GAUSS FACTORIALS OF POLYNOMIALS OVER FINITE FIELDS

XIUMEI LI AND MIN SHA

Abstract. In this paper we initiate a study on Gauss factorials of polynomials over finite fields, which are the analogues of Gauss factorials of positive integers.

1. Introduction

A well-known result in number theory, called Wilson's theorem, says that for any prime number p, we have

$$(p-1)! \equiv -1 \pmod{p}. \tag{1.1}$$

If we replace p by any composite integer in (1.1), it is not correct any more. Gauss proved a composite analogue of Wilson's theorem: for any integer $n > 1$,

$$\prod_{\substack{1\le j\le n-1\\ \gcd(j,n)=1}} j \equiv \begin{cases} -1 \pmod{n} & \text{for } n = 2, 4, p^k, \text{ or } 2p^k, \\ 1 \pmod{n} & \text{otherwise,} \end{cases} \tag{1.2}$$

where p is an odd prime and k is a positive integer.

In [3], Cosgrave and Dilcher called the product

$$\prod_{\substack{1\le j\le N\\ \gcd(j,n)=1}} j \tag{1.3}$$

a *Gauss factorial*, where N and n are positive integers. We refer to [6] for a very good survey on Gauss factorials of integers, and [4, 5, 7, 8] for recent work. In particular, when $n \ge 3$ is odd and $N = (n-1)/2$, the multiplicative order of the Gauss factorial (1.3) modulo n has been determined in [3, Theorem 2].

Throughout the paper, the letter p always denotes a prime, and $q = p^s$ for some integer $s \ge 1$. Let $\mathbb{F}_q$ be the finite field of q elements. We denote by $\mathbb{F}_q[X]$ the polynomial ring over $\mathbb{F}_q$. In the sequel, for simplicity let $\mathbb{A} = \mathbb{F}_q[X]$. It is known that $\mathbb{A}$ has many properties in common with the integers $\mathbb{Z}$, and thus many number theoretic problems about $\mathbb{Z}$ have their analogues for $\mathbb{A}$.

For any polynomial $f(X) \in \mathbb{A}$ of degree $\deg f \geq 1$, we define the *Gauss factorial* (denoted by $G(f)$) of f as follows:

$$G(f) = \prod_{\substack{g\in\mathbb{A}\\ 0\leq \deg g<\deg f\\ \gcd(g,f)=1}} g.$$

That is, $G(f)$ is the product of all *non-zero* polynomials of degree less than $\deg f$ and coprime to f. By convention, if $f \in \mathbb{F}_q$, we define $G(f) = 1$. Note that if f is irreducible, the definition of $G(f)$ only depends on the degree of f.

Moreover, given integer $n \geq 1$ and polynomial $f \in \mathbb{A}$, we define

$$G(n, f) = \prod_{\substack{g\in\mathbb{A}\\ 0\leq \deg g\leq n\\ \gcd(g,f)=1}} g,$$

which is also called a *Gauss factorial*. In particular, $G(f) = G(\deg f - 1, f)$.

In this paper, we initiate the study of Gauss factorials of polynomials over finite fields by generalizing (1.2) and the main result in [3]. Certainly, there are many other things remaining to be explored.

We want to remark that one can similarly define *factorials* of polynomials over finite fields, and consider generalizing related classical results (some of them are listed in [2]).

2. Preliminaries

In this section, for the convenience of the reader we recall some basic results about polynomials over finite fields, which can be found in [11, Chapter 1 and Chapter 3].

For $f \in \mathbb{A}$, set $|f| = q^{\deg f}$ if $f \neq 0$, and $|f| = 0$ otherwise. For a non-constant polynomial $f \in \mathbb{A}$, write its prime factorization as

$$f = aP_1^{e_1} \cdots P_t^{e_t}, \tag{2.1}$$

where $a \in \mathbb{F}_q^*$, integer $e_j \geq 1$ $(1 \leq j \leq t)$, and each P_j $(1 \leq j \leq t)$ is a monic irreducible polynomial. Here, a monic irreducible polynomial in $\mathbb{A}$ is said to be a *prime polynomial*, and so in (2.1) each P_j $(1 \leq j \leq t)$ is a *prime divisor* of f.

Given a non-zero polynomial $f \in \mathbb{A}$, denote by $\mathbb{A}/f\mathbb{A}$ the residue class ring of $\mathbb{A}$ modulo f and by $(\mathbb{A}/f\mathbb{A})^*$ its unit group.

Lemma 2.1. *Let $f \in \mathbb{A}$ be a non-constant polynomial with prime factorization as in (2.1). Then, we have*

$$(\mathbb{A}/f\mathbb{A})^* \cong (\mathbb{A}/P_1^{e_1}\mathbb{A})^* \times \cdots \times (\mathbb{A}/P_t^{e_t}\mathbb{A})^*.$$

Lemma 2.2. *Let $P \in \mathbb{A}$ be an irreducible polynomial, and e a positive integer. Then, we have*

$$(\mathbb{A}/P^e\mathbb{A})^* \cong (\mathbb{A}/P\mathbb{A})^* \times (\mathbb{A}/P^e\mathbb{A})^{(1)},$$

where $(\mathbb{A}/P\mathbb{A})^*$ is a cyclic group of order $|P|-1$, and $(\mathbb{A}/P^e\mathbb{A})^{(1)}$ is a p-group of order $|P|^{e-1}$.

For any non-zero polynomial $f \in \mathbb{A}$, let $\Phi(f) = |(\mathbb{A}/f\mathbb{A})^*|$, which is the so-called *Euler totient function* of $\mathbb{A}$.

