INFINITUDE OF WILSON PRIMES FOR $\mathbb{F}_q[t]$

JIM SAUERBERG*, LINGHSUEH SHU, DINESH S. THAKUR** AND GEORGE TODD**

1. Introduction

For a prime p, the well-known Wilson congruence says that $(p-1)! \equiv -1$ modulo p. A prime p is called a Wilson prime, if the congruence above holds modulo p^2. We now quote from [R95, Pa. 346, 350]: 'It is not known whether there are infinitely many Wilson primes. In this respect, Vandiver wrote: This question seems to be of such a character that if I should come to life any time after my death and some mathematician were to tell me it had been definitely settled, I think I would immediately drop dead again.' He also mentions that search (by Crandall, Dilcher, Pomerance [CDP]) up to 5×10^8 produced the only known Wilson primes, namely 5, 13, and 563, which was discovered by Goldberg in 1953 (one of the first successful computer searches involving very large numbers). (See [R95, Dic19] for historical references.)

Many strong analogies [Gos96, Ro02, Tha04] between number fields and function fields over finite fields have been used to benefit the study of both. These analogies are even stronger in the base case $\mathbb{Q}, \mathbb{Z} \leftrightarrow F(t), F[t]$, where F is a finite field. We will study the concept of Wilson prime in this function field context, and in contrast to the $\mathbb{Z}$ case, we will exhibit infinitely many of them, at least for many F. For example, $\wp = t^{3*13^n} - t^{13^n} - 1$ are Wilson primes for $\mathbb{F}_3[t]$.

We also show strong connections between Wilson's and Fermat's quotients; between refined Wilson residues and discriminants, and introduce analogs of Bell numbers in $F[t]$ setting.

2. Wilson primes

Let us fix some basic notation. We use the standard conventions that empty sums are zero and the empty products are one.

q	a power of a prime p
A	$= \mathbb{F}_q[t]$
A_d	$= \{$elements of A of degree $d\}$
$[n]$	$= t^{q^n} - t$
D_n	$= \prod_{i=0}^{n-1} (t^{q^n} - t^{q^i}) = \prod [n-i]^{q^i}$
L_n	$= \prod_{i=1}^{n} (t^{q^i} - t) = \prod [i]$
F_i	the product of all (non-zero) elements of A of degree less than i
$\mathcal{N}a$	$= q^d$ for $a \in A_d$, i.e., the norm of a
$\wp$	a monic irreducible polynomial in A of degree d
a_s	defined by $a_s(t) = a(t^s)$, for $a \in A$ and positive integer s

1991 *Mathematics Subject Classification.* 11A41, 11T55, 11N05.

Key words and phrases. Carlitz factorial, Fermat quotient, Wilson quotient, Lerch formula, Bell number, Discriminant, Primitive polynomial.

If we interpret the factorial of $n-1$ as the product of non-zero 'remainders' when you divide by n, we get F_i as a naive analog of factorial of $a \in A_i$. Note that it just depends on the degree of a. By the usual group theory argument with pairing of elements with their inverses, we get an analog of Wilson's theorem that $F_d \equiv -1 \bmod \wp$, for $\wp$ a prime of degree d. Though not strictly necessary for this paper, we now introduce more refined notion of factorial due to Carlitz. For $n \in \mathbb{Z}$, $n \geq 0$, we define its factorial by

$$n! := \prod D_i^{n_i} \in A, \quad \text{for } n = \sum n_i q^i, \quad 0 \leq n_i < q.$$

See [Tha04, 4.5-4.8, 4.12, 4.13] and [Tha12] for its properties, such as prime factorization, divisibilities, functional equations, interpolations and arithmetic of special values, congruences, which are analogous to those of the classical factorial. See also [Bha00], which gives many interesting divisibility properties in great generality.

Carlitz proved D_n is the product of monics of degree n. This gives the connection between the two notions above, that for $a \in A_i$, $(\mathcal{N}a-1)! = (-1)^i F_i$. (See [Tha12, Thm. 4.1, Sec. 6] for more on these analogies and some refinements of analogs of Wilson's theorem). This also implies

$$F_d = (-1)^d \prod_{j=1}^{d-1} [d-j]^{q^j-1} = (-1)^d D_d/L_d. \tag{1}$$

So let us restate the above well-known analog of Wilson's theorem.

