[8] E. G. Whitehead, *The Ramsey number* $N(3, 3, 3, 3; 2)$, Discrete Mathematics, 4(1973), pp. 389–396.

[9] S. Znám, *Generalization of a number-theoretical result*, Mat.-Fyz. Časopis Sloven. Akad. Vied. 16 (1966), pp. 357–361.

[10] — *On k-thin sets and n-extensive graphs*, Mat. -Fyz. Časopis Sloven. Akad. Vied. 17(1967), pp. 297–307.

UNIVERSITY OF GLASGOW
Glasgow, Scotland
UNIVERSITY OF SALFORD
Salford, M5 4WT
U.K.

Received on 6. 7. 1972 (306)

ACTA ARITHMETICA
XXV (1973)

Factorization of irreducible polynomials over a finite field with the substitution $x^{q^r} - x$ for x

by

ANDREW F. LONG (Greensboro, N.C.)

1. Introduction. Let $GF(q)$ denote the finite field of order $q = p^n$, where p is an arbitrary prime and $n \geqslant 1$. $Q(x)$ will denote an irreducible polynomial of degree s over $GF(q)$. For convenience we assume $Q(x)$ monic throughout the paper.

It is well known ([3], p. 34) that if $Q(x)$ is irreducible of degree s over $GF(q)$, then $Q(x^p - x)$ is also irreducible over $GF(q)$ if the coefficient β of x^{s-1} in $Q(x)$ satisfies

$$\sum_{j=0}^{n-1} \beta^{p^j} \neq 0. \tag{1.1}$$

On the other hand if the sum in (1.1) is equal to zero, $Q(x^p - x)$ is the product of p irreducible factors each of degree s over $GF(q)$. It has also been shown ([4], p. 307) that $Q(x^{q^s} - x)$ is the product of p^{ns-1} irreducibles each of degree ps over $GF(q)$ with no restrictions on β. The purpose of this present paper is to describe the irreducible factors of $Q(x^{q^r} - x)$ over $GF(q)$ for an arbitrary positive integer r. The principal results are contained in the following two theorems from § 5:

Let

$$N(s, q) = \sum_{ij=s} \mu(i) q^j$$

where μ is the Möbius function, and let

$$Q_s(x) = \sum_{j=0}^{s-1} x^{q^{dj}}$$

where $d = (r, s)$.

THEOREM 1. *Let $Q(x)$ be irreducible of degree s over $GF(q)$. Let $(r, s) = d$, and let $s/d = s'$ and $r/d = r'$. If $Q(x) | Q_{s'}(x)$ then $Q(x^{q^r} - x)$ is the product over $GF(q)$ of irreducibles of degree st, $t | r'$. The number of irreducibles of*

degree st is

$$\sum_{\substack{v|d \\ (t,\,d/v)=1}} N(vt, q)/t$$

for each $t|r'$.

THEOREM II. *Let* $Q(x)$ *be irreducible of degree* s *over* GF(q). *Let* $(r, s) = d$, *and let* $s/d = s'$ *and* $r/d = r'$. *Let* $r' = p^k l$, $(p, l) = 1$ *and* $k \geqslant 0$. *If* $Q(x) \nmid \varrho_{s'}(x)$, *then* $Q(x^{q^r} - x)$ *is the product over* GF(q) *of irreducibles of degree* $p^{k+1}st$, $t|l$. *For each* $t|l$, *the number of irreducibles of degree* $p^{k+1}st$ *is*

$$\sum_{\substack{v|D \\ (t,\,D/v)=1}} N(vt, q)/p^{k+1}t$$

where $D = p^k d$.

2. Some preliminary concepts and theorems. Most of these results are found in [1], [4], and [5].

DEFINITION 2.1. If α is contained in GF(q^s) but is not contained in GF(q^t), $1 \leqslant t < s$, then s is called the *degree of* α *relative to* GF(q).

We use notation $\deg \alpha = s$.

THEOREM 2.1. *The number* $N(s, q)$ *of elements of* GF(q^s) *having degree* s *relative to* GF(q) *is given by*

$$N(s, q) = \sum_{ij=s} \mu(i) q^j$$

where μ *is the Möbius function.*

THEOREM 2.2. $Q(x)$ *is an irreducible polynomial of degree* s *over* GF(q) *if and only if*

$$Q(x) = \prod_{j=0}^{s-1} (x - \alpha^{q^j})$$

and $\deg \alpha = s$.