Lemma 2.3. *For any non-zero polynomial $f \in \mathbb{A}$, we have*

$$\Phi(f) = |f| \prod_{P|f} \big(1 - 1/|P|\big),$$

where the product runs through all the prime divisors of f.

Let $P \in \mathbb{A}$ be an irreducible polynomial. When q is odd, given a non-zero polynomial $g \in \mathbb{A}$ with $\gcd(g, P) = 1$, as usual we define the *Legendre symbol* $\left(\frac{g}{P}\right) = \pm 1$ such that

$$\left(\frac{g}{P}\right) \equiv g^{\frac{|P|-1}{2}} \pmod{P}.$$

Let $f \in \mathbb{A}$ be a non-constant polynomial with the prime factorization as in (2.1). Given a non-zero polynomial $g \in \mathbb{A}$ with $\gcd(g, f) = 1$, the *Kronecker symbol* $\left(\frac{g}{f}\right) = \pm 1$ is defined as

$$\left(\frac{g}{f}\right) = \prod_{j=1}^{t} \left(\frac{g}{P_j}\right)^{e_j}.$$

As usual, for two non-zero polynomials $g_1, g_2 \in \mathbb{A}$ with $\gcd(g_1 g_2, f) = 1$, we have

$$\left(\frac{g_1 g_2}{f}\right) = \left(\frac{g_1}{f}\right)\left(\frac{g_2}{f}\right).$$

Lemma 2.4 (The reciprocity law)**.** *Let $f, g \in \mathbb{A}$ be relatively prime non-zero polynomials. Assume that q is odd, and both f and g are monic. Then, we have*

$$\left(\frac{g}{f}\right) = (-1)^{\frac{q-1}{2}\deg f \deg g}\left(\frac{f}{g}\right).$$

The following lemma is essentially a special case of a result due to Artin [1, Section 18, Equation (10)].

Lemma 2.5. *Assume that q is odd. Let $P \in \mathbb{A}$ be a prime polynomial of odd degree. Denote by $h(-P)$ the class number of the quadratic function field $\mathbb{F}_q(X, \sqrt{-P})$. Then, we have*

$$h(-P) = \sum_{\substack{g \text{ monic} \\ 0 \le \deg g < \deg P}} \left(\frac{g}{P}\right).$$

Proof. Following Artin [1] the quadratic function field $\mathbb{F}_q(X, \sqrt{-P})$ is imaginary (see also [11, Proposition 14.6] and the discussions therein). So, using [1, Section 18, Equation (10)] and [1, Section 17, Equation (4)] directly (alternatively, applying arguments similar to those in the proof of [11, Theorem 16.8]), we obtain

$$h(-P) = \sum_{\substack{g \text{ monic} \\ 0 \le \deg g < \deg P}} \left(\frac{-P}{g}\right).$$

Here one should note that since $-P$ can be viewed as a monic polynomial with respect to $-X$, we can apply the results in [1].

For each summation term in the above formula, using the reciprocity law (Lemma 2.4) and noticing that $\deg P$ is odd, we deduce that

$$\left(\frac{-P}{g}\right) = (-1)^{\frac{(q-1)\deg g}{2}} \left(\frac{P}{g}\right) = \left(\frac{g}{P}\right),$$

which implies the desired result. □

Finally, we reproduce a useful result due to Miller [9, Section 1], which can yield a simple proof of (1.2).

Lemma 2.6. *Let A be an abelian group. Then, the product $\prod_{a \in A} a$ is the identity element if A either has no element of order two or has more than one element of order two, otherwise the product is equal to the element of order two.*

3. Congruence formulas

In this section, our main objective is to generalize (1.2) to $G(f)$ by following the approach in [9]. One can see that we have two quite different cases depending on the characteristic of $\mathbb{A}$ (that is, p).

We first remark that it is known that for any irreducible polynomial $P \in \mathbb{A}$, we have (for instance see [11, Chapter 1, Corollary 2])

$$G(P) \equiv -1 \pmod{P},$$

which is an analogue of (1.1). Besides, it is easy to see that if non-zero $f \in \mathbb{A}$ is reducible and square-free, then we have

$$\prod_{\substack{g \in \mathbb{A} \\ 0 \le \deg g < \deg f}} g \equiv 0 \pmod{f}.$$

Theorem 3.1. *Assume that p is odd. Then, for any polynomial $f \in \mathbb{A}$ of degree $\deg f \ge 1$, we have*

$$G(f) \equiv \begin{cases} -1 \pmod{f} & \text{if } f \text{ has only one prime divisor,} \\ 1 \pmod{f} & \text{otherwise.} \end{cases}$$

Proof. Note that p is odd. Then, for any irreducible polynomial $P \in \mathbb{A}$ and integer $e \ge 1$, by Lemma 2.2 the group $(\mathbb{A}/P^e\mathbb{A})^*$ has only one element of order two (that is, -1). So, applying Lemma 2.1, it is easy to see that the abelian group $(\mathbb{A}/f\mathbb{A})^*$ has only one element of order two if and only if f has only one prime divisor. Then, the desired result now follows from Lemma 2.6. □

Theorem 3.2. *Assume that $p = 2$. For any polynomial $f \in \mathbb{A}$ of degree $\deg f \ge 1$ with the prime factorization as in (2.1), we have*

$$G(f) \equiv \begin{cases} f/P_1 + 1 \pmod{f} & \text{if } q = 2, \deg P_1 = 1, 2 \le e_1 \le 3, \text{ and all the} \\ & \quad \text{other exponents } e_j = 1 \text{ if they exist,} \\ 1 \pmod{f} & \text{otherwise.} \end{cases}$$

Proof. We first remark that -1 is not an element of order two, because $p = 2$. We also note that for any irreducible polynomial $P \in \mathbb{A}$, the order of $(\mathbb{A}/P\mathbb{A})^*$ is an odd number, and thus the group $(\mathbb{A}/P\mathbb{A})^*$ has no element of order two.