Theorem 2.1. *If $\wp$ is a prime of A of degree d, then*

$$(-1)^d(\mathcal{N}\wp - 1)! = F_d \equiv -1 \bmod \wp.$$

This naturally leads to

Definition 2.2. A prime $\wp \in A_d$ is a Wilson prime, if $F_d \equiv -1 \bmod \wp^2$.

Remarks 2.3. (1) If $d = 1$, then $F_d = -1$. So the primes of degree one are Wilson primes.

(2) If $\wp(t)$ is Wilson prime, then so are $\wp(t+\theta)$ and $\wp(\mu t)$, for $\theta \in \mathbb{F}_q$ and $\mu \in \mathbb{F}_q^*$, as follows immediately from the formula for F_d.

(3) By [Tha12, Thm. 7.1], $\wp = t^p - t - a$ is Wilson prime, if $q = p > 2$ and $a \in \mathbb{F}_q^*$, with the congruence above holding modulo $\wp^{q-1}$, but not modulo $\wp^q$. (The last clause, though not mentioned in the statement of the Theorem referred, follows immediately from the exactness of the power mentioned in the proof.)

Next we introduce the Fermat quotient.

Definition 2.4. For $\wp$ as above, and $a \in A$, let $Q_\wp(a) := (a^{q^d} - a)/\wp$.

Remarks 2.5. By the Fermat-Lagrange theorem, for $a \in A$, $Q_\wp(a) \in A$. We collect some useful facts immediate from the definition.

(1) If $a \equiv a' \bmod \wp^k$, then $Q_\wp(a) \equiv Q_\wp(a') \bmod \wp^{k-1}$.

(2) For $a, b \in A$ and $c \in \mathbb{F}_q$, modulo $\wp$ we have

$$Q_\wp(a + b\wp) \equiv Q_\wp(a) - b, \quad Q_\wp(ca) = cQ_\wp(a), \quad Q_\wp(ab) \equiv aQ_\wp(b) + bQ_\wp(a).$$

(3) From the definition of $[n]$ above, the following are also clear.

$$[m+n] = [m]^{q^n} + [n], \quad [m-n]^{q^{m+n}} = [m]^{q^m} - [m]^{q^n} + [m] - [n].$$

We now give a useful equivalent formulation for a Wilson prime.

Theorem 2.6. *Assume $q > 2$ or $d > 1$. Then a prime $\wp$ is a Wilson prime if and only if $Q_\wp(Q_\wp(t)) \equiv 0 \bmod \wp$.*

Proof. Since $Q_\wp(t) = [d]/\wp$, we have

$$Q_\wp(Q_\wp(t)) = (([d]/\wp)^{q^d} - [d]/\wp)/\wp \equiv 0 \bmod \wp \iff ([d]/\wp)^{q^d} \equiv [d]/\wp \bmod \wp^2.$$

The product F_{2d} can be decomposed as the product over multiples of $\wp$, which contributes $F_d\wp^{q^d-1}$, times the product over polynomials prime to $\wp$, which contributes -1 modulo $\wp^2$, by again pairing off elements in $(A/\wp^2A)^*$ with their inverses and working out order two elements in this group and using that we are not in case $q = 2, d = 1$. (See e.g., [Tha04, pa. 7]). Thus,

$$\frac{F_{2d}}{\wp^{q^d-1}F_d} \equiv -1 \bmod \wp^2.$$

By manipulations using (1), the Remarks 2.5, and the fact from the basic theory of finite fields that $[d]$ is the product of monic irreducibles in A of degree dividing d, so that $\wp^2$ divides $[d]^{q^{d-j}}$, we see that modulo $\wp^2$,

