FERMAT VERSUS WILSON CONGRUENCES, ARITHMETIC DERIVATIVES AND ZETA VALUES

DINESH S. THAKUR

Dedicated to M. Ram Murty on his 60th birthday

Abstract. We look at two analogs each for the well-known congruences of Fermat and Wilson in the case of polynomials over finite fields. When we look at them modulo higher powers of primes, we find interesting relations linking them together, as well as linking them with derivatives and zeta values. The link with the zeta value carries over to the number field case, with the zeta value at 1 being replaced by Euler's constant.

1. Introduction

Since the finite fields occur as the residue fields of global fields (i.e., the number fields and function fields over finite fields), the fundamental and often used properties of $\mathbb{F}_q$ that $x^q = x$, for $x \in \mathbb{F}_q$ and that the product of all non-zero elements of $\mathbb{F}_q$ is -1, lift to the well-known generalizations of the elementary, but fundamental Fermat and Wilson congruences. In fact, the fundamental fact that the defining polynomial of $\mathbb{F}_q$ is $x^q - x$ implies both the congruences through its zeros and through the sign of its linear term.

The Fermat congruence says that for $a \in \mathbb{Z}$ prime to p, we have $a^{p-1} \equiv 1 \mod p$ (or $a^p \equiv a \mod p$ for any integer a), and the Wilson congruence says that $(p-1)! \equiv -1 \mod p$.

In this paper, we will describe two different analogs (multiplicative/arithmetic versus additive/geometric: this terminology is explained more in the last section) of these two congruences in the case of polynomials over finite fields. When we look at them modulo higher powers of primes, we discover new interesting relations linking the two congruences together in each of the analogs, as well as linking them with derivatives and arithmetic derivatives for the first analog and with the zeta values for the second analog. We will show that the link with the zeta value carries over to the number field case, with the zeta value at 1 being replaced by Euler's constant.

The results about the second analog and the number field case (Section 2.2 and section 3) are new, whereas the exposition in Section 2.1 describes recent results [Tha13] omitting the proofs, and the exposition in Section 4 describes the analogies further. Our goal in this exposition is to describe multiple analogies between integers and polynomials over finite fields and to explain quickly how simple questions about these basic structures of finite field and congruence theory lead to diverse objects such as arithmetic derivatives, zeta values and Euler constants, higher tensor powers of Carlitz-Drinfeld modules, Iwasawa invariants, higher cyclotomic units and

Supported in part by NSA grant H98230-13-1-0244 and H98230-14-1-0162.

randomness questions in arithmetic statistics. A several interesting open questions are also mentioned on the way.

Before we deal with polynomials over finite fields, let us briefly recall some basic motivating facts, terminology and history for these congruences for integers.

It is interesting to note that, while the Wilson congruence holding for an integer $p > 1$ implies that p is a prime, this is never used in practice as a primality test. On the other hand, even if the Fermat congruence holds for an integer p and for all the a's prime to it, this does not imply that p is a prime. It can be a Carmichael number such as 561, and there are infinitely many of them. Even with the Elliptic curves primality tests there are infinitely many composite numbers [EPT12] passing them under the standard conjectures. On the other hand, the Fermat congruence test, even with a single a such as 2, is used, not only to disqualify p as a prime, but also to pass it as a probable prime. This is because $a^{p-1} \mod p$ can be computed only in less than $c \log p$ steps and that probability that a random large composite p passes the test is close to zero.

If we consider a^{p-1} or $(p-1)!$ as actual integers rather than congruence classes, we can ask whether the congruences hold modulo higher powers of p.

Here is some sample history [Dic19, Rib95, Gra97]: A prime p is called a Wieferich prime (or a Wieferich prime for $a = 2$), if $2^{p-1} \equiv 1 \mod p^2$. Wieferich showed that if p is not a Wieferich prime, then the first case of Fermat's last theorem for the exponent p follows easily. Only two Wieferich primes are known: 1093 and 3511. (This criterion was later extended by many to have similar result with 2 replaced by any prime $a \leq 109$.)

A prime p is called a Wilson prime, if $(p-1)! \equiv -1 \mod p^2$. Even after extensive search, only three such are known: 5, 13, and 563.

About the question of infinitude of Wilson primes, there is famous quote of Vandiver: 'This question seems to be of such a character that if I should come to life after my death and some mathematician were to tell me it had been definitely settled, I would immediately drop dead again.'

What do we expect about whether there are infinitely many Wieferich, Wilson primes? Since we do not know any structural restrictions, some choose to extrapolate the random model [Was82, Sec. 5.3], introduced by Siegel to predict (successfully, at least numerically up till now) specific positive density of irregular primes, to predict very thin zero density set of about $\sum_{p \leq x} 1/p \sim \log \log x$ such primes up to x. With the analogies between Fermat quotients and derivatives, differential forms, explored by Ihara, Buium [Iha92, Bui05] etc., some expect only finitely many exceptions. For Vandiver primes, i.e., primes p dividing the class number of $Q(\cos(2\pi/p))$, where the random model predicts the same asymptotics, because of the nice known consequences [Was82] of the assumption of their non-existence, some hope that there are none!

Lerch connected these two questions via the congruence

$$\sum \frac{a^{p-1} - 1}{p} \equiv \frac{(p-1)! + 1}{p} \mod p,$$

which follows easily by Eisenstein's observation that modulo p the quantity being summed on left satisfies logarithmic relation, thus the sum over a turns into factorial product giving the desired congruence via Wilson's theorem and the binomial expansion.