THEOREM 2.3. *Let* α *belong to* GF(q^s). *Then* $x^q - x = \alpha$ *is solvable in* GF(q^s) *if and only if*

$$\sum_{j=0}^{s-1} \alpha^{q^j} = 0.$$

THEOREM 2.4. GF(q^k) *is contained in* GF(q^m) *if and only if* k *divides* m.

DEFINITION 2.2. A polynomial of the form

$$f(x) = \sum_{i=0}^{s} a_i x^{q^i}$$

is called a *linear* polynomial [5].

Remark. The (ordinary) sum of two linear polynomials is a linear polynomial.

DEFINITION 2.3. Let $f(x)$ and $g(x)$ be linear polynomials. The symbolic product $f \cdot g$ is given by

$$f \cdot g(x) = f\big(g(x)\big).$$

In general the symbolic product is not commutative, but it is commutative if the a_i belong to GF(q).

DEFINITION 2.4. The linear polynomial

$$f(x) = \sum_{i=0}^{s} a_i x^{q^i}$$

is said to *correspond* to the ordinary polynomial

$$F(x) = \sum_{i=0}^{s} a_i x^i.$$

THEOREM 2.5. *If* $F(x)$ *and* $G(x)$ *are polynomials over* GF(q) *and if* $f(x)$ *and* $g(x)$ *are the corresponding linear polynomials, then the symbolic product* $f \cdot g(x)$ *corresponds to the ordinary product* $F(x)G(x)$.

THEOREM 2.6. *Let* α *be a root of the irreducible polynomial* $Q(x)$ *of degree* s *over* GF(q). *Let* $s = ds'$ *and let*

$$\varrho_{s'}(x) = \sum_{j=0}^{s'-1} x^{q^{dj}}.$$

Then $Q(x)$ *divides* $\varrho_{s'}(x)$ *if and only if* $\varrho_{s'}(\alpha) = 0$.

THEOREM 2.7. *Let* $Q(x)$ *be irreducible of degree* s *over* GF(q). *Then* $Q(x^{q^s} - x)$ *is the product of* p^{ns-1} *irreducible polynomials of degree* ps *over* GF(q).

3. Lemmas. The following lemmas will be required for the proofs of the theorems in § 4 and § 5.

LEMMA 3.1. *Let* λ *be of degree* s *over* GF(q) *and let* γ *be of degree* r *over* GF(q) *with* $(r, s) = 1$. *Then the degree of* $\lambda + \gamma$ *is* rs *over* GF(q).

Proof. Clearly the degree of $\lambda + \gamma$ is k, a divisor of rs. Thus $k = r_1 s_1$ where $r = r_1 r_2$ and $s = s_1 s_2$. Now let $\theta = \lambda + \gamma$. By Theorem 2.4,

$$\gamma^{q^{s_1 r}} = (\theta - \gamma)^{q^{s_1 r}} = \theta^{q^{s_1 r}} - \gamma^{q^{s_1 r}} = \theta^{q^{kr_2}} - \gamma = \theta - \gamma = \lambda.$$

Thus $s|s_1 r$ and hence $s|s_1$ since $(r, s) = 1$. Similarly $r|r_1$ and we conclude that $rs|k$. The conditions $rs|k$ and $k|rs$ imply $k = rs$.

LEMMA 3.2. *Let a be of degree s over $\mathrm{GF}(q)$ and let $s' = s/d$, where $d = (r, s)$. If*

$$\sum_{j=0}^{s'-1} a^{q^{dj}} = 0$$

then $x^{q^r} - x - a$ has a root λ belonging to $\mathrm{GF}(q^s)$.

Proof. Consider $(x^r - 1, x^s - 1) = x^d - 1$. There exist polynomials $A(x)$ and $B(x)$ such that

$$A(x)(x^r - 1) + B(x)(x^s - 1) = x^d - 1. \tag{3.1}$$

In terms of the corresponding linear polynomials (3.1) becomes

$$a(x)\cdot(x^{q^r} - x) + b(x)\cdot(x^{q^s} - x) = x^{q^d} - x, \tag{3.2}$$

where the symbolic multiplication commutes since the coefficients belong to $\mathrm{GF}(q)$.