Let $P \in \mathbb{A}$ be an irreducible polynomial, and e a positive integer. If h is an element of order two of $(\mathbb{A}/P^e\mathbb{A})^*$, then $P^e \mid (h+1)^2$. So, it is easy to see that when e is even, the set of elements of order two of $(\mathbb{A}/P^e\mathbb{A})^*$ is

$$\Big\{ gP^{e/2} + 1 : g \in \mathbb{A}, 0 \le \deg g < \frac{e}{2} \deg P \Big\},$$

whose cardinality is $q^{\frac{1}{2}e \deg P} - 1$. Similarly, if e is odd and greater than 1, then the set of elements of order two of $(\mathbb{A}/P^e\mathbb{A})^*$ is

$$\Big\{ gP^{(e+1)/2} + 1 : g \in \mathbb{A}, 0 \le \deg g < \frac{e-1}{2} \deg P \Big\},$$

whose cardinality is $q^{\frac{1}{2}(e-1)\deg P} - 1$. Thus, $(\mathbb{A}/P^e\mathbb{A})^*$ has only one element of order two if and only if $\deg P = 1, 2 \le e \le 3$, and $q = 2$.

Hence, the desired result follows by using Lemma 2.1 and Lemma 2.6, and noticing that f/P_1+1 is indeed an element of order two of $(\mathbb{A}/f\mathbb{A})^*$ if $e_1 \geq 2$. □

Furthermore, we can get a congruence identity for $G(n,f)$ when $n \geq \deg f$. This can also be viewed as an analogue of (1.2).

Theorem 3.3. *For any polynomial $f \in \mathbb{A}$ of degree $\deg f \geq 1$, if the integer n satisfies $n \geq \deg f$, we have*

$$G(n,f) \equiv \begin{cases} -1 \pmod{f} & \text{if } p \text{ is odd and } f \text{ has only one prime divisor,} \\ 1 \pmod{f} & \text{otherwise.} \end{cases}$$

Proof. Fix an arbitrary integer $m \geq \deg f$. For any polynomial $g \in \mathbb{A}$ with $\deg g < \deg f$ and $\gcd(g,f)=1$, it is easy to see that the set of polynomials in $\mathbb{A}$ of degree m and congruent to g modulo f is

$$\Big\{g + fr : r \in \mathbb{A}, \deg r = m - \deg f\Big\},$$

whose cardinality is $(q-1)q^{m-\deg f}$.

Thus, we obtain

$$\begin{aligned} G(n,f) &\equiv G(f) \prod_{m=\deg f}^{n} G(f)^{(q-1)q^{m-\deg f}} \\ &\equiv G(f)^{q^{n+1-\deg f}} \pmod{f}. \end{aligned}$$

We then conclude the proof by using Theorem 3.1 and Theorem 3.2. □

4. Multiplicative orders

As mentioned before, when the integer $n \geq 3$ is odd and $N=(n-1)/2$, Cosgrave and Dilcher have determined the multiplicative order of the Gauss factorial (1.3) modulo n in [3, Theorem 2]. That is, they only considered *half* of the positive integers less than n. In this section, assume that q is odd, then our aim is to get some similar results concerning a special divisor of $G(f)$. For this divisor, we only consider *half* of the polynomials of degree less than $\deg f$ and coprime to f.

For any non-zero $g \in \mathbb{A}$, we denote by $\operatorname{sgn}(g)$ the leading coefficient of g, which is called the *sign* of g. Let S be a subset of $\mathbb{F}_q^*$ such that $|S| = (q-1)/2$ and for any $\alpha \in \mathbb{F}_q^*$ if $\alpha \in S$ then $-\alpha \notin S$. Obviously, the set S has $2^{(q-1)/2}$ choices.

Define $\delta(S) = \prod_{a\in S} a$. Notice that

$$\delta(S)^2 = (-1)^{\frac{q-1}{2}} \prod_{a\in\mathbb{F}_q^*} a = (-1)^{\frac{q+1}{2}}. \tag{4.1}$$

So, if $q \equiv 3 \pmod 4$, we have $\delta(S)^2 = 1$, and then $\delta(S) = \pm 1$.

Note that for any non-zero $g \in \mathbb{A}$, $\operatorname{sgn}(g) \in S$ if and only if $\operatorname{sgn}(-g) \notin S$. So, for any polynomial $f \in \mathbb{A}$ of degree $\deg f \geq 1$, we easily have

$$G(f) = (-1)^{\Phi(f)/2} G(f, S)^2,$$

where

$$G(f, S) = \prod_{\substack{g \in \mathbb{A}, \operatorname{sgn}(g) \in S \\ 0 \leq \deg g < \deg f \\ \gcd(g, f) = 1}} g.$$

Thus, by Theorem 3.1 we obtain

$$G(f, S)^2 \equiv \begin{cases} -(-1)^{\Phi(f)/2} \pmod f & \text{if } f \text{ has only one prime divisor,} \\ (-1)^{\Phi(f)/2} \pmod f & \text{otherwise.} \end{cases}$$

This implies that the multiplicative order of $G(f, S)$ modulo f only can possibly be 1, 2 or 4.

Here, we want to determine the multiplicative order of $G(f, S)$ modulo f, which is denoted by $\operatorname{ord}_f G(f, S)$. The main result is as follows.