$$\begin{aligned}
-1 &\equiv \frac{(-1)^{2d}[d]^{q^d-1}}{(-1)^d\wp^{q^d-1}} \prod_{1\le j<d} \frac{\left([d]^{q^{d-j}} + [d-j]\right)^{q^j-1}[d-j]^{q^{d+j}-1}}{[d-j]^{q^j-1}} \\
&\equiv (-1)^d Q_\wp(t)^{q^d-1} \prod_{1\le j<d} [d-j]^{q^{d+j-1}} \\
&\equiv (-1)^d Q_\wp(t)^{q^d-1} \prod_{1\le j<d} \frac{[d]^{q^d} - [d]^{q^j} + [d] - [j]}{[d-j]} \\
&\equiv (-1)^d Q_\wp(t)^{q^d-1} \prod_{1\le j<d} [d-j]^{q^j-1} \\
&\equiv Q_\wp(t)^{q^d-1}F_d.
\end{aligned}$$

Thus we have

$$Q_\wp(t)^{q^d-1}(1 + F_d) \equiv Q_\wp(t)^{q^d-1} - 1 \bmod \wp^2.$$

Hence, $\wp$ is a Wilson Prime, i.e., $F_d \equiv -1 \bmod \wp^2$ if and only if $Q_\wp(t)^{q^d-1} - 1 \equiv 0 \bmod \wp^2$, proving the theorem, because $Q_\wp(t)$ is non-zero modulo $\wp$. □

Definition 2.7. If t does not divide $a \in A$, the order of a is defined to be the order of t modulo a, i.e., it is the smallest positive integer e such that a divides $t^e - 1$.

We refer to [LN97, Cha.3] for many results concerning this, but we will only need the following special case of [LN97, Thm. 3.35].

Theorem 2.8. *Let a be a monic prime of A of degree m and order e, and let s be a positive integer whose prime factors divide e, but not $(q^m - 1)/e$. Assume also that $q^m \equiv 1 \bmod 4$, if $s \equiv 0 \bmod 4$. Then a_s is a monic prime of degree ms and order es.*

Next, we show how to construct new Wilson primes from a given one, if certain conditions hold.

Theorem 2.9. *Let $\wp$ be a Wilson prime of degree $d > 1$. Let e be the order of $\wp$. Let s be a positive integer whose prime factors divide e but not divide $(q^d-1)/e$ and $s \equiv 1 \bmod p$. Assume also that $q^d \equiv 1 \bmod 4$, if $s \equiv 0 \mod 4$. Then $\wp_s(t) = \wp(t^s)$ is a Wilson prime.*

Proof. Since $Q_\wp(t) \in A$ and t is prime to $\wp$, for some $f, g \in A$,

$$\frac{t^{q^d-1}-1}{\wp} \equiv f + g\wp (\mathrm{mod}\, \wp^2), \quad \frac{t^{s(q^d-1)}-1}{\wp_s} \equiv f_s + g_s\wp_s (\mathrm{mod}\, \wp_s^2). \tag{2}$$

By Theorem 2.6, $\wp$ is a Wilson prime, if and only if, modulo $\wp$ we've

$$0 \equiv Q_\wp(tf+tg\wp) \equiv Q_\wp(tf)-tg \equiv tQ_\wp(f)+fQ_\wp(t)-tg \equiv tQ_\wp(f)+tf^2-tg \equiv Q_\wp(f)+f^2-g.$$

By Theorem 2.8, $\wp_s$ is irreducible with degree ds and order es, so that by Fermat-Lagrange theorem es divides $q^{ds}-1 = (q^d-1)N$, say. Since s and $(q^d-1)/e$ are relatively prime, s divides N, so that $q^{ds}-1 = sr(q^d-1)$ for some $r \in \mathbb{Z}$. This implies $r \equiv 1 \bmod p$.

Now, by the binomial theorem, we have modulo $\wp_s^2$

$$Q_{\wp_s}(t) = t\left(\frac{\left(\left((t^s)^{q^d-1}-1\right)+1\right)^r-1}{\wp_s}\right) \equiv t\left(\frac{r\left((t^s)^{q^d-1}-1\right)}{\wp_s}\right) \equiv t(f_s+g_s\wp_s),$$

since in characteristic p, $r = 1$, the second term in the binomial expansion is zero as 'r choose 2' is zero, and the higher terms are zero modulo $\wp_s^2$.