By Theorem 2.3, with q replaced by q^d, $x^{q^d} - x = a$ has a solution ξ belonging to $\mathrm{GF}(q^{ds'}) = \mathrm{GF}(q^s)$. Substituting ξ in the identity (3.2) we obtain

$$a(\xi)\cdot(\xi^{q^r} - \xi) = \xi^{q^d} - \xi$$

or

$$[a(\xi)]^{q^r} - [a(\xi)] = a.$$

Since ξ belongs to $\mathrm{GF}(q^s)$, $a(\xi)$ also belongs to $\mathrm{GF}(q^s)$ by closure properties of the field operations. Thus $\lambda = a(\xi)$ is a root of $x^{q^r} - x - a$ belonging to $\mathrm{GF}(q^s)$.

LEMMA 3.3. *Let a be of degree s over $\mathrm{GF}(q)$ and let $s' = s/d$ where $d = (r, s)$. Suppose $r = p^k l d$, $(p, l) = 1$ and $k \geqslant 0$. If*

$$\sum_{j=0}^{s'-1} a^{q^{dj}} \neq 0$$

then $x^{q^r} - x - a$ has a root λ belonging to $\mathrm{GF}(q^{p^{k+1}s})$.

Proof. Observe that

$$(r, p^{k+1}s) = (p^k l d, p^{k+1}s'd) = p^k d$$

as $(l, ps') = 1$. Consider

$$(x^r - 1, x^{p^{k+1}s} - 1) = x^{p^k d} - 1.$$

There exist polynomials $A(x)$ and $B(x)$ such that

$$A(x)(x^r - 1) + B(x)(x^{p^{k+1}s} - 1) = x^{p^k d} - 1. \tag{3.3}$$

In terms of the corresponding linear polynomials (3.3) becomes

$$a(x)\cdot(x^{q^r} - x) + b(x)\cdot(x^{q^{p^{k+1}s}} - x) = x^{q^{p^k d}} - x. \tag{3.4}$$

We seek a solution ξ in $\mathrm{GF}(q^{p^{k+1}s})$ which satisfies

$$x^{q^{p^k d}} - x = a. \tag{3.5}$$

Let $P = q^{p^k}$. Then (3.5) becomes

$$x^{P^d} - x = a \tag{3.6}$$

which has a solution $\xi \in \mathrm{GF}(P^{dps'}) = \mathrm{GF}(P^{ps})$ by Theorem 2.3 since

$$\sum_{j=0}^{ps'-1} a^{P^{dj}} = p \sum_{j=0}^{s'-1} a^{P^{dj}} = 0.$$

Substituting ξ in the identity (3.4) we obtain

$$[a(\xi)]^{q^r} - [a(\xi)] = a,$$

where $\lambda = a(\xi)$ is a root of $x^{q^r} - x - a$ belonging to $\mathrm{GF}(q^{p^{k+1}s})$.

LEMMA 3.4. *Let $r = r'd$. Then the set*

$$\{tv\colon t|r',\ v|d,\ (t, d/v) = 1\}$$

contains each divisor of r exactly once.

Proof. Let k be a prime such that $k^e \| r$, ($k^e \| r$ denotes that e is the highest power of k dividing r). Then for some λ and δ, $k^\lambda \| r'$ and $k^\delta \| d$ with $\lambda + \delta = e$. For $t|r'$ and $v|d$, there exist τ and ν such that $k^\tau \| t$ and $k^\nu \| d$. We must show that $\{\tau + \nu\} = \{0, 1, \ldots, e\}$ with no repetitions.

The condition $(t, d/v) = 1$ implies that $\min(\tau, \delta - \nu) = 0$, and we have the following two mutually exclusive cases:

Case I: $\tau = 0$.

Case II: $\tau \neq 0$ and $\delta = \nu$.

For Case I, $\{\tau + \nu\} = \{\nu\colon \nu \leqslant \delta\} = \{0, 1, \ldots, \delta\}$.

For Case II, $\{\tau + \nu\} = \{\tau + \delta\colon 1 \leqslant \tau \leqslant \lambda\} = \{\delta + 1, \delta + 2, \ldots, \delta + \lambda\}$.

Since $\delta + \lambda = e$, we find on combining the two cases that

$$\{\tau + \nu\} = \{0, 1, \ldots, e\},$$

with each of the exponents occurring exactly once in the listing.

Since k was an arbitrary prime divisor of r, the result follows by the unique factorization theorem for integers.