Theorem 4.1. *Assume that q is odd, and let $f \in \mathbb{A}$ be a polynomial having the prime factorization as in (2.1). Then*

(1) $\operatorname{ord}_f G(f, S) = 4$ *when* $t = 1$, *and either* $q \equiv 1 \pmod 4$ *or* $\deg P_1$ *is even.*
(2) $\operatorname{ord}_f G(f, S) = 2$ *when*
   (a) $t = 1$, $q \equiv 3 \pmod 4$, $\deg P_1$ *is odd,* $\delta(S) = 1$, *and* $e_1 + \frac{1}{2}(h(-P_1) - 3) \equiv 1 \pmod 2$, *or*
   (b) $t = 1$, $q \equiv 3 \pmod 4$, $\deg P_1$ *is odd,* $\delta(S) = -1$, *and* $e_1 + \frac{1}{2}(h(-P_1) - 3) \equiv 0 \pmod 2$, *or*
   (c) $t = 2$, $q \equiv 1 \pmod 4$, *and* P_1 *is not a quadratic residue modulo* P_2, *or*
   (d) $t = 2$, $q \equiv 3 \pmod 4$, *both* $\deg P_1$ *and* $\deg P_2$ *are even, and* P_1 *is not a quadratic residue modulo* P_2, *or*
   (e) $t = 2$, $q \equiv 3 \pmod 4$, *and either* $\deg P_1$ *or* $\deg P_2$ *is odd;*
(3) $\operatorname{ord}_f G(f, S) = 1$ *in all other cases.*

From Theorem 4.1 one can see that for many cases $\operatorname{ord}_f G(f, S)$ is independent of the choice of S. Especially some results are related to the class numbers of function fields. Actually, we do more in the paper: the value of $G(f, S)$ modulo f is either explicitly given or easily computable.

Before proving Theorem 4.1, we illustrate an example to confirm some results in Theorem 4.1 by using the computer algebra system PARI/GP [12]. Choose $q = 3$ and $P = X^3 + 2X + 2$, then by Lemma

2.5 we have $h(-P) = 7$. If furthermore we choose $S = \{1\}$, we have $\delta(S) = 1$ and $G(P, S) = -1$, and thus $\mathrm{ord}_P G(P, S) = 2$, which is compatible with Theorem 4.1 (2); otherwise if we choose $S = \{-1\}$, we get $\mathrm{ord}_P G(P, S) = 1$, which is also consistent with Theorem 4.1 (3).

In the following, we divide the proof of Theorem 4.1 into several cases.

4.1. **One prime divisor.** We continue the general discussion about $G(f, S)$.

Suppose that f has the prime factorization as in (2.1). Then, by Lemma 2.3 we get

$$\Phi(f) = \prod_{i=1}^{t} q^{(e_i-1)\deg P_i}(q^{\deg P_i} - 1).$$

Note that q is odd, so

$$(-1)^{\frac{1}{2}\Phi(f)} = (-1)^{\frac{1}{2}\prod_{i=1}^{t}(q^{\deg P_i}-1)}.$$

If $t \geq 2$, that is, f has at least two distinct prime divisors, then we have $(-1)^{\frac{1}{2}\Phi(f)} = 1$, and thus

$$G(f, S)^2 \equiv 1 \pmod{f}.$$

Now assume that $t = 1$, that is, f has only one prime divisor P_1. Then it is easy to see that

$$G(f, S)^2 \equiv \begin{cases} -1 & \text{if } q \equiv 1 \pmod 4, \text{ or } \deg P_1 \text{ is even,} \\ 1 & \text{otherwise.} \end{cases}$$

Thus, for any $f \in \mathbb{A}$ of positive degree and with the prime factorization as in (2.1), we have

(4.2)

$$G(f, S)^2 \equiv \begin{cases} -1 \pmod f & \text{if } t = 1, \text{ and either } q \equiv 1 \pmod 4 \text{ or } \deg P_1 \text{ is even,} \\ 1 \pmod f & \text{otherwise.} \end{cases}$$

The above equation immediately gives the following partial result:

Theorem 4.2. *Assume that q is odd. If f has only one prime divisor P, and either $q \equiv 1 \pmod 4$ or P has even degree, then* $\mathrm{ord}_f G(f, S) = 4$. *Otherwise,* $\mathrm{ord}_f G(f, S) = 1$ *or* 2.

For further deductions, we need to get a new expression of $G(f, S)$. Fix an arbitrary polynomial $f \in \mathbb{A}$ of degree $\deg f \geq 1$. Let i_n be the

cardinality of the set $\{g \in \mathbb{A} : g \text{ monic}, \deg g = n, \gcd(g, f) = 1\}$. Note that

$$\sum_{n=0}^{\deg f-1} i_n = \frac{\Phi(f)}{q-1}.$$

Denote

$$M(f) = \Big(\prod_{\substack{g \text{ monic} \\ 0 \le \deg g < \deg f, \gcd(g,f)=1}} g \Big)^{(q-1)/2},$$

which is also a polynomial in $\mathbb{A}$. Now, we deduce that

$$\begin{aligned} G(f,S) &= \prod_{a \in S} \Big(\prod_{n=0}^{\deg f-1} a^{i_n} \prod_{\substack{g \text{ monic} \\ \deg g = n, \gcd(g,f)=1}} g \Big) \\ &= \Big(\prod_{a \in S} a \Big)^{\frac{\Phi(f)}{q-1}} \Big(\prod_{\substack{g \text{ monic} \\ 0 \le \deg g < \deg f, \gcd(g,f)=1}} g \Big)^{\frac{q-1}{2}} \\ &= \delta(S)^{\frac{\Phi(f)}{q-1}} M(f). \end{aligned} \tag{4.3}$$

So, our problem is reduced to studying $M(f)$ modulo f.