This implies, using (2) and Remarks 2.5, that modulo $\wp_s$ we have

$$\begin{aligned} Q_{\wp_s}(Q_{\wp_s}(t)) &\equiv Q_{\wp_s}(tf_s + tg_s\wp_s) && \equiv Q_{\wp_s}(tf_s) - tg_s \\ &\equiv tQ_{\wp_s}(f_s) - tg_s + f_sQ_{\wp_s}(t) && \equiv -tf_s^2 + f_sQ_{\wp_s}(t) \\ &\equiv f_s(-tf_s + Q_{\wp_s}(t)) && \equiv 0. \end{aligned}$$

This implies that $\wp_s$ is a Wilson prime as claimed. □

Note that if we can choose $s > 1$ in this theorem, we get a new Wilson prime. We now show that we can often successively do that to get infinitely many Wilson primes.

It has been conjectured/speculated that when $q = p$ a prime, the order of the prime $t^p - t - 1$ of A is $w := w_p := (p^p-1)/(p-1)$. (Note that the order divides w because, it is the order in $\mathbb{F}_{p^p}$ of the root x which is of norm 1, i.e., killed by the w-th power.) It has been verified [MNW10] only for small primes, e.g., $p < 127$. For several references and heuristic reasons, see [MNW10, LD62]. This question has interesting connections [LN97, Thm. 3.84] with question of existence of primitive polynomials of Artin-Schreier type, and with period modulo p (this connection is through a recursion mod p due to Touchard, see [LD62, (1.7)]) of the sequence of the Bell numbers which show up in many combinatorial questions. The reader can check small cases easily, e.g., for $p = 3$ or 5 the order is $w = 13$ or 781 respectively.

Theorem 2.10. *Let $q = p$ be an odd prime, such that prime $\wp := t^p - t - 1$ of A has order $w := (p^p-1)/(p-1)$, (e.g., p any odd prime < 127). Then $P_n(t) := \wp_{w^n} = t^{pw^n} - t^{w^n} - 1$ are Wilson primes for A, for any non-negative integer n.*

Proof. Consider the induction hypothesis that P_n is a Wilson prime of degree pw^n and order w^{n+1}. For $n = 0$, this follows from Remark 2.3 and the hypothesis. We will use induction and Theorem 2.9, with $s = w$. Note $w \equiv 1 \bmod p$. Also, $w \equiv 0 \bmod 4$, if $p^p \equiv 1 \bmod 4$. Now $w = 1 + p + p^2 + \cdots + p^{p-1} \equiv 1 + \cdots + 1 = p \equiv 1 \bmod (p-1)$ implying that the greatest common divisor of w and $p-1$ is one. Thus $s = w$ satisfies the hypothesis and $n = 1$ case follows. More generally, we claim that $s = w$ satisfies the hypothesis of Theorem 2.9 to deduce it for n replaced by $n+1$ by Theorems 2.8, 2.9.

We have already noted that $w \equiv 1 \bmod p$. We have $p^{pw^n} \equiv 1 \bmod 4$, if $w \equiv 0 \bmod 4$. It is thus sufficient to prove that the greatest common divisor of w and $(p^{pw^n} - 1)/w^{n+1}$ is one. This follows from the claim that $p^{pw^n} = 1 + rw^{n+1} + m_n w^{n+2}$, for some r relatively prime to w and some integer m_n.

This follows by induction on n as follows. For $n = 0$, we have checked this above. Write the right side as $1+y$, say, so that w^{n+1} divides y. By the binomial theorem, $p^{pw^{n+1}} = (1 + y)^w = 1 + yw + y^2 w(w-1)/2+$ terms divisible by y^3. Since w is prime to $p-1$, it is odd and thus modulo w^{n+3}, the left side is $1+yw \equiv 1+rw^{n+2}$, proving the claim and the Theorem. □

Remarks 2.11. (1) In view of the fact that only 3 Wilson primes are known in $\mathbb{Z}$ case, it may be worth pointing out that, at least in the sequences we construct, the size of n-th Wilson prime grows roughly as a double exponential in n, with the base growing with p (and the size grows faster than a double exponential in p). In the $\mathbb{Z}$ case, the simple heuristic that random number divisible by p is divisible by p^2 with probability $1/p$, also gives about $\log\log(x)$ primes up to x. For more discussion and consequences for search in $\mathbb{Z}$ case, see [CDP].