LEMMA 3.5. *Let $r = p^k l d$ and let $p^k d = D$. Then the set*

$$[tv\colon t|l,\ v|D,\ (t, D/v) = 1\}$$

contains each divisor of r exactly once.

Proof. Replace d by D and r' by l in Lemma 3.4.

4. Theorems involving the substitution $x^{q^r} - x$ with $(r, s) = 1$. Theorems 4.1 and 4.2 contain results for $(r, s) = 1$; they are special cases of Theo-

rems 5.3 and 5.4 where $(r, s) = d$. It is instructive however to consider the proofs for $(r, s) = 1$ separately.

THEOREM 4.1. *Let $Q(x)$ be irreducible of degree s over $\mathrm{GF}(q)$ with the coefficient β of x^{s-1} satisfying $\beta = 0$. If $(r, s) = 1$, then $Q(x^{q^r} - x)$ is the product over $\mathrm{GF}(q)$ of irreducibles of degree st, $t|r$. For each $t|r$ the number of irreducibles of degree st is*

$$N(t, q)/t.$$

Remark. Note that $N(t, q)/t$ is the number of monic irreducible polynomials of degree t over $\mathrm{GF}(q)$ where $N(t, q)$ is defined as in Theorem 2.1.

Proof. By Theorem 2.2,

$$Q(x) = \prod_{j=0}^{s-1} (x - \alpha^{q^j}) \qquad (\deg \alpha = s). \tag{4.1}$$

Substituting $x^{q^r} - x$ for x, (4.1) becomes

$$Q(x^{q^r} - x) = \prod_{j=0}^{s-1} (x^{q^r} - x - \alpha^{q^j}). \tag{4.2}$$

Take $j = 0$. The polynomial $x^{q^r} - x - \alpha$ has a root λ not belonging to $\mathrm{GF}(q^r)$ such that

$$\lambda^{q^r} = \lambda + \alpha. \tag{4.3}$$

Raising (4.3) to successive powers of q^r, we obtain the sequence of equations:

$$\begin{aligned} \lambda^{q^r} &= \lambda + \alpha, \\ \lambda^{q^{2r}} &= \lambda + \alpha + \alpha^{q^r}, \\ &\cdots\cdots\cdots\cdots \\ \lambda^{q^{sr}} &= \lambda + \sum_{j=0}^{s-1} \alpha^{q^{rj}} = \lambda, \end{aligned} \tag{4.4}$$

since

$$\sum_{j=0}^{s-1} \alpha^{q^{rj}} = \sum_{j=0}^{s-1} \alpha^{q^j}$$

when $(r, s) = 1$. Now (4.4) implies that the degree of λ is at most sr. Since α is a polynomial in λ, Theorem 2.4 implies that $s|\deg\lambda$. Hence the degree of λ has the form st, $t|r$, for any root λ of (4.3).

By Lemma 3.2 a root of (4.3) of minimum degree s does occur; denote this root by λ_1. Then all the linear factors of $Q(x^{q^r} - x)$ over $\mathrm{GF}(q^{sr})$ can be represented in terms of λ_1 as follows:

If λ_1 is a root of (4.3), so is $\lambda_1 + \gamma$, $\gamma \in \mathrm{GF}(q^r)$. Thus

$$x^{q^r} - x - \alpha = \prod_{\gamma \in \mathrm{GF}(q^r)} [x - (\lambda_1 + \gamma)].$$

Consider the factor $x^{q^r} - x - \alpha^{q^j}$ of (4.2). Raising (4.3) to the q^jth power we obtain

$$(\lambda_1^{q^j})^{q^r} = \lambda_1^{q^j} + \alpha^{q^j}.$$

Thus $\lambda_1^{q^j}$ is a root of degree s over $\mathrm{GF}(q)$ of the polynomial $x^{q^r} - x - \alpha^{q^j}$. Hence

$$Q(x^{q^r} - x) = \prod_{\gamma \in \mathrm{GF}(q^r)} \prod_{j=0}^{s-1} [x - (\lambda_1^{q^j} + \gamma)]. \tag{4.5}$$

Let $\deg\gamma = t$, $t|r$. Now $(r, s) = 1$ implies $(t, s) = 1$. Since $\lambda_1^{q^j}$ has degree s, $0 \leqslant j \leqslant s-1$, Lemma 3.1 asserts that the degree of $\lambda_1^{q^j} + \gamma$ is st. For any $t|r$ the number $N(t, q)$ of γ in $\mathrm{GF}(q^r)$ of degree t is given by Theorem 2.1. Since st of the factors in (4.5) are required to form an irreducible of degree st, we obtain

$$sN(t, q)/st = N(t, q)/t$$

irreducibles of degree st for each $t|r$.