2. Function Field situation

We now explore these questions in the situation with $\mathbb{Z}$ replaced by $A := \mathbb{F}_q[t]$. We will see two analogs, with proof of infinitude, and in fact, a full characterization, for the first. We will see tighter connections between these questions, as well as connections with zeta values, arithmetic derivatives and discriminants. We will see a strong actual connection (rather than analogy mentioned above for integers) with derivatives. For the first analog, this connection allows us to show infinitude of Wilson primes for any A. Our main new results in this section are in 2.2.

Let $\mathbb{F}_q$ be a finite field of q elements, and of characteristic p. Let $\wp$ be a prime (i.e., an irreducible polynomial) in A, which we assume to be a monic polynomial of degree d in t.

2.1. **First analog.** Recall the usual norm $\mathcal{N}\wp = q^d$, which is the number of remainders or residue classes modulo $\wp$. By the usual group-theoretic method of proof, now applied to $(A/\wp A)^*$ in place of $(\mathbb{Z}/p\mathbb{Z})^*$, we see that for $a \in A$ not divisible by $\wp$, we have

$$a^{\mathcal{N}\wp - 1} \equiv 1 \mod \wp, \quad F_d \equiv -1 \mod \wp,$$

where F_d is the product of all non-zero polynomials of degree less than d (note that these form the standard representatives of non-zero remainders modulo $\wp$).

2.1.1. *Remarks.* In fact, $F_d = (-1)^d(\mathcal{N}\wp - 1)!_c$, where $!_c$ is the Carlitz factorial. See [Tha04, 4.5-4.8, 4.12, 4.13] and [Bha00, Gos96] for its definition, properties, such as prime factorization, divisibilities, functional equations, interpolations and arithmetic of special values, which are analogous to those of the classical factorial.

2.1.2. *Definition.* We call a prime $\wp$ an m-Wieferich prime for a, if $\wp^2$ divides $a^{\mathcal{N}\wp - 1} - 1$. We call a prime $\wp$ a $!_c$-Wilson prime, if $F_d \equiv -1 \mod \wp^2$.

2.1.3. *Remarks.* The basic theory of finite fields shows that $[d] := t^{q^d} - t$ is the product of monic irreducible polynomials of degree d, so that $\wp$ is never m-Wieferich for t. On the other hand, if a is p-th power in A, taking p-th powers of Fermat congruence for its p-th root, we see that every $\wp$ is m-Wieferich for a.

Theorem 1. *For $a \in A$, there are infinitely many m-Wieferich primes for a, if and only if a is a p-th power, if and only if $da/dt = 0$.*

Proof. (See [SS97, Cor. 2.4] and [Tha13, Thm. 2.6]). The last equivalence is clear and the 'if' direction of the first is already noted above. If $a = \sum a_i t^i$, we have, modulo $\wp^2$, (without loss of generality $\wp \neq t$) that

$$a^{q^d} - a \equiv \sum a_i t^i ((t^{q^d - 1} - 1 + 1)^i - 1) \equiv \sum a_i t^i \binom{i}{1} ([d]/t)^1 \equiv (da/dt)[d],$$

which is non-zero, if a is not a p-th power and $d > \deg a$. □

2.1.4. *Remarks.* If an integer a prime to p is b^p modulo p^2, then $a^{p-1} \equiv b^{p(p-1)} \equiv 1$ modulo p^2 and thus p is a Wieferich prime for a. If p is odd, conversely, if p is a Wieferich prime for a, writing $a = g^k$, for g a primitive root modulo p^2 (i.e., a generator of the cyclic group $(\mathbb{Z}/p^2\mathbb{Z})^*$), we see $1 \equiv a^{p-1} \equiv g^{k(p-1)}$, so that k is a multiple of p, and thus a is p-th power modulo p^2. By generalized Hensel's lemma application, we see, in fact, that a is p -th power of a p-adic integer. (In more detail, the usual version of Hensel needs p-th power modulo p^3 to be able to lift

p-adically, but if $a \equiv b^p$ modulo p^2, then $a = b^p + kp^2 \equiv (b+kp)^p$ modulo p^3 takes care of that). In our characteristic p case, $(A/\wp^2 A)^*$ is not necessarily cyclic, and the derivative of $x^p - a$ is identically zero, so that this argument fails. On the other hand, by additivity of the p-th power map in characteristic p, if $a \in A$ is a p-th power of a power series in t, then it is clearly p-th power of a polynomial, and this works modulo $\wp$ also, if a has degree less than d.

We now show that the derivative interpretation is fruitful also for $!_c$-Wilson question. For this, we introduce some differential, difference and arithmetic differential operators.

2.1.5. *Definition.* (1) For $\wp$ as above, and $a \in A$, let $Q_\wp(a) := (a^{q^d} - a)/\wp$ be the Fermat quotient. We denote its i-th iteration by $Q_\wp^{(i)}$.

(2) For $a = a(t) \in A$, we denote by $a^{(i)}$ its i-th derivative $d^i a/dt^i$ with respect to t.

(3) Let $A_\wp$ be the completion of A at $\wp$ and let $\mathbb{F}_\wp$ be its residue field. Let $\theta \in \mathbb{F}_\wp$ be the Teichmüller representative of t modulo $\wp$. We define the higher difference quotients $a^{[i]}$ of $a \in A$ by $a^{[0]}(t) = a(t)$ and $a^{[i+1]}(t) = (a^{[i]}(t) - a^{[i]}(\theta))/(t-\theta)$.