By definition we also rewrite

$$\begin{aligned} G(f) = \prod_{\substack{0 \le \deg g < \deg f \\ \gcd(g,f)=1}} g &= \prod_{n=0}^{\deg f-1} \Big(\prod_{\substack{\deg g = n \\ \gcd(g,f)=1}} g \Big) \\ &= \prod_{n=0}^{\deg f-1} \left(\Big(\prod_{a \in \mathbb{F}_q^*} a \Big)^{i_n} \Big(\prod_{\substack{g \text{ monic} \\ \deg g = n, \gcd(g,f)=1}} g \Big)^{q-1} \right) \\ &= (-1)^{\frac{\Phi(f)}{q-1}} M(f)^2. \end{aligned}$$

Now assume that f has the prime factorization as in (2.1). So, using Theorem 3.1 we obtain

$$M(f)^2 \equiv \begin{cases} -1 \pmod f & \text{if } t = 1 \text{ and } \deg P_1 \text{ is even}, \\ 1 \pmod f & \text{otherwise.} \end{cases} \tag{4.4}$$

We first handle $M(f)$ in the case when f is irreducible.

Lemma 4.3. *Assume that $q \equiv 3 \pmod 4$. If $f \in \mathbb{A}$ is an irreducible polynomial of odd degree with the form $f = aP$, where $a \in \mathbb{F}_q^*$ and*

$P \in \mathbb{A}$ is a prime polynomial, then

$$M(f) \equiv (-1)^{\frac{1}{2}(h(-P)-1)} \pmod{P}.$$

Proof. We apply similar arguments as in [10]. By definition, we directly have $M(f) = M(P)$. So, it is equivalent to determine the value of $M(P)$ modulo P (or equivalently modulo f).

Put $d = \deg P$. We first make some preparations. Let N (resp. R) be the number of monic polynomials in $\mathbb{A}$ of degree less than d which are quadratic non-residues (resp. quadratic residues) modulo P. So,

$$N + R = 1 + q + \cdots + q^{d-1},$$

which, together with Lemma 2.5, implies that

$$N = \frac{1}{2}\Big(1 + q + \cdots + q^{d-1} - h(-P)\Big).$$

Note that $q \equiv 3 \pmod 4$ and d is odd, so we have

$$1 + q + \cdots + q^{d-1} \equiv 1 \pmod 4.$$

Thus, we get

$$N \equiv \frac{1}{2}\big(h(-P) - 1\big) \pmod 2. \tag{4.5}$$

Given a non-zero polynomial g which is a quadratic residue modulo P, bg is also a quadratic residue for any square element $b \in \mathbb{F}_q^*$ (equivalently, b is a quadratic residue modulo P), and

$$\prod_{b\in\mathbb{F}_q^*, \left(\frac{b}{P}\right)=1} bg = g^{(q-1)/2}.$$

Besides, note that for any non-zero polynomial $g \in \mathbb{A}$, we can write $g = cg_0$ for some $c \in \mathbb{F}_q^*$ and monic polynomial $g_0 \in \mathbb{A}$. Then, noticing $q \equiv 3 \pmod 4$, we get

$$g^{(q-1)/2} = \pm g_0^{(q-1)/2} = (\pm g_0)^{(q-1)/2}.$$

Based on the above observations and the fact that -1 is not a quadratic residue modulo P and is the unique element of order two in $(\mathbb{A}/P\mathbb{A})^*$, we deduce that

$$1 = \prod_{\substack{\left(\frac{g}{P}\right) = 1 \\ 0\le\deg g<d}} g = \prod_{\substack{\mathrm{sgn}(g) = \pm 1,\ \left(\frac{g}{P}\right) = 1 \\ 0\le\deg g<d}} g^{(q-1)/2}, \tag{4.6}$$

where we also use the simple fact that the inverse of a quadratic residue is also a quadratic residue (modulo P).

Using (4.6), we obtain

$$\begin{aligned} M(P) &= \Big(\prod_{\substack{g \text{ monic, } (\frac{g}{P})=1 \\ 0\le \deg g<d}} g \prod_{\substack{g \text{ monic, } (\frac{g}{P})=-1 \\ 0\le \deg g<d}} g \Big)^{(q-1)/2} \\ &= (-1)^N \prod_{\substack{g \text{ monic, } (\frac{g}{P})=1 \\ 0\le \deg g<d}} g^{(q-1)/2} \prod_{\substack{g \text{ monic, } (\frac{g}{P})=-1 \\ 0\le \deg g<d}} (-g)^{(q-1)/2} \\ &= (-1)^N \prod_{\substack{\mathrm{sgn}(g)=\pm 1, \ (\frac{g}{P})=1 \\ 0\le \deg g<d}} g^{(q-1)/2} \\ &\equiv (-1)^N \pmod P. \end{aligned}$$

Now, the desired result follows from (4.5). □

In the following, we extend the result in Lemma 4.3 to the case when f is a power of some prime polynomial up to a constant. Actually, we can obtain a more general form.