Note that the condition $\beta = 0$ in the hypothesis of Theorem 4.1 could be replaced by $Q(x)|\varrho_s(x)$ according to Theorem 2.6 and (4.4).

EXAMPLE 4.1. Let $Q(x) = x^3 + x + 1$, an irreducible over $\mathrm{GF}(2)$. Let $r = 2$. Since $\beta = 0$, Theorem 4.1 predicts $N(1, 2) = 2$ irreducibles of degree 3 and $N(2, 2)/2 = 1$ irreducible of degree 6 in the factorization of $Q(x^4 - x)$ over $\mathrm{GF}(2)$. We find that

$$Q(x^4 - x) = (x^3 + x + 1)(x^3 + x^2 + 1)(x^6 + x^5 + x^3 + x^2 + 1).$$

EXAMPLE 4.2. Let $Q(x) = x^5 + x^2 + 1$, an irreducible over $\mathrm{GF}(2)$. Let $r = 2$. Since $\beta = 0$, Theorem 4.1 predicts $N(1, 2) = 2$ irreducibles of degree 5 and $N(2, 2)/2 = 1$ irreducible of degree 10 in the factorization of $Q(x^4 - x)$ over $\mathrm{GF}(2)$. We find that

$$\begin{aligned} &Q(x^4 - x) \\ &= (x^5 + x^3 + x^2 + x + 1)(x^5 + x^4 + x^3 + x + 1)(x^{10} + x^9 + x^8 + x^4 + x^3 + x^2 + 1). \end{aligned}$$

THEOREM 4.2. *Let $Q(x)$ be irreducible of degree s over $\mathrm{GF}(q)$ with the coefficient β of x^{s-1} satisfying $\beta \neq 0$. If $(r, s) = 1$ then $Q(x^{q^r} - x)$ is the product over $\mathrm{GF}(q)$ of irreducibles of degree $p^{k+1}st$ where $t|l$ in the factorization $r = p^k l$, $(p, l) = 1$ and $k \geqslant 0$. The number of irreducibles of degree $p^{k+1}st$ is*

$$\sum_{u=0}^{k} N(p^u t, q)/p^{k+1}t$$

for each $t|l$.

Proof. By Theorem 2.2,

$$Q(x) = \prod_{j=0}^{s-1}(x-\alpha^{q^j}) \qquad (\deg\alpha = s) \tag{4.6}$$

and

$$Q(x^{q^r}-x) = \prod_{j=0}^{s-1}(x^{q^r}-x-\alpha^{q^j}). \tag{4.7}$$

Take $j=0$. The polynomial $x^{q^r}-x-\alpha$ has a root λ not belonging to $GF(q^r)$ such that

$$\lambda^{q^r} = \lambda+\alpha. \tag{4.8}$$

Now $\lambda^{q^{sr}} \neq \lambda$ since $\lambda^{q^{sr}} = \lambda+\sum_{j=0}^{s-1}\alpha^{q^{jr}} = \lambda-\beta$ and $\beta \neq 0$. The sequence of equations:

$$\begin{aligned} \lambda^{q^{sr}} &= \lambda-\beta,\\ \lambda^{q^{2sr}} &= \lambda-2\beta,\\ &\cdots\cdots\cdots\\ \lambda^{q^{psr}} &= \lambda-p\beta = \lambda, \end{aligned} \tag{4.9}$$

shows that the degree of λ is at most psr.

By (4.8) $s|\deg\lambda$ and thus $\deg\lambda = sm$ where $m|pr$. By (4.9) $\deg\lambda\nmid sr$ which means that $m\nmid r$. Thus $m = p^{k+1}t$ where p^k is the highest power of p dividing r, and $t|l$ in the factorization $r = p^k l$, $(p,l)=1$. Hence $\deg\lambda = p^{k+1}st$, $t|l$.

