Annales Mathematicae Silesianae **25** (2011), 49–57
Prace Naukowe Uniwersytetu Śląskiego nr 2944, Katowice

AN ELEMENTARY PROOF OF THE d-TH POWER RECIPROCITY LAW OVER FUNCTION FIELDS

Anna Blaszczok

Abstract. This paper generalises the proof of quadratic reciprocity law in $\mathbb{F}_q[T]$ presented by Chun-Gang Ji and Yan Xue [2] to the case of d-th power residues, where d divides the order of $\mathbb{F}_q^*$. Using only elementary properties of finite fields and basic number-theoretic tools we show that if $P, Q \in \mathbb{F}_q[T]$ are distinct irreducible polynomials then

$$\left(\frac{P}{Q}\right)_d = (-1)^{\frac{q-1}{d}\deg(P)\deg(Q)} \left(\frac{Q}{P}\right)_d,$$

where $\left(\frac{P}{Q}\right)_d$ is the d-th power residue symbol.

1. Introduction

Let $\mathbb{F}_q[T]$ be the polynomial ring in one variable over the finite field $\mathbb{F}_q$ with q elements. Every element in $\mathbb{F}_q[T]$ has the form

$$f(T) = \alpha_n T^n + \alpha_{n-1} T^{n-1} + \cdots + \alpha_1 T + \alpha_0,$$

where $n = \deg(f)$ and $\alpha_i \in \mathbb{F}_q$, $\alpha_n \neq 0$.

The leading coefficient α_n of polynomial f will be denoted by $\operatorname{sgn}(f)$. In particular, if $\operatorname{sgn}(f) = 1$, we say that f is a *monic* polynomial. We assume

Received: 20.12.2010. Revised: 25.11.2011.
(2010) Mathematics Subject Classification: 11T55, 11A15.
Key words and phrases: polynomial ring, d-th power residue, reciprocity law.

that $\operatorname{sgn}(0) = 0$ and $\deg(0) = -\infty$. If $f \in \mathbb{F}_q[T]$ is non-zero polynomial, set $|f| = q^{\deg(f)}$. If $f = 0$, set $|f| = 0$.

Let $P \in \mathbb{F}_q[T]$ be an irreducible polynomial, d be a natural number greater than 1 and $g \in \mathbb{F}_q[T]$ be not divisible by P. We say that g is a *d-th power residue modulo P* if the congruence $X^d \equiv g \pmod P$ has a solution in $\mathbb{F}_q[T]$, equivalently if $g + (P)$ is a d-th power in the field $\mathbb{F}_q[T]/(P)$.

In the case of $d = 2$ we also say that g is a *quadratic residue* modulo P. If g is not a quadratic residue modulo P and $\gcd(P, g) \sim 1$ then we say that g is a *quadratic nonresidue* modulo P.

PROPOSITION 1.1. *Let $P \in \mathbb{F}_q[T]$ be an irreducible polynomial and $g \in \mathbb{F}_q[T]$ be not divisible by P. Further, let d and n be natural numbers such that $d \neq 1$ and $n = \gcd(d, |P| - 1)$. Then g is a d-th power residue modulo P if and only if*

$$g^{\frac{|P|-1}{n}} \equiv 1 \pmod P.$$

PROOF. It is a simple generalization of Proposition 1.10 of [5] in the case of power residues modulo irreducible polynomial. □

Let $d \neq 1$ divide the order of $\mathbb{F}_q^*$. In this case, a very useful tool in the theory of power residues is a power residue symbol.

Let P be a monic irreducible polynomial in $\mathbb{F}_q[T]$. Then for every $g \in \mathbb{F}_q[T]$ there exists a unique element $\left(\frac{g}{P}\right)_d \in \mathbb{F}_q$ such that

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

The function $\left(\frac{\cdot}{P}\right)_d : \mathbb{F}_q[T] \to \mathbb{F}_q$ is called a *d-th power residue symbol*.