Theorem 2. [Tha13] *(i) A prime $\wp$ is a $!_c$-Wilson prime if and only if $\wp^{[2]}(\theta) = 0$.*

(ii) When $p > 2$, $\wp$ is a $!_c$-Wilson prime if and only if $\wp^{(2)} = d^2\wp/dt^2$ is identically zero. In other words, the $!_c$-Wilson primes are exactly the primes of the form $\sum p_i t^i$, with p_i non-zero implying $i \equiv 0, 1 \bmod p$.

(iii) When $p > 2$, if $\wp$ is a $!_c$-Wilson prime, then the Wilson congruence holds modulo $\wp^{p-1}$. Also, $\wp^{[i]}(\theta) = 0$, for $1 < i < p$.

(iv) When $p = 2$, the $!_c$-Wilson primes are exactly the primes of the form $\sum p_i t^i$, with p_i non-zero implying $i \equiv 0, 1 \bmod 4$. For such $\wp$, the Wilson congruence holds modulo $\wp^3$, and $\wp^{[i]}(\theta) = 0$, for $1 < i < 4$.

In particular, there are infinitely many $!_c$-Wilson primes, for any A.

In fact, the higher power congruences are detected by arithmetic derivatives up to multiplicity (at least) $q-1$.

Theorem 3. [Tha13] *Let $d := \deg \wp$. If $d = 1$, then $F_d = -1$ and the valuation of $Q_\wp(t)$ at $\wp$ is $q-2$.*

Let $d > 1$, and $k \le q$. Then $F_d \equiv -1 \bmod \wp^k$, if and only if $Q_\wp^{(2)}(t) \equiv 0 \bmod \wp^{k-1}$, if and only if $Q_\wp^{(r)}(t) \equiv 0 \bmod \wp$, for $2 \le r \le k$.

2.1.6. *Remarks.* (1) We only know, so far, examples of multiplicity $p-1$ rather than $q-1$ as in the theorem (when p is odd).

(2) For an interesting connection between the 'refined Wilson question' of the determination of the residue class of $((\mathcal{N}\wp - 1)/(q-1))!_c$ and the discriminant of polynomial $\wp$, see [SSTT13].

Finally, the Lerch congruence has the following stronger analog which is an equality!

Theorem 4. [SSTT13] *Let $a \in A$ run through all non-zero elements of degree d (standard reduced congruence class representatives modulo $\wp$ of degree d). Then*

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

2.2. **Second analog.** The second analog we will now consider follows well-known analogies [Gos96, Ros02, Tha04] between the Carlitz maps (recalled below) $x \to C_a(x)$, for $a \in A$ and the power maps $x \to x^n$, (or $x \to (1+x)^n - 1$), for $n \in \mathbb{Z}$, and replaces the Carlitz factorial $!_c$ by another factorial Π defined by

$$\Pi(x) := \prod_{a \in A+} (1 + \frac{x}{a})^{-1} \in \mathbb{F}_p(t),$$

for $x \in A$, with $-x$ not monic, where $A+$ denotes the set of monic polynomials in t. See [Tha04, 4.9-4.13] for its analogous properties such as the location of poles (in -$A+$), functional equations, interpolations at all primes and arithmetic of special values etc., and also for how the two analogs we consider are related to the two natural families of cyclotomic function fields: the constant field extensions obtained by adjoining roots of unity and the Carlitz-Drinfeld cyclotomic extensions obtained by adjoining the torsion of the Carlitz map. Note also that we basically excluded $q = 2$ with the conditions on x.

2.2.1. *Definitions and facts.* Let us now recall [Gos96, Tha12], [Tha04, Sec. 2.5] some basic definitions and facts related to Carlitz maps.

Let A_i+ denote the set of monic polynomials of degree i. For $n \in \mathbb{Z}$, $n \geq 0$, let $[n] := t^{q^n} - t$. For the following divisibility, congruence arguments in the proof of the theorem below, we only need to recall that $[n]$ is the product of monic irreducible polynomials of degree dividing n.

Let $d_n := \prod_{i=0}^{n-1} (t^{q^n} - t^{q^i}) = \prod [n-i]^{q^i}$ and $\ell_n := \prod_{i=1}^{n} (-[i])$, so that $d_0 = \ell_0 = 1$. Then (we will not need this), d_n is the product, whereas ℓ_n is the least common (monic) multiple, of all the monic polynomials of degree n.

Also, we have (see [HHM12] and [Tha10, Sec.6] and references above for different proofs) 'the reciprocal sum formula' $\sum 1/a = 1/\ell_i$, where the sum is over $a \in A_i+$.

For a non-negative integer i, we have the Carlitz binomial coefficient

$$\binom{x}{q^i} = \sum_{k=0}^{i} \frac{x^{q^k}}{d_k \ell_{i-k}^{q^k}} = \frac{\prod_{a \in A, \deg a < i} (x-a)}{d_i}.$$

We have

$$\prod_{a \in A_i+} (1 + x/a) = 1 + \binom{x}{q^i}.$$

The Carlitz maps are given by $C_a(z) = \sum_{i=0}^{\deg a} \binom{a}{q^i} z^{q^i}$, for $a \in A$. We have $C_{a+b}(z) = C_a(z) + C_b(z)$ and $C_a(C_b(z)) = C_{ab}(z)$, for $a, b \in A$.

2.2.2. *New Fermat-Wilson analogs.* The second analog of the Fermat congruence is then $C_\wp(a) \equiv a^{\mathcal{N}\wp} \equiv a \mod \wp$. The first congruence follows from the Eisenstein property [Tha04, p. 66] of $C_\wp(z)$ immediate also from the divisibility and explicit formulas mentioned above, and the second congruence then is the usual Fermat congruence.