As in (4.4), $\sum_{j=0}^{s-1}\alpha^{q^j} = -\beta$ with $\beta\neq 0$, and by Lemma 3.3 a λ of minimum degree $p^{k+1}s$ does occur; call it λ_1. Then, as in the proof of Theorem 4.1,

$$Q(x^{q^r}-x) = \prod_{\gamma\in GF(q^r)}\prod_{j=0}^{s-1}[x-(\lambda_1^{q^j}+\gamma)]. \tag{4.10}$$

Let γ in $GF(q^r)$ have degree $p^u t$, $0\leqslant u\leqslant k$ and $t|l$. We show that $\lambda_1+\gamma$ has degree $p^{k+1}st$ over $GF(q)$. Let $0 = \lambda_1+\gamma$. The degree of 0 must be of the form $p^{k+1}st'$ where $t'|t$. Now $\gamma = 0-\lambda_1$ and

$$\gamma^{q^{p^{k+1}st'}} = 0^{q^{p^{k+1}st'}} - \lambda_1^{q^{p^{k+1}st'}} = 0-\lambda_1,$$

so that

$$\gamma^{q^{p^{k+1}st'}} = \gamma. \tag{4.11}$$

Thus $\deg\gamma | p^{k+1}st'$ and this implies that $t|p^{k+1-u}st'$. Now $(s,r)=1$ implies $(s,t)=1$, and $(p,l)=1 \to (p^{k+1-u},t)=1$. Therefore $(p^{k+1-u}s,t)=1$ and we conclude that $t|t'$. The conditions $t'|t$ and $t|t'$ imply that $t=t'$.

We remark that $\lambda_1^{q^j}+\gamma$, $1\leqslant j\leqslant s-1$, also has degree $p^{k+1}st$ over $GF(q)$ if γ has degree $p^u t$ over $GF(q)$.

Every element of $GF(q^r)$ has degree over $GF(q)$ of the form $p^u t$, $0\leqslant u\leqslant k$ and $t|l$. The number of γ of degree $p^u t$ is given by $N(p^u t, q)$ in Theorem 2.1. Thus in the factorization (4.10) we have

$$s\sum_{u=0}^{k} N(p^u t, q)/p^{k+1}st = \sum_{u=0}^{k} N(p^u t, q)/p^{k+1}t$$

irreducibles of degree $p^{k+1}st$ over $GF(q)$.

Note that the hypothesis $\beta\neq 0$ can be replaced by $Q(x)\nmid \varrho_s(x)$.

Example 4.3. Let $Q(x) = x^2+x+1$, the irreducible of degree 2 over $GF(2)$. Let $r=3$. Since $\beta\neq 0$, $k=0$ and $l=3$, Theorem 4.2 predicts $N(1,2)/2 = 1$ irreducible of degree 4 and $N(3,2)/6 = 1$ irreducible of degree 12 in the factorization of $Q(x^8-x)$ over $GF(2)$. Indeed the factorization is

$$Q(x^8-x) = (x^4+x+1)(x^{12}+x^9+x^8+x^6+x^3+x^2+1).$$

Example 4.4. Let $Q(x) = x^3+x^2+1$, an irreducible of degree 3 over $GF(2)$. Let $r=2$. Since $\beta\neq 0$, $k=1$ and $l=1$, Theorem 4.2 predicts $[N(1,2)+N(2,2)]/4 = 1$ irreducible of degree 12.

$$Q(x^4-x) = x^{12}+x^9+x^8+x^6+x^3+x^2+1,$$

an irreducible of degree 12 over $GF(2)$.

5. Theorems involving the substitution $x^{q^r}-x$ with $(r,s)=d$. Let $\varrho_{s'}(x)$ be defined as in Theorem 2.6.

Theorem 5.1. *Let $Q(x)$ be irreducible of degree s over $GF(q)$. Let $(r,s)=d$ and let $s/d=s'$ and $r/d=r'$. Suppose that $(r',d)=1$. If $Q(x)|\varrho_{s'}(x)$, then $Q(x^{q^r}-x)$ is the product over $GF(q)$ of irreducibles of degree st, $t|r'$. For each $t|r'$ the number of irreducibles of degree st is*

$$\sum_{v|d} N(vt, q)/t.$$

Proof. As in the proof of Theorem 4.1

$$Q(x^{q^r}-x) = \prod_{j=0}^{s-1}(x^{q^r}-x-\alpha^{q^j}) \qquad (\deg\alpha = s).$$