PROPOSITION 1.2. *Let $P \in \mathbb{F}_q[T]$ be a monic irreducible polynomial and $g, h \in \mathbb{F}_q[T]$. Then*

(1) *if $h \equiv g \pmod P$ then $\left(\frac{h}{P}\right)_d = \left(\frac{g}{P}\right)_d$,*

(2) $\left(\frac{gh}{P}\right)_d = \left(\frac{g}{P}\right)_d \left(\frac{h}{P}\right)_d$,

(3) *g is a d-th power residue modulo P if and only if $\left(\frac{g}{P}\right)_d = 1$,*

(4) $\left(\frac{g}{P}\right)_d = \left(\frac{g}{P}\right)_{q-1}^{\frac{q-1}{d}}$.

PROOF. Properties 1, 2 and 4 follow directly from the definition of power residue symbol. The equivalence in 3 follows from the fact that if $d|(q-1)$ then proposition 1.1 implies that g is a d-th power residue modulo P if and only if $g^{\frac{|P|-1}{d}} \equiv 1 \pmod P$. □

It is easy to prove that the non-zero values of the d-th power residue symbol are d-th roots of the unity in $\mathbb{F}_q$. In particular, if $d = 2$ then from item 3 of the above proposition we obtain that

$$\left(\frac{f}{P}\right)_2 = \begin{cases} 1, & \text{if } f \text{ is a quadratic residue modulo } P, \\ -1, & \text{if } f \text{ is a quadratic nonresidue modulo modulo } P, \\ 0, & \text{if } P \text{ divides } f, \end{cases}$$

which property is analogous to the definition of Legendre symbol for integers. For this ring, one of the most important tools of the quadratic residues theory is reciprocity law, which states the relation between the Legendre symbols involving two odd primes.

Fifty-six years after the publication by Gauss of his first proof of quadratic reciprocity law, Dedekind in [3] stated an analogous law over function fields. In polynomial rings over finite fields, unlike in the case of integers, it is possible to prove reciprocity law more general than quadratic without using advanced tools and theories.

THEOREM 1.3 (Reciprocity law). *Let P and Q be distinct monic irreducible polynomials in $\mathbb{F}_q[T]$. Then*

$$\left(\frac{P}{Q}\right)_d = (-1)^{\frac{q-1}{d}\deg(P)\deg(Q)} \left(\frac{Q}{P}\right)_d.$$

Leonard Carlitz thought he was the first to prove the generalization of quadratic reciprocity law over function fields (see [1]). However O. Ore pointed out that F.K. Schmidt had published the result before Carlitz. Since the 1930s Carlitz has published several proofs of general reciprocity law. One of his proofs, that relies only on properties of the finite fields, is included by Michael Rosen in [5].

The main aim of this paper is to present an elementary proof of Theorem 1.3 which was created by analogy to the quadratic reciprocity law's proof given by Chun-Gang Ji and Yan Xue in [2]. We will use only basic number-theoretic tools and elementary properties of finite fields.

2. The proof of the reciprocity law

In the proof of the reciprocity law, we will use the following lemmas.

LEMMA 2.1. *Let $g_1, \ldots, g_n \in \mathbb{F}_q[T]$ be pairwise relatively prime polynomials of positive degrees and let $g = g_1 \cdot \ldots \cdot g_n$.*
If $\Phi\colon \mathbb{F}_q[T]/(g) \to \mathbb{F}_q[T]/(g_1) \times \ldots \times \mathbb{F}_q[T]/(g_n)$ is given by

$$\Phi\left(f + (g)\right) = \left(f + (g_1), \ldots, f + (g_n)\right),$$

then the restriction of Φ to the group $U(\mathbb{F}_q[T]/(g))$ of units of the ring $\mathbb{F}_q[T]/(g)$ is an isomorphism of the groups $U(\mathbb{F}_q[T]/(g))$ and

$$U(\mathbb{F}_q[T]/(g_1)) \times \ldots \times U(\mathbb{F}_q[T]/(g_n)).$$

PROOF. See Corollary of Proposition 1.4 in [2]. □

LEMMA 2.2. *If F is a finite field then*

$$\prod_{\alpha \in F^*} \alpha = -1.$$

PROOF. If F is a finite field with n elements and K is its subfield, then the polynomial $X^n - X \in K[X]$ factors over F as

$$X^n - X = \prod_{\alpha \in F} (X - \alpha)$$

(for the proof see Lemma 2.4 in [4]). The formula in the lemma follows by dividing both sides of the above equality by the monomial X and setting $X = 0$. □