The second analog [Tha12, Thm. 4.2] of the Wilson congruence is $\Pi(\wp) \equiv 1/2 \mod \wp$, if $p \neq 2$. (The reason why we choose this congruence, for this definition, out of the q congruences in [Tha12, Thm. 4.2] will be clear from the theorem below).

2.2.3. *Definition.* We call a prime $\wp$ a c-Wieferich prime for base a, if $\wp^2$ divides $C_\wp(a) - a^{\mathcal{N}\wp}$. We call a prime $\wp$ a c-Wieferich prime, if $\wp^2$ divides $C_{\wp-1}(1)$. We call a prime $\wp$, a Π-Wilson prime, if $\Pi(\wp) \equiv 1/2 \mod \wp^2$.

2.2.4. *Remarks.* (a) The c-Wieferich (short form for c-Wieferich for $a = 1$) condition is an analog of p^2 dividing $(1+1)^{p-1} - 1$.

(b) In defining $\Pi(x)$, we basically excluded $q = 2$, and in the definition of Π-Wilson, we basically excluded $p = 2$. When $q = 2$ and $\wp$ is of degree more than 1, then $t^2 + t$ divides $\wp - 1$, and thus $C_{\wp-1}(1) = 0$, and all such $\wp$'s are then c-Wieferich. We have [Tha04, Cha. 5], [Gos96] the Goss $\wp$-adic zeta value

$$\zeta_\wp(1) = \sum_{i=0}^{\infty} \sum_{a \in A_i +, (\wp,a)=1} \frac{1}{a}.$$

When $q = 2$ and $\wp$ is any prime, we have $\zeta_\wp(1) = 0$, as 1 is then 'even' (i.e., a multiple of $q-1$), the case excluded in [Tha94, p. 162], where the notion of c-Wieferich was introduced and the equivalence below with zeta values was mentioned.

Theorem 5. *Let $\wp$ be a monic prime of A of degree d.*

(i) When $q > 2$, or when $q = 2$ and $d > 1$, the prime $\wp$ is a c-Wieferich prime if and only if $\wp$ divides $\zeta_\wp(1)$.

(ii) Let the characteristic p be odd. Then the prime $\wp$ is a c-Wieferich prime, if and only if $\wp$ divides $\zeta_\wp(1)$, if and only if $\wp$ is a Π-Wilson prime.

(iii) We have $C_{\wp-1}(1)/\wp \equiv \zeta_\wp(1)$ modulo $\wp^{q-1}$, if $d > 1$, and the congruence holds to the $(q-2)$-th power when $d = 1$.

Proof. It was already noticed in [Tha94, p.162] that (i) follows from the log-algebraicity result [AT90, Thm. 3.8.3 II] on Carlitz zeta values that $\log_\wp(C_{\wp-1}(1)) = \wp\zeta_\wp(1)$, together with the fact (easily seen from the logarithmic series expression using the valuations of terms described in [Tha04, p. 46]) that for $z \in \mathbb{F}_q[t]$, divisible by $\wp$, the valuation at $\wp$ of $\log_\wp(z)$ and that of z are the same, unless $q = 2$ and $\deg \wp = 1$.

Now we give a more direct proof, using the combination of several results mentioned at the start of Section 2.2.

First, we have

$$\frac{C_{\wp-1}(1)}{\wp} = 1 + \sum_{i=1}^{d-1} \frac{\binom{\wp}{q^i}}{\wp} = 1 + \sum_{i=1}^{d-1} \sum_{k=0}^{i} \frac{\wp^{q^k-1}}{d_k \ell_{i-k}^{q^k}} \equiv 1 + \sum_{i=1}^{d-1} \frac{1}{\ell_i} \mod \wp^{q-1}.$$

On the other hand,

$$\zeta_\wp(1) = 1 + \sum_{i=0}^{d-1} \frac{1}{\ell_i} + \sum_{i \geq d} \Big(\sum_{a \in A_i +, (\wp,a)=1} \frac{1}{a} \Big).$$

So to prove (i) and (iii), it is enough to prove the claim that the sum inside the last round bracket (i.e., $1/\ell_i - 1/(\wp\ell_{i-d})$, by the reciprocal sum formula) is divisible by $\wp^{q-1}$, if $i \geq d$:

When $i > d$, this inner sum decomposes as the sums over orbits $1/(a + \theta\wp)$, as θ runs over the elements of $\mathbb{F}_q$. But using the $i = 1$ case of the reciprocal sum formula above, with $t = a/\wp$, the orbit sum is seen to be $\wp^{q-1}/(a\wp^{q-1} - a^q)$ which is divisible by $\wp^{q-1}$, as a is prime to $\wp$.

The special case $i = d + 1$ of the claim just proved gives $[1] \equiv (-1)^d [1] \cdots [d-1]([d]/\wp)[d+1]$ modulo $\wp^q$. On the other hand, $[d+1] - [1] = [d]^q$, and thus $[1] \equiv [d+1]$ modulo $\wp^q$. Also, if $d > 1$, these quantities are prime to $\wp$, thus

cancellation (and then multiplication by $\wp$) gives

$$[1][2]\cdots[d] \equiv (-1)^d \wp \mod \wp^{q+1},$$

which is equivalent to the claim for $i = d$. This finishes the proof of (i) and (iii).