Take $j=0$. Observe that $x^{q^r}-x-\alpha$ has a root λ not belonging to $GF(q^r)$ such that

$$\begin{aligned} \lambda^{q^r} &= \lambda+\alpha,\\ \lambda^{q^{2r}} &= \lambda+\alpha+\alpha^{q^r},\\ &\cdots\cdots\cdots\cdots\\ \lambda^{q^{s'r}} &= \lambda+\sum_{j=0}^{s'-1}\alpha^{q^{rj}} = \lambda. \end{aligned} \tag{5.1}$$

This is a consequence of the hypothesis $Q(x)|\varrho_{s'}(x)$ which is equivalent by Theorem 2.6 to the condition

$$\sum_{j=0}^{s'-1} \alpha^{q^{rj}} = \sum_{j=0}^{s'-1} \alpha^{q^{dj}} = 0.$$

Since $s'r = sr'$, we see that $\deg\lambda | sr'$. Since α is a polynomial in λ we also have $s|\deg\lambda$. Hence the degree of λ has the form st where $t|r'$. Further, Lemma 3.2 guarantees that a λ of minimum degree s does occur; call it λ_1. Then, as in the proof of Theorem 4.1,

$$Q(x^{q^r}-x) = \prod_{\gamma\in \mathrm{GF}(q^r)} \prod_{j=0}^{s-1} [x-(\lambda_1^{q^j}+\gamma)]. \tag{5.2}$$

Let γ in $\mathrm{GF}(q^r)$ have degree vt, $v|d$ and $t|r'$. We show that $\lambda_1+\gamma$ has degree st. Let $\theta = \lambda_1+\gamma$. The degree of θ is of the form st', $t'|t$. Now $\gamma = \theta-\lambda_1$ and

$$\gamma^{q^{st'}} = \theta^{q^{st'}} - \lambda_1^{q^{st'}} = \theta-\lambda_1 = \gamma$$

so that $\deg\gamma | st'$. This condition implies that $vt|st'$, i.e. $t|t's'\dfrac{d}{v}$. Now $t|r'$ implies $(t, s') = 1$ as $(r', s') = 1$. Also $t|r'$ and $d/v|d$ implies $(t, d/v) = 1$ by our assumption that $(r', d) = 1$. Thus $(t, s'd/v) = 1$ and $t|t'$. The conditions $t|t'$ and $t'|t$ imply that $t = t'$.

We again note that $\lambda_1^{q^j}+\gamma$, $1\leqslant j\leqslant s-1$, also has degree st over $\mathrm{GF}(q)$ if γ has degree vt, $v|d$, over $\mathrm{GF}(q)$.

Every γ in $\mathrm{GF}(q^r)$ has degree of the form vt where $v|d$ and $t|r'$. The number of γ of degree vt is given by $N(vt, q)$ in Theorem 2.1. Since st of the factors in (5.2) are required to form an irreducible of degree st, we obtain

$$s\sum_{v|d} N(vt, q)/st = \sum_{v|d} N(vt, q)/t$$

irreducibles of degree st for each $t|r'$.

THEOREM 5.2. *Let $Q(x)$ be irreducible of degree s over $\mathrm{GF}(q)$. Let $(r, s) = d$, and let $s/d = s'$ and $r/d = r'$. Let $r' = p^k l$, $(p, l) = 1$ and $k\geqslant 0$. Suppose that $(l, d) = 1$. If $Q(x)\nmid \varrho_{s'}(x)$, then $Q(x^{q^r}-x)$ is the product over $\mathrm{GF}(q)$ of irreducibles of degree $p^{k+1}st$, $t|l$. For each $t|l$, the number of irreducibles of degree $p^{k+1}st$ is*

$$\sum_{v|D} N(vt, q)/p^{k+1}t \tag{5.3}$$

where $D = p^k d$.

