PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 126, Number 3, March 1998, Pages 647–652
S 0002-9939(98)04582-1

ON CERTAIN CHARACTER SUMS OVER $\mathbb{F}_q[T]$

CHIH-NUNG HSU

(Communicated by Dennis A. Hejhal)

ABSTRACT. Let $\mathbb{F}_q$ be the finite field with q elements and let $\mathbf{A}$ denote the ring of polynomials in one variable with coefficients in $\mathbb{F}_q$. Let P be a monic polynomial irreducible in $\mathbf{A}$. We obtain a bound for the least degree of a monic polynomial irreducible in $\mathbf{A}$ (q odd) which is a quadratic non-residue modulo P. We also find a bound for the least degree of a monic polynomial irreducible in $\mathbf{A}$ which is a primitive root modulo P.

1. Introduction

In [1], on the assumption of the Extended Riemann Hypothesis, Ankeny proved that the least positive quadratic non-residue of the prime k is $\mathrm{O}((\log k)^2)$ and the least positive primitive root $(\bmod\, k)$ is $\mathrm{O}\{(2^{\nu(k-1)}\log k(\log 2^{\nu(k-1)}\log k))^2\}$, where $\nu(k-1)$ denotes the number of distinct prime factors of $k-1$.

Let $\mathbb{F}_q$ be the finite field with q elements and let $\mathbf{A}$ denote the ring of polynomials in one variable with coefficients in $\mathbb{F}_q$. Let P be a monic irreducible in $\mathbf{A}$. In this note, we establish the following results:

(1) When q is odd, the least degree of a monic irreducible in $\mathbf{A}$ which is a quadratic non-residue modulo P is less than $2+2\log_q(1+\deg P)$ (corollary 2.2). In fact, this result is deduced from a more general situation (proposition 2.1).

(2) The least degree of a monic irreducible in $\mathbf{A}$ which is a primitive root modulo P is $\mathrm{O}(\frac{\deg P}{\log_q \deg P})$ (theorem 3.1). Moreover, if $\frac{q^{\deg P}-1}{q-1}$ is a prime number, then the least degree of a monic irreducible primitive root modulo P is less than $8+2\log_q \deg P$ (proposition 3.1).

The above results will be deduced from a character sum estimate (theorem 2.1) due to Effinger and Hayes [3], Chapter 5.

2. The least positive quadratic non-residues

Let $\mathbb{F}_q$ denote the finite field with q elements and let $\mathbf{A}$ denote the ring of polynomials in one variable T with coefficients in $\mathbb{F}_q$. We denote by $\mathbf{A}_+$ the set consisting of all positive (monic) polynomials in $\mathbf{A}$, and by $\mathbf{A}_+^{(n)}$ the set consisting of all positive polynomials in $\mathbf{A}_+$ of degree n. We may write any element f of $\mathbf{A}$ in the

Received by the editors August 20, 1996.
1991 *Mathematics Subject Classification.* Primary 11A07; Secondary 11L40, 11N05.
Key words and phrases. Riemann Hypothesis, quadratic non-residues, primitive roots.

form

$$f = \sum_{i=0}^{d} a_i T^i \quad \text{with} \quad a_i \in \mathbb{F}_q \quad \text{and} \quad a_d \neq 0.$$

The degree of f is defined by $\deg f = d$, and the valuation of f is defined by $|f| = q^d$.

It is known that the number π_n of all positive irreducibles in $\mathbf{A}_+$ of degree n satisfies

$$\frac{q^n}{n} - q^{\frac{n}{2}} + 1 \leq \pi_n \leq \frac{q^n}{n}. \tag{1}$$

Suppose that Δ is a positive polynomial in $\mathbf{A}_+$. A character χ modulo Δ is a group homomorphism $\chi : (\mathbf{A}/\Delta)^\times \to \mathbb{C}^\times$. We define $\chi(f) = 0$ if $(f, \Delta) \neq 1$ and define $\pi_n(\chi)$ by

$$\pi_n(\chi) = \sum_{\text{irreducible } P \in \mathbf{A}_+^{(n)}} \chi(P).$$

These characters modulo Δ can be identified as the idele class characters of Dirichlet type for the rational function field $\mathbb{F}_q(T)$ (cf. [3], Exercise 2 of Section 5.1).