To prove (ii), we note that, since $\binom{\wp}{q^d} = 1$, we have,

$$\Pi(\wp)^{-1} = \prod_{i=0}^{d}(1 + \binom{\wp}{q^i}) \equiv 2\prod_{i=0}^{d-1}(1 + \frac{\wp}{\ell_i}) \mod \wp^q$$

where the equality follows by [Tha04, 4.9.3] and the congruence follows by the steps just as above. Hence, $\wp$ is Π-Wilson, if and only if $\wp$ divides $\sum_{i=0}^{d-1} 1/\ell_i$, the same condition as above, thus finishing the proof. □

2.2.5. *Remarks.* (0) By simple $\mathbb{F}_q$-linearity consideration, the base $a = 1$ in this connection can be changed to $a = \theta \in \mathbb{F}_q^*$, whereas in Theorem 3, the base $a = t$ can be changed to any generator $\theta t + \mu, \theta \in \mathbb{F}_q^*, \mu \in \mathbb{F}_q$ of A. The part of Theorem 5 generalizes by the same proof showing that $\wp$ is c-Wieferich for $a \in A$, if and only if $\wp$ divides $\log_\wp(a)$, where $\log_\wp(z) = \sum z^{q^i}/\ell_i$ is the series for Carlitz logarithm considered $\wp$-adically. (Note that both the conditions are trivially satisfied if $\wp$ divides a). The corresponding statement, for general a, in the m-Wieferich case is unclear.

(i) Theorem 5 shows that for the second analog of Wilson primes also, there is a connection with Fermat type quotient, this time obtained using the Carlitz module. A simple example of a c-Wieferich prime, which the reader can verify directly, is $\wp = t^2 + t + \theta$, for $A = \mathbb{F}_4[t]$, with $\mathbb{F}_4 = \mathbb{F}_2(\theta)$. The proof shows that the degree d c-Wieferich primes can be efficiently found by taking the greatest common divisor of $A := 1 - [d-1] + \cdots + \ell_{d-1} = \ell_{d-1}\sum_{i=0}^{d-1} 1/\ell_i$ with $B := [d]$. Earlier by brute force and then by this method, my student George Todd (thanks to him) found that (a) for $q = 3$, for $d \le 9$ there are two such, $t^6 + t^4 + t^3 + t^2 + 2t + 2$ and $t^9 + t^6 + t^4 + t^2 + 2t + 2$, (b) for $q = 5$, $d \le 5$, there is only one, $t^5 - t + 1$, and (c) there are none for $q = 7$, $d \le 5$ or none for $d \le 4$ and $q = 11, 13, 17$. (At least for these examples, the valuation of $C_{\wp-1}(1)/\wp$ at $\wp$ is one). This very limited data may suggest that the degree of c-Wieferich prime is a multiple of the characteristic. There is no degree 1 c-Wieferich prime. With $x = [1]$, we have for $d = 2$, $A^q + B = x + 1$, and for $d = 3$,

$$A + xA^{q^2} + A^q(x^q + x + 3) + B^q(x^{q^2+1} + x) + B(x + 3 - x^{2q} - 2x^q) = 4 + 4x + 2x^2,$$

which is non-zero in odd characteristic, and the degree guess follows for $d = 2, 3$ (except for characteristic 2 when $d = 3$), exactly as in [Tha12, Sec. 9]. The author thanks Dong Quan Nguyen who pointed out the reference [Mau96, Pa. 237] where in fact the counterexamples to the naive guess above are presented in characteristic 2 for $d = 3$. See also his recent preprint [Ngup] for some more results on Carlitz-Wieferich and other types of primes in function fields.

(ii) We do not know whether there are infinitely many c-Wieferich primes if $q > 2$. See [AD12p] for some discussion, as well as connection of this question with Anderson's 'cyclotomic' units.

(iii) The last but one displayed congruence in the proof of the theorem above can be considered as a naive hybrid analog [Tha04, 4.13] of the classical Wilson congruence consequence that $p! \equiv -p \mod p^2$. (Compare congruence [Tha12, Thm. 7.1] for special primes).

(iv) The log-algebraicity result [AT90] mentioned in the proof above is, in fact, more general and gives 'zeta elements' proving Bloch-Kato type result for Carlitz zeta values $\zeta(n)$ for all positive integers n and for all primes of K, including the prime at infinity. Generalizing part (i) (found by the author in 1991 in response to Kato's question to him about divisibility of zeta values) from $n = 1$ to higher n, there are thus 'higher Wieferich criteria' [Tha94]. What are their number field analogs and arithmetic significance?

(v) The groups $(\mathbb{Z}/p\mathbb{Z})^*$ and $(A/\wp A)^*$ are cyclic, but while $(\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic for p odd, $(A/\wp^n A)^*$ is far from cyclic (see, e.g., [Tha04, p. 6]) in general, when $n > 1$.

(vi) We end this section by constructing some c-Wieferich primes $\wp$ of 'Artin-Schreier' type. Let $q = p$ be a prime and $\wp = t^p - t - \theta$, $\theta \in \mathbb{F}_q^*$. Then it is easy to see that modulo $\wp$, we have $[i] \equiv i\theta$ and A of remark (i) is congruent to $P(\theta) := \sum_{k=0}^{p-1} k!\theta^k$ (a simple transform of the truncated exponential), so that $\wp$ is c-Wieferich, if (and only if) $P(\theta) = 0$. Some (p, θ) satisfying this condition are $(5, 4), (7, 4), (11, 7), (13, 5), (13, 12), (19, 17), (31, 11), (37, 16), (37, 22), (37, 30), (37, 36)$, and there is no θ for $p = 3, 17, 23, 29$. Are there infinitely many p's for which there is a θ satisfying the condition? I thank Noam Elkies, who by writing and running a very nice 4-5 line Pari code for half a minute on his PC, found that out of first 168 primes, 1 has 5, 4 have 4, 9 have 3, 40 have 2, 60 have 1 and 54 have 0 such θ's, and observed that this distribution is close to random, which corresponds to probability $1/(N!e)$ for exactly N solutions.