LEMMA 2.3. *If P is an irreducible polynomial of degree m, then*

$$\prod_{\substack{g \in \mathbb{F}_q[T] \\ 0 \le \deg(g) < m}} g \equiv -1 \,(\mathrm{mod}\, P).$$

PROOF. The congruence follows immediately from previous lemma considered for $F = \mathbb{F}_q[T]/(P)$. □

PROOF OF THEOREM 1.3. Let P and Q be distinct monic and irreducible polynomials. Then from part 4 of Proposition 1.2 it follows that it is enough to show that

$$\left(\frac{P}{Q}\right)_{q-1} = (-1)^{\deg(P)\deg(Q)} \left(\frac{Q}{P}\right)_{q-1}.$$

For the proof we introduce some useful notation. Let $f \in \mathbb{F}_q[T]$ be a monic polynomial of positive degree. Set

$$\mu(f) = \{g \in \mathbb{F}_q[T] : 0 \le \deg(g) < \deg(f)\}$$

and

$$\mu_\beta(f) = \{g \in \mu(f) : \operatorname{sgn}(f) = \beta\} \quad \text{for every } \beta \in \mathbb{F}_q^*.$$

Then $|\mu(f)| = |f| - 1$ and $|\mu_\beta(f)| = \frac{|f|-1}{q-1}$, for every $\beta \in \mathbb{F}_q^*$.

Let for every pair $(v, w) \in \mu(P) \times \mu_1(Q)$ element $k_{v,w} \in \mathbb{F}_q[T]$ be a polynomial of a degree smaller than $\deg(PQ)$ such that

$$\begin{cases} k_{v,w} \equiv v \pmod P, \\ k_{v,w} \equiv w \pmod Q. \end{cases}$$

From Lemma 2.1 it follows that such a polynomial exists and is unique. Moreover, since a given polynomial g represents a unit in $\mathbb{F}_q[T]/(PQ)$ if and only if $(g, PQ) \sim 1$, polynomials $k_{v,w}$ and PQ are relatively prime.

Observe that, if $(v, w), (v_1, w_1) \in \mu(P) \times \mu_1(Q)$ and $(v, w) \ne (v_1, w_1)$ then $\beta k_{v,w} \ne \gamma k_{v_1,w_1}$ for every $\beta, \gamma \in \mathbb{F}_q^*$. Indeed, if $\beta k_{v,w} = \gamma k_{v_1,w_1}$ then

$$\begin{cases} \beta v \equiv \gamma v_1 \pmod P, \\ \beta w \equiv \gamma w_1 \pmod Q. \end{cases}$$

Since $\deg(\beta v)$, $\deg(\gamma v_1) < \deg(P)$ and $\deg(\beta w)$, $\deg(\gamma w_1) < \deg(Q)$, we get that $\beta v = \gamma v_1$ and $\beta w = \gamma w_1$. Moreover polynomials w and w_1 are monic, so $\gamma = \beta$ and $(v, w) = (v_1, w_1)$.

For every $(v, w) \in \mu(P) \times \mu_1(Q)$ set $k^*_{v,w} = \beta k_{v,w}$, where $\beta = (\operatorname{sgn}(k_{v,w}))^{-1}$. Then $\operatorname{sgn}(k_{v,w})^* = 1$ and by our above observation

$$\begin{aligned} (1) \qquad |\{k^*_{v,w} : v \in \mu(P), w \in \mu_1(Q)\}| &= |\mu(P) \times \mu_1(Q)| \\ &= (|P| - 1) \cdot \frac{1}{q-1}(|Q| - 1). \end{aligned}$$