(2) It is quite possible that there are infinitely many Wilson primes for each A, even constructible in a similar way, without needing any conjectures, by appropriate choices of s dividing w and starting with appropriate Wilson primes for A. We have not investigated this.

3. Complements

Probably, the first connection noticed between the Fermat quotients and Wilson's congruence is Lerch's 1905 famous congruence formula $\sum(a^{p-1}-1)/p \equiv ((p-1)!+1)/p \bmod p$, for any odd prime p, where the sum is over $0 < a < p$. The proof [Sp11], through immediate application of easily checked logarithmic relation $Q_\wp(a)/a + Q_\wp(b)/b \equiv Q_\wp(ab)/(ab) \bmod p$ due to Eisenstein, and Wilson, Fermat congruences carries over immediately to the proof of analogous function field formula obtained by replacing p by $\wp$ or $\mathcal{N}\wp$ appropriately, and by replacing $(p-1)!$ by F_d. We leave it to the reader and point out that in the function field case, in fact, the congruence improves to equality!

Theorem 3.1. *Let $a \in A$ run through all non-zero elements of degree $< d$ (standard reduced congruence class representatives modulo $\wp$). Then*

$$\sum(a^{\mathcal{N}\wp-1} - 1) = F_d + 1 = (-1)^d(\mathcal{N}\wp - 1)! + 1.$$

In particular, the sum of Fermat quotients (rather $Q_\wp(a)/a$'s in our notation, which are appropriate for reduced system) is the Wilson quotient $(F_d + 1)/\wp$ in our notation.

Proof. Once observed, the proof is an exercise in combining several results of Carlitz: By [Tha04, Cor. 5.6.4], the left side evaluates to $-\sum(-1)^i D_d/(L_i D_{d-i}^{q^i}) - (q^d-1)$. We have seen that the right side evaluates to $(-1)^d D_d/L_d + 1$. Now [Tha04, 2.5] the Carlitz exponential $\sum z^{q^i}/D_i$ has inverse function $\sum z^{q^i}(-1)^i/L_i$. Hence the coefficient of z^{q^d} of the composition is zero. This exactly translates to the two evaluations above being the same. □

Remarks 3.2. We mention the congruence connection between the Wilson quotient and Bernoulli numbers due to Glaisher [Sp11] that $((p-1)!+1)/p \equiv B_{p-1} + 1/p - 1 \bmod p$, and record an analog

$$\frac{F_d+1}{\wp} = \frac{(-1)^d(\mathcal{N}\wp-1)!+1}{\wp} \equiv (-1)^d B_{\mathcal{N}\wp-1} + \frac{1}{\wp} \bmod \wp^{q-1},$$

(if $d>1$ and modulo $\wp^{q-2}$ if $d=1$), which follows from [Tha04, 4.16.1] and [Tha12, Remark 7.8 (ii)]. The Glaisher congruence above works modulo higher power, if the Lerch's formula works modulo higher power of that prime, which it always does in our case, 'explaining' our higher power congruence!

See [SS97] for much more on the notion of Fermat quotient in the function field setting, e.g., for the theorem that for a non-constant a of degree less than d, the valuation at $\wp$ of $Q_\wp(a)$ is p^e-1, where e is the largest integer such that a is a p^e-th power in A. In particular, for a given non-constant a, there are infinitely many $\wp$ (analogs of 'Wieferich primes for a') such that $\wp$ divides $Q_\wp(a)$ if and only if a is a p-th power (if part being immediate from just the definitions).