3. $\wp$-adic zeta value at 1 versus p-adic Euler gamma constant

We now show that the part of the Theorem 5 carries over to the number field situation, once we use γ_p, the p-adic Euler gamma constant of J. Diamond and Y. Morita as a replacement of $\zeta_\wp(1)$, since $\zeta_p(1)$ does not exist.

Note that $\zeta(1)$ converges for the Carlitz zeta function [Tha04, 5.1], but not for the Riemann zeta function, and one often considers Euler gamma constant

$$\gamma = \lim_{x\to\infty} \sum_{n\le x} \frac{1}{n} - \log(x) = -\Gamma'/\Gamma(1)$$

as its renormalized substitute. (In the Carlitz zeta case, we have [Tha04, 4.9.2] $\zeta(1) = -\Pi'/\Pi(0)$). Similarly, $\zeta_\wp(1)$ above is convergent sum for the Carlitz-Goss zeta, but for the Kubota-Leopaldt p-adic zeta ζ_p, the value $\zeta_p(1)$ would be a limit of $\zeta(1 - p^n(p-1)) = -B_{(p-1)p^n}/((p-1)p^n)$ (up to an Euler factor which approaches 1) which diverges p-adically. We can then consider the p-adic analog $\gamma_p \in \mathbb{Q}_p$ of $\gamma \in \mathbb{R}$ introduced [Dia77, Kob78] by J. Diamond in his thesis by taking the value of the derivative of his p-adic log-gamma function (one can also use logarithmic derivative of Morita's p-adic gamma function). As in the case of the Euler gamma, it is the suitable renormalization of the divergent zeta value, as described below.

Fix p to be an odd prime. Let $\sum'$ and $\prod'$ denote the sum and product with indices restricted to those prime to p. We have [Dia77, Kob78]

$$\begin{aligned}\gamma_p :&= \frac{p}{p-1}\lim_{\epsilon\to 0}(\zeta_p(1+\epsilon)-\frac{1-1/p}{\epsilon})\\ &= -\frac{p}{p-1}\lim_{n\to\infty}(\frac{B_{(p-1)p^n}}{(p-1)p^n}-p^{-n-1})\\ &= -\frac{p}{p-1}\lim_{k\to\infty}\frac{1}{p^k}\sum_{i=1}^{p^k}{}'\log_p(i).\end{aligned}$$

Let $v_p(x)$ denote the valuation of $x\in\mathbb{Q}_p$ at p, normalized as usual so that $v_p(p)=1$.

Theorem 6. *For a prime $p\geq 5$, we have $v_p(\gamma_p)\geq 1$, and p is a Wilson prime, if and only if $v_p(\gamma_p)\geq 2$.*

Proof. Put

$$P_n := \prod_{i=1}^{p^n}{}' i, \qquad P_{n,k} := \prod_{i=1}^{p^n}{}'(i+kp^n).$$

Generalized Wilson theorem, proved using the same group theory argument applied to the cyclic group $(\mathbb{Z}/p^n\mathbb{Z})^*$, says that for an odd prime p, we have $P_n\equiv -1 \mod p^n$.

We claim $v_p(P_n+1)=n$ for all $n\geq 1$ for non-Wilson primes $p\geq 5$ and $v_p(P_n+1)\geq n+1$, if p is a Wilson prime.

Given the claim, the theorem follows, since $v_p(\gamma_p)=\lim v_p(\log_p(P_k))-k+1$, by the functional equation of p-adic logarithm turning sum into a product, and since $v_p(\log_p(x))=v_p(\log_p(-x))=v_p(1+x)$, when the last term is positive, by the series expansion of the p-adic logarithm.

We prove the claim by induction on n. The $n=1$ case follows from the definition of Wilson primes.

Let us recall two classical congruences by Bauer and Leudesdorf [HW71, Thm. 126, 128]:

$$\prod_{i=1}^{p^n}{}'(x-i)\equiv (x^{p-1}-1)^{p^{n-1}} \mod p^n,\ \ (p>2) \qquad (I),$$

$$\sum_{i=1}^{p^n}{}' 1/i\equiv 0 \mod p^{2n}, (p\geq 5) \qquad (II).$$

Now we first show that $P_{n,k}\equiv P_n \mod p^{3n}$, for $n\geq 1$ and $0\leq k<p$. For $p\geq 5$, just expanding the product, we have modulo p^{3n}, for example, $P_{n,k}\equiv P_n+P_n(\sum' 1/i)kp^n+P_n(\sum' 1/(i_1i_2))k^2p^{2n}\equiv P_n$ by (I) and (II), since (I) implies $\sum' 1/(i_1i_2)\equiv 0 \mod p^n$. Now $3n\geq n+2$. Hence, if $P_n\equiv -1+r_np^n \mod p^{n+1}$, then modulo p^{n+2}, we have

$$P_{n+1}=\prod_0^{p-1}P_{n,k}\equiv P_n^p\equiv(-1+r_np^n)^p\equiv -1-r_np^{n+1}.$$

Hence, whether p divides r_n or not stabilizes immediately, finishing the proof. □

3.1. **Remarks.** (1) The proof shows that if $v_p(P_n+1) = n+1$ for $n = 1$, then it is true for all $n \geq 1$. We have not made full use of the powerful congruences. They allow to extend this even if p is a Wilson prime with congruence holding to high power, by showing stabilization after some small n, but we are content here with proving the claim in the theorem.