We will show that for a certain $\gamma \in \mathbb{F}^*$ we have

$$\begin{aligned} (2) \qquad (-1)^{\frac{|Q|-1}{q-1}} \left(\frac{Q}{P}\right)^{-1}_{q-1} &\equiv \prod_{\substack{f \in \mu_1(PQ) \\ \gcd(f, PQ) \sim 1}} f \equiv \gamma \prod_{\substack{v \in \mu(P) \\ w \in \mu_1(Q)}} k_{v,w} \\ &\equiv \gamma (-1)^{\frac{|Q|-1}{q-1}} \pmod P \end{aligned}$$

and

$$(3)\qquad (-1)^{\frac{|P|-1}{q-1}}\left(\frac{P}{Q}\right)_{q-1}^{-1} \equiv \prod_{\substack{f\in\mu_1(PQ)\\ \gcd(f,PQ)\sim 1}} f \equiv \gamma \prod_{\substack{v\in\mu(P)\\ w\in\mu_1(Q)}} k_{v,w}$$
$$\equiv \gamma(-1)^{\frac{|Q|-1}{q-1}\frac{|P|-1}{q-1}}(-1)^{\frac{|P|-1}{q-1}} (\mathrm{mod}\, Q).$$

From these congruences

$$\left(\frac{P}{Q}\right)_{q-1}^{-1} = \left(\frac{Q}{P}\right)_{q-1}^{-1} (-1)^{\frac{|Q|-1}{q-1}\frac{|P|-1}{q-1}}.$$

Then

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

which equality, as we observed, it is sufficient to show.

For the proof of congruences (2) and (3), set

$$\mathcal{F}_1 = \{k_{v,w}^* : v\in\mu(P), w\in\mu_1(Q)\},$$
$$\mathcal{F}_2 = \{f\in\mu_1(PQ) : \gcd(f,PQ)\sim 1\},$$

and

$$\mathcal{F}_3 = \{f\in\mu_1(PQ) : \gcd(f,P)\sim 1\}\setminus\{f\in\mu_1(PQ) : Q|f\}.$$

It is easy to show that $\mathcal{F}_1\subseteq\mathcal{F}_2=\mathcal{F}_3$.

Since $\{f\in\mathbb{F}_q[T] : 0\le\deg(f)<\deg(PQ), \gcd(f,PQ)\sim 1\}$ is the set of representatives for $U(\mathbb{F}_q[T]/(PQ))$, from Lemma 2.1 and equality (1) we obtain

$$|\mathcal{F}_2| = \frac{1}{q-1}|U(\mathbb{F}_q[T]/(PQ))|$$
$$= \frac{1}{q-1}|U(\mathbb{F}_q[T]/(P))||U(\mathbb{F}_q[T]/(Q))|$$
$$= \frac{1}{q-1}(|P|-1)(|Q|-1) = |\mathcal{F}_1|.$$

Thus, finally $\mathcal{F}_1=\mathcal{F}_2=\mathcal{F}_3$.

From the equality of sets $\mathcal{F}_1$, $\mathcal{F}_2$ and by the definition of polynomials $k^*_{v,w}$ we obtain identity

$$\prod_{\substack{f\in\mu_1(PQ)\\ \gcd(f,PQ)\sim 1}} f = \prod_{\substack{v\in\mu(P)\\ w\in\mu_1(Q)}} k^*_{v,w} = \gamma \prod_{\substack{v\in\mu(P)\\ w\in\mu_1(Q)}} k_{v,w} \tag{4}$$

for a certain $\gamma \in \mathbb{F}_q^*$.

Identity $\mathcal{F}_2 = \mathcal{F}_3$ shows that

$$\prod_{\substack{f\in\mu_1(PQ)\\ \gcd(f,PQ)\sim 1}} f = \prod_{\substack{f\in\mu_1(PQ)\\ \gcd(f,P)\sim 1}} f \Big/ \prod_{\substack{g\in\mu_1(PQ)\\ Q|g}} g. \tag{5}$$

By Lemma 2.3 we have

$$\begin{aligned}\prod_{\substack{f\in\mu_1(PQ)\\ \gcd(f,P)\sim 1}} f &= \prod_{f\in\mu_1(P)} f \prod_{\substack{b\in\mu_1(Q)\\ h\in\mu(P)}} (bP+h) \equiv \prod_{f\in\mu_1(P)} f\left(\prod_{h\in\mu(P)} h\right)^{|\mu_1(Q)|} \\ &\equiv \prod_{f\in\mu_1(P)} f(-1)^{\frac{|Q|-1}{q-1}} \pmod P.\end{aligned} \tag{6}$$