Lemma 4.4. *If $f \in \mathbb{A}$ is a polynomial of the form $f = aP^e$, where $a \in \mathbb{F}_q^*$, $P \in \mathbb{A}$ is a prime polynomial and e is a positive integer, then*

$$M(f) \equiv (-1)^{\frac{(e-1)(q-1)}{2} \deg P} M(P) \pmod P.$$

Proof. Put $d = \deg P$. Note that for any non-zero polynomial $g \in \mathbb{A}$ of degree $\deg g < \deg f = de$, by the Euclidean division we can write

$$g = g_1 P + g_2 \quad \text{for some } g_1, g_2 \in \mathbb{A},$$

where g_1 and g_2 satisfy $\deg g_1 < d(e-1)$ and $g_2 = 0$ or $0 \le \deg g_2 < d$. Then by definition, we have

$$M(f) = \Big(Q_0 Q_1 \Big)^{(q-1)/2},$$

where

$$Q_0 = \prod_{\substack{g \text{ monic} \\ 0\le \deg g<d}} g \quad \text{and} \quad Q_1 = \prod_{\substack{g_2 \in \mathbb{A} \\ 0\le \deg g_2<d}} \prod_{\substack{g_1 \text{ monic} \\ 0\le \deg g_1<d(e-1),}} (g_1 P + g_2).$$

Now for Q_1, we deduce that

$$\begin{aligned} Q_1 &\equiv \Big(\prod_{\substack{g \in \mathbb{A} \\ 0\le \deg g<d}} g \Big)^{\frac{q^{d(e-1)}-1}{q-1}} \pmod P \\ &\equiv G(P)^{\frac{q^{d(e-1)}-1}{q-1}} \pmod P \\ &\equiv (-1)^{d(e-1)} \pmod P, \end{aligned}$$

where we have applied Theorem 3.1. Therefore

$$\begin{aligned} M(f) &= \Big(Q_0 Q_1\Big)^{(q-1)/2} \\ &\equiv (-1)^{\frac{d(e-1)(q-1)}{2}} M(P) \pmod{P}, \end{aligned}$$

which completes the proof. □

We also need a simple but useful result, which is an analogue of [3, Lemma 1]. One can prove it in a straightforward manner; we therefore omit its proof.

Lemma 4.5. *Suppose that q is odd. Let $f, g \in \mathbb{A}$ be two non-constant polynomials. Given an integer $e \geq 1$, assume that $f^2 \equiv 1 \pmod{g^e}$. Then, $f \equiv \pm 1 \pmod{g^e}$ if and only if $f \equiv \pm 1 \pmod{g}$, with the signs corresponding to each other.*

Now we are ready to get a partial result about the value of $G(f, S)$ modulo f. We use the product $\delta(S)$ defined just before (4.1).

Theorem 4.6. *Assume that $q \equiv 3 \pmod 4$. If $f \in \mathbb{A}$ is a polynomial of the form $f = aP^e$, where $a \in \mathbb{F}_q^*$, $P \in \mathbb{A}$ is a prime polynomial of odd degree and e is a positive integer, then*

$$G(f, S) \equiv (-1)^{e+\frac{1}{2}(h(-P)-3)} \delta(S) \pmod{f}.$$

Proof. By (4.3), we first note that

$$G(f, S) = \delta(S)^{\frac{\Phi(f)}{q-1}} M(f) = \delta(S) M(f),$$

where we use the fact that $\delta(S) = \pm 1$ since $q \equiv 3 \pmod 4$. From Lemma 4.4, we have

$$M(f) \equiv (-1)^{\frac{(e-1)(q-1)}{2} \deg P} M(P) \equiv (-1)^{e-1} M(P) \pmod{P},$$

which, together with Lemma 4.3, gives

$$M(f) \equiv (-1)^{e-1+\frac{1}{2}(h(-P)-1)} \pmod{P}. \tag{4.7}$$

Since $M(f)^2 \equiv 1 \pmod{P^e}$ by (4.4), using Lemma 4.5 we know that $M(f) \equiv \pm 1 \pmod{P^e}$ if and only if $M(f) \equiv \pm 1 \pmod{P}$, with the signs corresponding to each other. Thus, by (4.7) we obtain

$$M(f) \equiv (-1)^{e+\frac{1}{2}(h(-P)-3)} \pmod{P^e}. \tag{4.8}$$

Now, the desired result follows. □

4.2. **Two or more prime divisors.** In this section, we deal with the case when f has more than one prime divisors. We start with a key lemma.

Lemma 4.7. *If $f \in \mathbb{A}$ is a polynomial having the prime factorization as in (2.1), then*

$$M(f) \equiv \begin{cases} (-1)^{\frac{q-1}{2}\deg P_2} P_2^{-\frac{\Phi(P_1^{e_1})}{2}} \pmod{P_1^{e_1}} & \text{if } t = 2, \\ P_t^{-\frac{\Phi\left(P_1^{e_1}P_2^{e_2}\cdots P_{t-1}^{e_{t-1}}\right)}{2}} \pmod{P_1^{e_1}P_2^{e_2}\cdots P_{t-1}^{e_{t-1}}} & \text{if } t \geq 3. \end{cases}$$

Proof. Put $\widetilde{f} = P_1^{e_1}P_2^{e_2}\cdots P_{t-1}^{e_{t-1}}, d_t = \deg P_t$. Note that for any non-zero polynomial $g \in \mathbb{A}$ of degree $\deg g < \deg f$, by the Euclidean division we can write

$$g = g_1\widetilde{f} + g_2 \quad \text{for some } g_1, g_2 \in \mathbb{A},$$

where g_1 and g_2 satisfy $\deg g_1 < d_t e_t$ and $g_2 = 0$ or $0 \leq \deg g_2 < \deg \widetilde{f}$. Then by definition, we have

$$M(f) = \Big(Q_0 Q_1\Big)^{(q-1)/2}, \tag{4.9}$$

where

$$Q_0 = \prod_{\substack{g_2 \text{ monic} \\ 0\leq \deg g_2 < \deg \widetilde{f} \\ \gcd(g_2, f)=1}} g_2 \quad \text{and} \quad Q_1 = \prod_{\substack{g_2 \in \mathbb{A} \\ 0\leq \deg g_2 < \deg \widetilde{f} \\ \gcd(g_2, f)=1}} \prod_{\substack{g_1 \text{ monic} \\ 0\leq \deg g_1 < d_t e_t,}} (g_1\widetilde{f} + g_2).$$