Finally, we mention another trick to produce more Wilson primes in some situations. Given $a \in A_d$, with $a(0) \neq 0$, $a^*(t) := t^d a(1/t) \in A_d$ is reciprocal polynomial, and we have $(a^*)^* = a$ and $(ab)^* = a^*b^*$ for a, b with $a(0)b(0) \neq 0$. Thus $\wp$ (not equal to t) is a prime if and only if $\wp^*$ is. (We can also modify by correcting degree, if $a(0)=0$).

Theorem 3.3. *Let $d>1$. If $\wp$ is a Wilson prime, then the reciprocal polynomial $\wp^*$ is also a Wilson prime, if and only if $d \equiv 1 \bmod p$.*

Proof. Let $\wp$ be a Wilson prime, so that $([d]/\wp)^{q^d} \equiv [d]/\wp \bmod \wp^2$. Replacing t by $1/t$ and multiplying by appropriate powers of t, modulo $(\wp^*)^2$ (from now on in this proof) we have, $([d]/\wp^*)^{q^d} \equiv t^{(q^d-d+1)(q^d-1)}[d]/\wp^*$. Hence $\wp^*$ is a Wilson prime if and only if $t^{(q^d-d+1)(q^d-1)} \equiv 1$. Now $t^{q^d-1}-1 = r\wp$ for some r non-zero modulo $\wp$ and thus $t^{q^d-1} = 1 + s\wp^*$, for some s prime to $\wp^*$, by taking reciprocals. Thus, the power of t above is $\equiv (1+s\wp^*)^{q^d-d+1} \equiv 1 + (-d+1)s\wp^*$. □

4. Complements: Analog of Bell numbers

We consider a 'Carlitzian' analog of Bell numbers [Be38], which were mentioned above and study their periodicity modulo primes in the A-case.

We basically replace the usual exponential and factorials in the original definition by Carlitz exponential and Carlitz factorial and shift by 1 to adjust for additive rather than multiplicative group involved. Bell used any number of iterated exponentials, which we can also do, but here we will restrict to only two iterations, which lead to the numbers mentioned above.

In other words, let $e(z) = \sum z^{q^i}/D_i$ be the Carlitz factorial, then define analog $B_{[n]}$ of Bell numbers (polynomials in A now) by $e(e(z)) = \sum B_{[n]} z^{q^n}/D_n$.

Directly from the definitions, we have

$$B_{[n]} = \sum \frac{D_n}{D_i D_{n-i}^{q^i}} = 2 + \sum_{j=0}^{n-2} \frac{[n]\cdots[n-j]^{q^j}}{[j+1]\cdots[1]^{q^j}}.$$

The interpretation of $[n]$ as the product of monic irreducible polynomials of degrees dividing n immediately shows that $B_{[n]} \in A$.

Theorem 4.1. *We have $B_{[n+d]} \equiv B_{[n]} + 1 \bmod \wp$, so that the sequence $B_{[n]} \bmod \wp$ is periodic with period dp.*

Proof. In this proof, the congruences are modulo $\wp$. Since $\wp^{q^r}$ is the exact power of $\wp$ dividing $[r+d]-[r]$, we have $[r+d] \equiv [r]$ and for r divisible by d, we have $[r+d]/\wp \equiv [r]/\wp \not\equiv 0$, so that $[r+d]/[r] \equiv 1$ in that case. This implies by using the expression above for $B_{[n]}$'s that

$$B_{[n+d]} = 2 + \sum_{j=0}^{n-2} + \frac{[n+d]\cdots[d+1]^{q^{n-1}}}{[n]\cdots[1]^{q^{n-1}}} + \sum_{j=n}^{n+d-2} \equiv B_{[n]} + 1 + \sum 0.$$

□

It would be interesting to settle whether dp is the minimal period, and to understand combinatorial interpretation of these analogs.