Theorem 2.1. *Let χ be a non-trivial character modulo Δ. Then*

$$|\pi_n(\chi)| \leq (\deg \Delta + 1) \cdot \frac{q^{\frac{n}{2}}}{n}.$$

Proof. Let $m(\chi)$ be the conductor of the idele class character χ. It follows from [3], Exercise 2 of Section 5.1, that $m(\chi) \mid \infty\Delta$ if χ is ramified at ∞ and $m(\chi) \mid \Delta$ if χ is unramified at ∞. From [3], theorem 5.7, we know that

$$|\pi_n(\chi)| \leq \{\deg m(\chi) - \lambda(\chi) + 2\} \cdot \frac{q^{\frac{n}{2}}}{n},$$

where $\lambda(\chi) = 2$ if χ is ramified at ∞ and $\lambda(\chi) = 1$ if χ is unramified at ∞. This completes the proof. ∎

Theorem 2.2. *Let χ be a non-trivial character modulo Δ and let the complex number ξ with $|\xi| = 1$ be a value of the character χ. If a positive integer n satisfies*

$$n \geq \begin{cases} 1 + 2\log_q \frac{1+\deg\Delta}{\sqrt{q}-2} & \textit{for} \quad q \geq 5, \\ 2 + 2\log_q(1 + \deg\Delta) & \textit{for} \quad q = 3, 4, \\ 5 + 2\log_q(1 + \deg\Delta) & \textit{for} \quad q = 2, \end{cases}$$

there then exists at least one positive irreducible P in $\mathbf{A}_+^{(n)}$ such that $(P, \Delta) = 1$ and $\chi(P) \neq \xi$.

Proof. Suppose that $\chi(P) = \xi$ for all positive irreducible P in $\mathbf{A}$ with $\deg P = n$ and $(P, \Delta) = 1$. By the assumption, we have

$$\pi_n - \deg\Delta \leq |\pi_n(\chi)|.$$

Using (1), we get

$$\frac{q^n}{n} - q^{\frac{n}{2}} - \deg\Delta < \pi_n - \deg\Delta,$$

and by theorem 2.1, we obtain

$$|\pi_n(\chi)| \leq (\deg \Delta + 1) \cdot \frac{q^{\frac{n}{2}}}{n}.$$

Combining these, we obtain (under the above assumption)

$$\frac{q^n}{n} - q^{\frac{n}{2}} - \deg \Delta < (\deg \Delta + 1) \cdot \frac{q^{\frac{n}{2}}}{n}. \tag{2}$$

If $n \geq 1 + 2\log_q \frac{1+\deg \Delta}{\sqrt{q}-2}$ and $q \geq 5$, then we have

$$\frac{1+\deg \Delta}{q^{\frac{n}{2}}} \leq \frac{\sqrt{q}-2}{\sqrt{q}} \leq 1, \quad q^{\frac{n-1}{2}} \geq n.$$

This implies that

$$\begin{aligned} \frac{q^{\frac{n}{2}}}{n} - 1 - \frac{\deg \Delta}{q^{\frac{n}{2}}} &\geq \frac{(\sqrt{q}-2) \cdot q^{\frac{n-1}{2}}}{n} + \left(2 \cdot \frac{q^{\frac{n-1}{2}}}{n} - 2\right) \\ &\geq \frac{1+\deg \Delta}{n} + 0 \geq (\deg \Delta + 1) \cdot \frac{1}{n}. \end{aligned}$$

Thus we obtain

$$\frac{q^n}{n} - q^{\frac{n}{2}} - \deg \Delta \geq (\deg \Delta + 1) \cdot \frac{q^{\frac{n}{2}}}{n}.$$

This contradicts (2); hence it contradicts the assumption. There thus exists at least one positive irreducible P in $\mathbf{A}_+^{(n)}$ such that $(P, \Delta) = 1$ and $\chi(P) \neq \xi$. The proofs of the other cases are similar. $\square$

Corollary 2.1. *Let χ be a non-trivial character modulo Δ. If $q \geq 5$ and $\deg \Delta \leq q - 2\sqrt{q} - 1$, then there exists at least one positive irreducible P in $\mathbf{A}_+^{(2)}$ such that $\chi(P) \neq 1$.*

Proof. This follows immediately from theorem 2.2. $\square$

If $\Delta = P$ is a positive irreducible in $\mathbf{A}_+$, we then have the following:

Proposition 2.1. *Let χ be a non-trivial character modulo P and let the complex number ξ with $|\xi| = 1$ be a value of the character χ. If a positive integer n satisfies*

$$n \geq \begin{cases} 1 + 2\log_q \frac{1+\deg P}{\sqrt{q}-1} & \textit{for} \quad q \geq 4, \\ 2 + 2\log_q(1 + \deg P) & \textit{for} \quad q = 3, \\ 4 + 2\log_q(1 + \deg P) & \textit{for} \quad q = 2, \end{cases} \tag{3}$$

there then exists at least one positive irreducible P' in $\mathbf{A}_+^{(n)}$ such that $P' \neq P$ and $\chi(P') \neq \xi$.