Now, we define

$$\overline{Q_0} = \prod_{\substack{g_2 \text{ monic} \\ 0\leq \deg g_2 < \deg \widetilde{f} \\ (g_2, \widetilde{f})=1}} g_2 \quad \text{and} \quad \overline{Q_1} = \prod_{\substack{g_2 \in \mathbb{A} \\ 0\leq \deg g_2 < \deg \widetilde{f} \\ \gcd(g_2, \widetilde{f})=1}} \prod_{\substack{g_1 \text{ monic} \\ 0\leq \deg g_1 < d_t e_t}} (g_1\widetilde{f} + g_2),$$

and obtain

$$\begin{aligned} \overline{Q_1} &\equiv \Big(\prod_{\substack{g_2 \in \mathbb{A} \\ 0\leq \deg g_2 < \deg \widetilde{f} \\ \gcd(g_2, \widetilde{f})=1}} g_2 \Big)^{\frac{q^{d_t e_t}-1}{q-1}} \pmod{\widetilde{f}} \\ &\equiv G(\widetilde{f})^{\frac{q^{d_t e_t}-1}{q-1}} \pmod{\widetilde{f}}. \end{aligned}$$

For relating Q_j to $\overline{Q_j}$, we multiply all relevant multiples of P_t back to Q_0 and Q_1. More precisely, on the right-hand side of (4.9) we multiply

numerator and denominator by

$$\Big(\prod_{\substack{g \text{ monic}\\ 0\le \deg g<\deg \widetilde{f}+d_t(e_t-1)\\ \gcd(g,\widetilde{f})=1}} gP_t\Big)^{\frac{q-1}{2}},$$

which is equal to

$$\Big(\prod_{\substack{g \text{ monic}\\ 0\le \deg g<\deg \widetilde{f}\\ \gcd(g,\widetilde{f})=1}} gP_t\Big)^{\frac{q-1}{2}}\Big(\prod_{\substack{g_2\in\mathbb{A}\\ 0\le \deg g_2<\deg \widetilde{f}\\ \gcd(g_2,\widetilde{f})=1}}\prod_{\substack{g_1 \text{ monic}\\ 0\le \deg g_1<d_t(e_t-1),}} (g_1\widetilde{f}+g_2)P_t\Big)^{\frac{q-1}{2}}$$

$$\equiv M(\widetilde{f})P_t^{\frac{\Phi(\widetilde{f})}{2}}\left(\prod_{\substack{g_2\in\mathbb{A}\\ 0\le \deg g_2<\deg \widetilde{f}\\ \gcd(g_2,\widetilde{f})=1}}\Big(g_2P_t\Big)^{\frac{q^{d_t(e_t-1)}-1}{q-1}}\right)^{\frac{q-1}{2}} \pmod{\widetilde{f}}$$

$$\equiv M(\widetilde{f})P_t^{\frac{\Phi(\widetilde{f})}{2}}G(\widetilde{f})^{\frac{q^{d_t(e_t-1)}-1}{2}} \pmod{\widetilde{f}}.$$

Hence, from the above discussions, we deduce that

$$\begin{aligned} M(f) &\equiv \frac{\Big(\overline{Q_0}\cdot\overline{Q_1}\Big)^{\frac{q-1}{2}}}{M(\widetilde{f})P_t^{\frac{\Phi(\widetilde{f})}{2}}G(\widetilde{f})^{\frac{q^{d_t(e_t-1)}-1}{2}}} \pmod{\widetilde{f}}\\ &\equiv \frac{M(\widetilde{f})\cdot G(\widetilde{f})^{\frac{q^{d_te_t}-1}{2}}}{M(\widetilde{f})P_t^{\frac{\Phi(\widetilde{f})}{2}}G(\widetilde{f})^{\frac{q^{d_t(e_t-1)}-1}{2}}} \pmod{\widetilde{f}}\\ &\equiv \frac{G(\widetilde{f})^{\frac{1}{2}q^{d_t(e_t-1)}(q^{d_t}-1)}}{P_t^{\frac{\Phi(\widetilde{f})}{2}}} \pmod{\widetilde{f}}. \end{aligned}$$

By Theorem 3.1, this completes the proof. □

Now, we first address the case when f has exactly two prime divisors.

Theorem 4.8. *Assume that q is odd, and $f\in\mathbb{A}$ is a polynomial having the prime factorization as in (2.1) with $t=2$. Then, if one of the following two conditions holds:*

(1) $q\equiv 1 \pmod 4$,
(2) $q\equiv 3 \pmod 4$ *and both* $\deg P_1$ *and* $\deg P_2$ *are even,*

we have

$$G(f,S)\equiv\Big(\frac{P_1}{P_2}\Big) \pmod f;$$

otherwise, we have

$$G(f,S) \not\equiv \pm 1 \pmod{f}.$$

Proof. First, since q is odd and $t=2$, by (4.1) and (4.3) we have

$$G(f,S) = \delta(S)^{\frac{\Phi(f)}{q-1}} M(f) = M(f). \tag{4.10}$$

Put $d_j = \deg P_j, j = 1,2$. By Lemma 4.7, we have

$$\begin{aligned} M(f) &\equiv (-1)^{\frac{(q-1)d_2}{2}} P_2^{-\frac{\Phi(P_1^{e_1})}{2}} \pmod{P_1} \\ &\equiv (-1)^{\frac{(q-1)d_2}{2}} \left(\frac{P_2}{P_1}\right)^{-1} \pmod{P_1} \\ &\equiv (-1)^{\frac{(q-1)d_2}{2}} \left(\frac{P_2}{P_1}\right) \pmod{P_1}. \end{aligned}$$