5. Complements: Refined Wilson theorem and Discriminants

By [Tha12, Thm. 4.1], $M := ((\mathcal{N}\wp - 1)/(q-1))!$ modulo $\wp$ is a $q-1$-th root of $(-1)^{d-1}$. The question on its distribution, as $\wp$ varies, was raised [Tha12] with some partial results given. We want to point out that the root depends on the discriminant of $\wp$ as a polynomial. This follows from the explicit formula and the observation that modulo $\wp$, t is a root of the polynomial $\wp(t)$, and other roots are t^{q^i}, so that $M = D_{d-1}\cdots D_0 = \prod(t^{q^i} - t^{q^j})$, where the product is over $d > i > j \geq 0$, is congruent modulo $\wp$ to a square root of the discriminant. In other words, modulo $\wp$, M^2 is congruent to the discriminant of $\wp$ and the question of distribution of this factorial gets transformed into distribution of discriminants. An easy implication of [Tha12, Thm. 4.1] is that when q is odd, for an irreducible $\wp$, its discriminant is a square if and only if its degree is odd. (Fact already noticed in [Dic06]).

We proved some facts (for more information and data on many of these topics, see [To12]) on the distribution of discriminant/refined Wilson residue, but in correspondence with the third author, Elkies and Bhargava have announced a nice complete answer for $d = 3, 4, 5$.

Acknowledgment The third author's work was supported in part by NSA grant H98230-10-1-0200.

References

[Be38] E. T. Bell. *The iterated exponential integers*, Ann. of Math. 39 (1938), 539-557. 4

[Bha00] Manjul Bhargava. *The factorial function and generalizations*, Amer. Math. Monthly, 107(9):783-799 (2000). 2

[CDP] Richard Crandall, Karl Dilcher, and Carl Pomerance. *A search for Wieferich and Wilson Primes*. Math. Comp. 66 no. 217 (1997), 433-449. 1, 2.11

[Dic06] Leonard Dickson. *Criterion for the irreducibility of functions in a finite field.* Bul Amer Math Soc (1906), Oct. issue 1-8. 5

[Dic19] Leonard Dickson. *History of the Theory of Numbers*, (1919), Dover edition 2005, Volume I, Chapter 9. 1

[Gos96] David Goss. *Basic structures of function field arithmetic*, volume 35 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1996. 1

[LD62] J. Levine and R. E. Dalton. *Minimum periods modulo p of first order Bell exponential integers*. Math. Comp. 16 (1962) 416-423. 2

[LN97] Rudolf Lidl and Harold Niederreiter. *Finite Fields* Encyclopedia of mathematics and its applications, Vol. 20. Cambridge University Press, Cambridge, Second Edition 1997. 2, 2

[MNW10] P. L. Montgomery, S. Nahm, and S. S. Wagstaff. *The period of the Bell numbers modulo a prime*. Math. Comp. 79 (2010) 1793-1800. 2

[R95] Paulo Ribenboim. *The new book of prime number records* 3rd Edition, Springer-Verlag, New York 1995. 1

[Ro02] Michael Rosen. *Number theory in function fields* Springer-Verlag, New York 2002. 1

[Sp11] Jonathan Sondow. *Lerch quotients, Lerch primes, Fermat-Wilson quotients and Wieferich-non-Wilson primes 2, 3, 14771*. arXiv 1110.3113v2.pdf [Math NT] 17 Oct 2011. 3, 3.2

[SS97] Jim Sauerberg and Linghsueh Shu. *Fermat quotients over function fields*. Finite fields and their applications 3, 275-286 (1997). 3

[Tha04] Dinesh S. Thakur. *Function field arithmetic*. World Scientific Publishing Co. Inc., River Edge, NJ, 2004. 1, 2, 2, 3, 3.2

[Tha12] Dinesh S. Thakur. *Binomial and Factorial Congruences for* $\mathbb{F}_q[t]$. Finite fields and their applications, 18 (2012), 271-282. 2, 2.3, 3.2, 5

[To12] George Todd. *Congruences for* $\mathbb{F}_q[t]$. Masters thesis, University of Arizona, (In progress) 2012. 5

*Department of Math, Saint Mary's College of California, Moranga, CA 94575,
**Department of Math, University of Arizona, Tucson, AZ 85721, USA
E-mail address: jsauerbe@stmarys-ca.edu, thakur@math.arizona.edu, gtodd@math.arizona.edu