Proof. The proof is a modification of the proof of theorem 2.2. $\square$

Corollary 2.2. *Let P be a positive irreducible in $\mathbf{A}_+$ (q odd). If n satisfies the condition* (3)*, then there exists at least one positive irreducible in $\mathbf{A}_+$ of degree n which is a quadratic non-residue modulo P and at least one positive irreducible in $\mathbf{A}_+$ of degree n which is a quadratic residue modulo P.*

Proof. In proposition 2.1, let χ be the quadratic symbol for $\mathbf{A}$ (cf. [2]). The corollary then follows immediately. $\square$

Corollary 2.3. *Let P be a positive irreducible in $\mathbf{A}_+$, and let the positive integer d divide $|P|-1$. If n satisfies the condition* (3), *there then exists at least one positive irreducible in $\mathbf{A}_+$ of degree n which is a d-th power non-residue modulo P.*

Proof. Since the unit group $(\mathbf{A}/P\mathbf{A})^\times$ is a cyclic group, its character group is cyclic of order $|P|-1$. This corollary then follows immediately from $d \mid |P|-1$ and proposition 2.1. $\square$

Let norm be the norm homomorphism of $(\mathbf{A}/P\mathbf{A})^\times$ onto $\mathbb{F}_q^\times$, where P is a positive irreducible in $\mathbf{A}_+$. Let $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ be any non-trivial character. Then, by proposition 2.1, we also have

Corollary 2.4. *If n satisfies the condition* (3), *there then exists at least one positive irreducible P' in $\mathbf{A}_+$ of degree n such that $\chi \circ \mathrm{norm}(P') \neq 1$.*

3. The least positive primitive roots

Let P be a positive irreducible in $\mathbf{A}_+$ with $\deg P \geq 2$. We say that a polynomial P' is a primitive root modulo P if $\bar{P}'$ is a generator of the cyclic group $(\mathbf{A}/P\mathbf{A})^\times$, where $\bar{P}'$ is the canonical image of P' in $\mathbf{A}/P\mathbf{A}$. The purpose of this section is to find a bound for the least degree of a positive irreducible primitive root modulo P.

Theorem 3.1. *There exists a positive number c such that for any positive irreducible P in $\mathbf{A}_+$, if $n \geq c \cdot \frac{\deg P}{\log_q \deg P}$, one can find at least one positive irreducible of degree n which is a primitive root modulo P.*

Proof. Since $(\mathbf{A}/P\mathbf{A})^\times$ is a cyclic group of order $|P|-1$, the group C_P consisting of all characters modulo P is also a cyclic group of order $|P|-1$.

If m is a positive integer such that $m \mid (|P|-1)$, then it is known that for any $P' \in \mathbf{A}$

$$\sum_{\chi \in C_P,\, \chi^m = \chi_0} \chi(P') = \begin{cases} m & \text{if } P'^{\frac{|P|-1}{m}} \equiv 1 \pmod{P}, \\ 0 & \text{otherwise,} \end{cases}$$

where χ_0 is the trivial character modulo P. We define

$$\begin{aligned} S_m(n) &= \frac{1}{m} \sum_{\chi \in C_P,\, \chi^m = \chi_0} \; \sum_{\text{irreducible } P' \in \mathbf{A}_+^{(n)}} \chi(P') \\ &= \frac{\pi_n(\chi_0)}{m} + \frac{1}{m} \sum_{\chi_0 \neq \chi \in C_P,\, \chi^m = \chi_0} \; \sum_{\text{irreducible } P' \in \mathbf{A}_+^{(n)}} \chi(P'). \end{aligned} \tag{4}$$