(2) The congruences do not hold for $p = 3$. In fact, for $p = 3$, $v_p(P_n + 1)$ is 1 for $n = 1$, and $n + 1$ for $n > 1$ by obvious modification of the proof, starting at $n = 2$. For $p = 2$, $v_p(P_n + 1)$ is $1, 2, 1$ according as $n = 1, 2$ or more than 2. Noting that $1 \equiv -1 \mod 2$, if we consider $v_p(P_n - 1)$ instead, then it is infinite, 1, n according as n is 1, 2 or more than 2 respectively.

(3) While the author was led to this theorem by the analogy with the previous theorem in the function field case, because of the more direct factorial, gamma, γ_p connection, given in the third (but not the first or second 'renormalization') displayed formula for γ_p, the proof here is more transparent and boils down to stabilization of Wilson congruences up the p-adic tower. It is quite plausible that such a proof can also be given in the function field case, but the author started with the question of zeta divisibility and Wieferich type connection was discovered [Tha94] as a pleasant surprise. Theorems 5 and 6 were discovered only recently and in that order!

(4) The author thanks John Coates who pointed out the following Iwasawa theoretic result [FK86] of somewhat similar spirit giving another connection of higher Wieferich type congruence with quantities related to p-adic zeta. Let k be a real quadratic field, with class number h_k and the fundamental unit $\epsilon > 1$, and let p be an odd prime which splits $\wp_1\wp_2 = p$ in k. If $\wp_1^{h_k} = (\alpha)$ with $\alpha^{p-1} - 1 \in p\mathbb{Z}_p - p^2\mathbb{Z}_p$, then for n defined by $\epsilon^{p-1} - 1 \in p^n\mathbb{Z}_p - p^{n+1}\mathbb{Z}_p$, if $n > 1$, then [FK86] proved that the p-part of the class number of the m-th layer of cyclotomic $\mathbb{Z}_p$-extension of k, for $m > n$ is p^{n-1} times the p-part of h_k. Note that the class number information for the base is encoded (with regulator mixed up!) in p-adic zeta via the analytic class number formula, while the p-part class number growth in towers is encoded in p-adic zeta function (not value), at least through Iwasawa's λ and μ invariants (which are zero in this case), though not the stabilized part corresponding to the ν-invariant determined here!

4. Multiplicative versus Additive, Arithmetic versus Geometric, and $\mathbb{Z}$-module versus A-module

In this section, we elaborate a little on these analogies mentioned in the title of this section, and which we have encountered above.

In both the number field and function field context, we have looked at the multiplicative groups. Now let us consider the (easier) additive case.

If we use additive group $\mathbb{Z}/p\mathbb{Z}$, we have trivial $ap \equiv 0$ modulo p, for $a \in \mathbb{Z}$, which cannot hold modulo p^2, unless $a \equiv 0$ modulo p.

The usual proof the Wilson theorem follows by pairing elements with their multiplicative inverses, which in the additive context is essentially the same trick as that commonly attributed to Gauss as a schoolboy when he evaluated $0+1+2+\cdots n = n(n+1)/2$, by pairing k and $n-k$, and which for $n = p-1$ gives 0 modulo p (if $p > 2$), but not p^2.

John Tate, when he learned, as a schoolboy, about the factorial $n! = 1 \cdots n$, decided to study $n? := 1 + \cdots + n$ (exclamation mark versus question mark) by analogy, abandoning after some time when he realized its evaluation above!

Thus in the context of integers, the additive counterparts are much easier.

If we just consider the additive group $A/\wp A$, the story is similar. In fact, for $a \in A$, Norm($\wp$) now equals zero (and not just zero modulo $\wp$), as we are in characteristic p. Similarly, adding all standard representatives modulo $\wp$ given by all polynomials of degree less than d, gives zero, unless $q = 2$ and $d = 1$.

But much subtle and interesting analogs are produced once we ask for A-modules for analogs of $\mathbb{Z}$-modules, which are just abelian groups. This is what gave the second analog above. Let us elaborate a little.

While the torsion of the multiplicative group, namely the roots of unity suffice to generate all abelian extensions of $\mathbb{Q}$, in function fields they only give the constant field extensions (usually called arithmetic extensions). We get the 'geometric' abelian extensions by adjoining torsion of the Carlitz module (see [Tha04, Sec. 2.1] for motivated introduction with this viewpoint). Here we use instead of the multiplicative group, a $\mathbb{Z}$-module under the usual power map, the additive group (in function fields, there are more additive functions than just the linear functions, namely linear combinations of p-power power maps), considered as A-module via the Carlitz map above, using such additive functions. The Carlitz module is just normalized nice module structure of rank one on the additive group.

See [Tha04, 4.12] for how the two notions of factorial $!_c$ and Π fit in the 'arithmetic' and 'geometric' situations in a uniform framework with the usual factorial, with the special values and functional equations being 'explained' by the corresponding 'cyclotomic' extensions, for example.

In this way of replacing the multiplicative group by the Carlitz A-module (or more generally, Drinfeld modules), there are many interesting replacements of the corresponding classical notions such as additive character (and Gauss sums), cyclotomic units, unit group, class group to their A-module counterparts, resulting into new analogous questions and answers. For example, the resulting analog due to Anderson and Taelman of the Vandiver conjecture was shown [ATa13] to have many counter-examples, with the heuristic asymptotic count for the counterexamples structurally similar to that [Tha13] for $!_c$-Wilson primes, in contrast to the much lower growing ($\log\log(x)$ growth mentioned above) similar count [Was82, Sec. 8.3] for both the questions in the number field case. Is that a coincidence, or is there more to it?