Furthermore

$$\begin{aligned}\prod_{\substack{g\in\mu_1(PQ)\\ Q|g}} g &= \prod_{f\in\mu_1(P)} fQ = Q^{\frac{|P|-1}{q-1}} \prod_{f\in\mu_1(P)} f \\ &\equiv \left(\frac{Q}{P}\right)_{q-1} \prod_{f\in\mu_1(P)} f \pmod P.\end{aligned} \tag{7}$$

From (5), (6) and (7) we obtain

$$\prod_{\substack{f\in\mu_1(PQ)\\ \gcd(f,PQ)\sim 1}} f \equiv (-1)^{\frac{|Q|-1}{q-1}} \left(\frac{Q}{P}\right)^{-1}_{q-1} \pmod P. \tag{8}$$

Similarly

$$\prod_{\substack{f\in\mu_1(PQ)\\ \gcd(f,PQ)\sim 1}} f \equiv (-1)^{\frac{|P|-1}{q-1}} \left(\frac{P}{Q}\right)^{-1}_{q-1} \pmod Q. \tag{9}$$

By the definition of polynomials $k_{v,w}$ and Lemma 2.3 we obtain that

$$\prod_{\substack{v\in\mu(P)\\ w\in\mu_1(Q)}} k_{v,w} \equiv \left(\prod_{v\in\mu(P)} v\right)^{\frac{|Q|-1}{q-1}} \equiv (-1)^{\frac{|Q|-1}{q-1}} \pmod{P} \tag{10}$$

and

$$\prod_{\substack{w\in\mu_1(Q)\\ v\in\mu(P)}} k_{v,w} \equiv \left(\left(\prod_{w\in\mu_1(Q)} w\right)^{q-1}\right)^{\frac{|P|-1}{q-1}} \pmod{Q}. \tag{11}$$

Since for every $\beta \in \mathbb{F}_q^*$ we have

$$\prod_{w\in\mu_\beta(Q)} w = \beta^{\frac{|Q|-1}{q-1}} \prod_{w\in\mu_1(Q)} w,$$

from congruence (11) we obtain that

$$\begin{aligned}\prod_{\substack{w\in\mu_1(Q)\\ v\in\mu(P)}} k_{v,w} &= \left(\prod_{\beta\in\mathbb{F}_q^*}\left(\beta^{-\frac{|Q|-1}{q-1}} \prod_{w\in\mu_\beta(Q)} w\right)\right)^{\frac{|P|-1}{q-1}}\\ &\equiv \left(\prod_{\beta\in\mathbb{F}_q^*}\beta\right)^{-\frac{|Q|-1}{q-1}\frac{|P|-1}{q-1}} \left(\prod_{w\in\mu(Q)} w\right)^{\frac{|P|-1}{q-1}} \pmod{Q}.\end{aligned}$$

Hence, by Lemmas 2.2 and 2.3 we have

$$\prod_{\substack{w\in\mu_1(Q)\\ v\in\mu(P)}} k_{v,w} = (-1)^{\frac{|Q|-1}{q-1}\frac{|P|-1}{q-1}} (-1)^{\frac{|P|-1}{q-1}} \pmod{Q}. \tag{12}$$

Finally, from (8), (4) and (10) we obtain congruence (2) and from (9), (4) and (12) we have (3), which, as we observed, was sufficient to complete the proof. □

References

[1] Caritz L., *The arithmetic of polynomials in a Galois field*, Amer. J. Math. **54** (1932), 39–50.
[2] Chun-Gang J., Yan X., *An elementary proof of the law of quadratic reciprocity over function fields*, Proc. Amer. Math. Soc. **136** (2008), no. 9, 3035–3039.
[3] Dedekind R., *Abriss einer Theorie der höheren Congruenzen in Bezug auf einer rellen Primzahl-Modulus*, J. Reine Angew. Math. **54** (1857), 1–26.
[4] Lidl R., Niederreiter H., *Finite fields*, Cambridge University Press, Cambridge, 2008.
[5] Rosen M., *Number theory in function fields*, Springer-Verlag, New York, 2002.

Institute of Mathematics
Silesian University
Bankowa 14
40-007 Katowice
Poland
e-mail: ablaszczok@math.us.edu.pl