From (4.4), we know that $M(f)^2 \equiv 1 \pmod{P_1^{e_1}}$. So, applying Lemma 4.5 we get

$$M(f) \equiv (-1)^{\frac{(q-1)d_2}{2}} \left(\frac{P_2}{P_1}\right) \pmod{P_1^{e_1}}. \tag{4.11}$$

By symmetry, we have

$$M(f) \equiv (-1)^{\frac{(q-1)d_1}{2}} \left(\frac{P_1}{P_2}\right) \pmod{P_2^{e_2}}. \tag{4.12}$$

Now, assume that either $q \equiv 1 \pmod 4$, or $q \equiv 3 \pmod 4$ and both d_1 and d_2 are even. Then, by the reciprocity law (Lemma 2.4) we obtain

$$\left(\frac{P_2}{P_1}\right) = \left(\frac{P_1}{P_2}\right),$$

and thus

$$M(f) \equiv \left(\frac{P_1}{P_2}\right) \qquad \pmod{P_1^{e_1}} \text{ and } \pmod{P_2^{e_2}}.$$

Using the Chinese Remainder Theorem, we get

$$M(f) \equiv \left(\frac{P_1}{P_2}\right) \qquad \pmod{f}. \tag{4.13}$$

So, by (4.10) we have

$$G(f,S) \equiv \left(\frac{P_1}{P_2}\right) \qquad \pmod{f}.$$

In all other cases, one can similarly see that the product of the right-hand sides of (4.11) and (4.12) is equal to -1. Hence, applying again the Chinese Remainder Theorem, we can conclude the proof. □

Finally, the case when f has more than two prime divisors is much easier.

Theorem 4.9. *Assume that q is odd. If $f \in \mathbb{A}$ is a polynomial having the prime factorization as in (2.1) with $t \geq 3$, then we have*

$$G(f,S) \equiv 1 \pmod{f}.$$

Proof. By Lemma 4.7, we have

$$\begin{aligned} M(f) &\equiv P_t^{-\frac{\Phi\left(P_1^{e_1}P_2^{e_2}\cdots P_{t-1}^{e_{t-1}}\right)}{2}} \pmod{P_1} \\ &\equiv \left(\frac{P_t}{P_1}\right)^{-\Phi\left(P_2^{e_2}\cdots P_{t-1}^{e_{t-1}}\right)} \pmod{P_1} \\ &\equiv 1 \pmod{P_1}. \end{aligned}$$

From (4.4), we know that $M(f)^2 \equiv 1 \pmod{P_1^{e_1}}$. So, applying Lemma 4.5 we get

$$M(f) \equiv 1 \pmod{P_1^{e_1}}.$$

By symmetry, we have

$$M(f) \equiv 1 \pmod{P_j^{e_j}} \quad \text{for } 2 \leq j \leq t.$$

So, by the Chinese Remainder Theorem we obtain

$$M(f) \equiv 1 \pmod{f}. \tag{4.14}$$

Noticing $G(f,S) = \delta(S)^{\frac{\Phi(f)}{q-1}} M(f) = M(f)$, we complete the proof. □

Acknowledgements

The authors are very grateful to the referee for careful reading and useful comments. The research of the first author was supported by National Natural Science Foundation of China Grant No.11526119, and the second author was supported by the Australian Research Council Grant DP130100237.

References

[1] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen I, II*, Math. Zeit., **19** (1924), 153–246.
[2] M. Bhargava, *The factorial function and generalizations*, Amer. Math. Monthly, **107** (2000), 783–799.
[3] J. B. Cosgrave and K. Dilcher, *Extensions of the Gauss–Wilson theorem*, Integers, **8** (2008), A39, available at http://www.integers-ejcnt.org/vol8.html.
[4] J. B. Cosgrave and K. Dilcher, *Mod p^3 analogues of theorems of Gauss and Jacobi on binomial coefficients*, Acta Arith., **142** (2010), 103–118.

[5] J. B. Cosgrave and K. Dilcher, *The multiplicative orders of certain Gauss factorials*, Int. J. Number Theory, **7** (2011), 145–171.
[6] J. B. Cosgrave and K. Dilcher, *An introduction to Gauss factorials*, Amer. Math. Monthly, **118** (2011), 812–829.
[7] J. B. Cosgrave and K. Dilcher, *The Gauss–Wilson theorem for quarter–intervals*, Acta Math. Hungar., **142** (2014), 199–230.
[8] J. B. Cosgrave and Karl Dilcher, *A role for generalized Fermat numbers*, Math. Comp., DOI:http://dx.doi.org/10.1090/mcom/3111.
[9] G. A. Miller, *A new proof of the generalized Wilson's theorem*, Ann. Math., **4** (1903), 188–190.
[10] L. J. Mordell, *The congruence* $(p-1/2)! \equiv \pm 1(\pmod p)$, Amer. Math. Monthly, **68** (1961), 145–146.
[11] M. Rosen, *Number theory in function fields*, Springer-Verlag, New York, 2002.
[12] The PARI Group, PARI/GP version `2.7.5`, Bordeaux, 2015, http://pari.math.u-bordeaux.fr/.

School of Mathematical Sciences, Qufu Normal University, Qufu Shandong, 273165, China
E-mail address: lxiumei2013@hotmail.com

School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia
E-mail address: shamin2010@gmail.com