Finally, we take this opportunity to correct misprints in [Tha12]: Replace '-1 and are' by '-1 and 1 are' in the third line of proof of Thm. 4.1. In Section 9 (A), 4th paragraph, line one, replace exponent '$q^s - 1$' by 'q^{s-1}', in fifth paragraph '$x - 1$' by '$1 - x$' and in 7th paragraph, second line, drop the extra 'F' in the expression for G (which is in clash of notation for gcd).

Notes added in the proof: Ravi Ramakrishna has recently informed the author that in his joint work with Ling Long on supercongruences, while determining valuation of the valuation of logarithm of Morita's p-adic log gamma function, he has found the last theorem independently with a different proof. Also, in a recent (unpublished) work, Alex Bamunoba has independently discovered the criterion for c-Wieferich Artin-Schreier primes in the remarks 2.2.5(vi) and has also proved the infinitude, when $q > 2$, of primes which are not c-Wieferich.

Acknowledgments: These results were presented on 15th October 2013 at the 60th birthday celebration conference at Montreal for M. Ram Murty. It is a pleasure to dedicate this paper to M. Ram Murty on his 60th birthday! I am grateful to him for a beautiful number theory course he taught at TIFR, when I was an undergraduate, and also for the encouragement and inspiring conversations over the years.

References

[AT90] Greg W. Anderson and Dinesh S. Thakur *Tensor powers of the Carlitz modules and Zeta values*. Ann. of Math. 132(1990), no.1, 159-191.

[AD12p] Bruno Angles and Mohamed Ould Douh. *Arithmetic of units in* $\mathbb{F}_q[t]$. ArXiv:1210.1660 (2012)

[ATa13] Bruno Angles and Lenny Taelman. *On a problem à la Kummer-Vandiver for function fields*. J. Number Theory, 133 (2013), 830-841.

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

[Bui05] Alexandru Buium. *Arithmetic differential equations*, Amer. Math. Soc. Providence (2005).

[Dia77] Jack Diamond. *The p-adic log-gamma function and p-adic Euler constants*, Trans. Amer. Math. Soc. 233 (1977), 321-337.

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

[EPT12] Aaron Ekstrom, Carl Pomerance, and Dinesh S. Thakur. *Infinitude of Elliptic Carmichael Numbers* J. Australian Math. Soc. 92 (2012), no. 1, 45-60, special issue in memory of van der Poorten.

[FK86] Takashi Fukuda and Keiichi Komatsu. *On* $\mathbb{Z}_p$*-extensions of real quadratic fields*, J. Math. Soc. Japan, **38**, no. 1 (1986), 95-102.

[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.

[Gra97] Andrew Granville. *Arithmetic properties of binomial coefficients I Binomial coefficients modulo prime powers* Organic Mathematics (Burnaby BC, 1995), 253-276, CMS Conf. Porc., 20, Amer. Math. Soc., Providence, RI 1997.

[HHM12] Kenneth Hickson, Xiang-dong Hou, and Gary L. Mullen. *Sums of reciprocals of polynomials over finite fields* Amer. Math. Monthky 119 (2012), no. 4, 313-317.

[HW71] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*, The English Language Book Society and Oxford University Press, 4th edition (1958), ELBS edition (1971).

[Iha92] Y. Ihara. *On Fermat quotient and differentiation of numbers* RIMS Kokyuroku 810 (1992), 324-341 (In Japanese) English translation by S. Hahn, U. Georgia preprint.

[Kob78] Neal Koblitz. *Interpretation of the p-adic log-gamma function and Euler constants using the Bernoulli measure*, Trans. Amer. Math. Soc. 242 (1978), 261-269.

[Mau96] Véronique Mauduit. *Carmichael-Carlitz polynomials and Fermat-Carlitz quotients*, in Finite Fields and applications (Glasgow 1995), 229-242, LMS lecture notes series **233**, Cambridge U Press, Cambridge (1996).

[Ngup] Dong Quan Nguyen *Carlitz module analogues of Merseene primes, Wieferich primes, and certain prime elements in cyclotomic function fields*, Preprint 2013.

[Rib95] Paulo Ribenboim. *The new book of prime number records* 3rd Edition, Springer-Verlag, New York 1995.

[Ros02] Michael Rosen. *Number theory in function fields* Springer-Verlag, New York 2002.

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

[SSTT13] Jim Sauerberg, Linghsueh Shu, Dinesh S. Thakur, and George Todd. *Infinitude of Wilson primes for* $\mathbb{F}_q[t]$. Acta Arith. 157, no. 1 (2013), 91-100.

[Tha94] Dinesh S. Thakur. *Iwasawa theory and cyclotomic function fields*. In Arithmetic Geometry (Tempe, AZ 1993), vol. 174 of Contemp. Math. 157-165, Amer. Math. Soc. 1994.

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

[Tha10] Dinesh S. Thakur. *Arithmetic of Gamma, Zeta and Multizeta values for function fields*. CRM Advanced courses 2010, to be published by Bikhauser.

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

[Tha13] Dinesh S. Thakur. *Differential characterization of Wilson primes for* $\mathbb{F}_q[t]$. Algebra and Number Theory 7:8 (2013), 1841-1848.

[Was82] Lawrence Washington, *Introduction to Cyclotomic Fields*, Springer, NY, 1982.

Department of Mathematics, University of Rochester, Rochester, NY 14627, dinesh.thakur@rochester.edu