, 11–26, 1988

[5] E.–U. Gekeler: Some new identities for Bernoulli–Carlitz numbers, J. Number Theory, to appear

[6] D. Goss: Von Staudt for $\mathbb{F}_q[T]$. Duke Math. J. 45, 885–910, 1978

[7] D. Goss: The arithmetic of function fields 2: The "cyclotomic" theory. J. Algebra 81, 107–149, 1983

[8] D. Goss: Analogies between global fields. Can. Math. Soc. Conf. Proc. 7, 83–114, 1987

[9] D. Hayes: Explicit class field theory for rational function fields. Trans. AMS 189, 77–91, 1974

[10] K. Ireland and D. Small: A note on Bernoulli–Goss polynomials. Canad. Math. Bull. 27, 179–184, 1984

[11] W. Johnson: Irregular primes and cyclotomic invariants. Math. Comp. 29, 113–120, 1975

[12] S. Okada: Kummer's theory for function fields. Unpublished

[13] C.L. Siegel: Zu zwei Bemerkungen Kummers. Nach. Akad. Wiss. Göttingen 6, 51–57, 1964 (= Ges. Abh. III, 436–442)

[14] S. Wagstaff: The irregular primes to 125000. Math. Comp. 32, 583–591, 1978