Using equation (4) and theorem 2.1, we obtain

$$
\begin{aligned}
\sum_{\substack{\text{irreducible } P'\in\mathbf{A}_+^{(n)} \\ P' \text{ is primitive modulo } P}} 1 &= \sum_{m\,|\,(|P|-1)} \mu(m) S_m(n) \\
&= \pi_n(\chi_0) \sum_{m\,|\,(|P|-1)} \frac{\mu(m)}{m} \\
&\quad + \sum_{m\,|\,(|P|-1)} \frac{\mu(m)}{m} \sum_{\chi_0\neq\chi\in C_P,\,\chi^m=\chi_0} \sum_{\text{irreducible } P'\in\mathbf{A}_+^{(n)}} \chi(P') \qquad (5) \\
&\geq \frac{\phi(|P|-1)}{|P|-1}\cdot\pi_n(\chi_0) - \sum_{\text{squarefree } m\,|\,(|P|-1)} (\deg P+1)\cdot\frac{q^{\frac{n}{2}}}{n}.
\end{aligned}
$$

From [4], Chapter XXII, there exist two positive numbers c_1 and c_2 such that the number of primes $m \mid (|P|-1)$ is less than $\frac{c_1\cdot\deg P}{\log_q \deg P}$ and

$$\frac{\phi(|P|-1)}{|P|-1} \geq \frac{c_2}{\log_q \deg P}.$$

Combining these with (1), we obtain

$$
\begin{aligned}
&\sum_{\substack{\text{irreducible } P'\in\mathbf{A}_+^{(n)} \\ P' \text{ is primitive modulo } P}} 1 \\
&\geq \frac{c_2}{\log_q \deg P}\cdot\left\{\frac{q^n}{n} - q^{\frac{n}{2}}\right\} - 2^{\frac{c_1\cdot\deg P}{\log_q \deg P}}\cdot(\deg P+1)\cdot\frac{q^{\frac{n}{2}}}{n} \\
&= \frac{q^{\frac{n}{2}}}{n\cdot\log_q \deg P}\cdot\left\{c_2\cdot q^{\frac{n}{2}} - c_2\cdot n - 2^{\frac{c_1\cdot\deg P}{\log_q \deg P}}\cdot(\deg P+1)\log_q \deg P\right\}.
\end{aligned}
$$

Hence there exists a positive number c such that, if $n \geq c\cdot\frac{\deg P}{\log_q \deg P}$, then there is at least one positive irreducible of degree n which is a primitive root modulo P. $\square$

Proposition 3.1. *Let P be a positive irreducible in $\mathbf{A}_+$ such that*

$$\frac{|P|-1}{q-1}$$

is a prime number. If positive integer n satisfies

$$n \geq \begin{cases} 4+2\log_q(1+\deg P) & \text{for} \quad q\geq 3, \\ 8+2\log_q(1+\deg P) & \text{for} \quad q=2, \end{cases}$$

there then exists at least one positive irreducible of degree n which is a primitive root modulo P.

Proof. By (5), (1) and the inequality

$$\frac{\phi(|P|-1)}{|P|-1} \geq \frac{1}{q},$$

we have

$$
\begin{aligned}
&\sum_{\substack{\text{irreducible } P'\in\mathbf{A}_{+}^{(n)}\\ P' \text{ is primitive modulo } P}} 1\\
&\geq \frac{\phi(|P|-1)}{|P|-1}\cdot\pi_n(\chi_0) - \sum_{\text{squarefree } m\,|\,|P|-1}(\deg P+1)\cdot\frac{q^{\frac{n}{2}}}{n}\\
&\geq \frac{1}{q}\cdot\left(\frac{q^n}{n}-q^{\frac{n}{2}}\right) - q\cdot(\deg P+1)\cdot\frac{q^{\frac{n}{2}}}{n} > 0.
\end{aligned}
$$

This completes the proof. □

Acknowledgements

The author would like to thank the referees for their useful suggestions.

References

[1] N. C., Ankeny 'The Least Quadratic Non Residue', Annals of Mathematics, Vol 55, No. 1 (1952), pp. 65-72. MR **13:**538c

[2] E. Artin, 'Quadratische Körper im Gebiete der höheren Kongruenzen I, II', Math. Zeitschrift 19 (1924), pp. 153-246.

[3] G. W. Effinger and D. R. Hayes, 'Additive Number Theory of Polynomials Over a Finite Field', Oxford, Clarendon Press (1991). MR **92k:**11103

[4] G. H. Hardy and E. M. Wright, 'An Introduction to the Theory of Numbers', Oxford, Clarendon Press (1945). MR **16:**673c (3rd ed.)

[5] S. A. Stepanov, 'Arithmetic Of Algebraic Curves', Translated from Russian by Irene Aleksanova, Plenum Publishing Corporation (1994). MR **95j:**11055

Department of Mathematics, National Taiwan Normal University, 88 Sec. 4 Ting-Chou Road, Taipei, Taiwan

E-mail address: `maco@math.ntnu.edu.tw`