Proof. As in the proof of Theorem 5.1,

$$Q(x^{q^r}-x) = \prod_{j=0}^{s-1} (x^{q^r}-x-\alpha^{q^j}) \quad (\deg\alpha = s).$$

Take $j = 0$. The polynomial $x^{q^r}-x-\alpha$ has a root λ not belonging to $\mathrm{GF}(q^r)$ such that

$$\lambda^{q^r} = \lambda+\alpha. \tag{5.4}$$

Now $\lambda^{q^{s'r}} \neq \lambda$ since

$$\lambda^{q^{s'r}} = \lambda + \sum_{j=0}^{s'-1} \alpha^{q^{dj}},$$

and by Theorem 2.6 the summation $\varrho_{s'}(\alpha)$ is not zero since $Q(x)\nmid\varrho_{s'}(x)$. The sequence of equations

$$\begin{aligned} \lambda^{q^{s'r}} &= \lambda+\varrho_{s'}(\alpha), \\ \lambda^{q^{2s'r}} &= \lambda+2\varrho_{s'}(\alpha), \\ &\cdots\cdots\cdots\cdots \\ \lambda^{q^{ps'r}} &= \lambda+p\varrho_{s'}(\alpha) = \lambda \end{aligned} \tag{5.5}$$

shows that $\deg\lambda | psr'$ since $s'r = sr'$.

By (5.4) $s|\deg\lambda$ and thus $\deg\lambda = sm$ where $m|pr'$. By (5.5) $\deg\lambda\nmid sr'$ which means that $m\nmid r'$. Hence $m = p^{k+1}t$ where p^k is the highest power of p dividing r', and $t|l$ in the factorization $r' = p^k l$, $(p, l) = 1$. Consequently $\deg\lambda = p^{k+1}st$, $t|l$.

By Lemma 3.3 a λ of minimum degree $p^{k+1}s$ does occur; call it λ_1. Then, as in the proof of Theorem 4.1,

$$Q(x^{q^r}-x) = \prod_{\gamma\in \mathrm{GF}(q^r)} \prod_{j=0}^{s-1} [x-(\lambda_1^{q^j}+\gamma)]. \tag{5.6}$$

Let $D = p^k d$. Suppose γ in $\mathrm{GF}(q^r)$ has degree vt where $v|D$ and $t|l$. We show that $\lambda_1+\gamma$ has degree $p^{k+1}st$ over $\mathrm{GF}(q)$. Let $\theta = \lambda_1+\gamma$. The degree of θ must be of the form $p^{k+1}st'$ where $t'|t$. Now $\gamma = \theta-\lambda_1$ and

$$\gamma^{q^{vp^{k+1}st'}} = \theta^{q^{vp^{k+1}st'}} - \lambda_1^{q^{vp^{k+1}st'}} = \theta-\lambda_1,$$

so that

$$\gamma^{q^{vp^{k+1}st'}} = \gamma.$$

Thus $\deg\gamma | p^{k+1}st'$, i.e.

$$vt | p^{k+1}st'. \tag{5.7}$$

Let $v = p^u v'$ where $(p, v') = 1$, $0\leqslant u\leqslant k$ and $v'|d$. Substituting this expression for v in (5.7) we obtain

$$t|p^{k+1-u}t's'\frac{d}{v'}. \tag{5.8}$$

Now $t|l$ and $(l, p) = 1$ imply $(t, p^{k+1-u}) = 1$. Since $t|l$ and d/v' divides d, the condition $(l, d) = 1$ implies $(t, d/v') = 1$. In addition $t|r'$ and $(r', s') = 1$

imply $(t, s') = 1$. Thus $\left(t, p^{k+1-u}d' \cdot \frac{d}{v'}\right) = 1$ and we conclude from (5.8) that $t|t'$. Hence the degree of $\lambda_1 + \gamma$ is $p^{k+1}st$.

Similarly $\lambda_1^{q^j} + \gamma$, $1 \leqslant j \leqslant s-1$, has degree $p^{k+1}st$ for γ of degree vt, $v|D$ and $t|l$.

Every element of $\mathrm{GF}(q^r)$ has degree over $\mathrm{GF}(q)$ of the form vt where $v|D$ and $t|l$. The number γ of degree vt is given by $N(vt, q)$ in Theorem 2.1. Thus in the factorization (5.5) we have

$$s \sum_{v|D} N(vt, q)/p^{k+1}st = \sum_{v|D} N(vt, q)/p^{k+1}t$$

irreducibles of degree $p^{k+1}st$ over $\mathrm{GF}(q)$.

Remark. It is interesting to note that if $(d, p) = 1$ (5.3) can be written in the form

$$\sum_{u=0}^{k} \sum_{v|d} N(p^u vt, q)/p^{k+1}t.$$

This is possible since $\{v: v|D = p^k d\} = \{p^u v: v|d \text{ and } 0 \leqslant u \leqslant k\}$ with no repetitions in the second set if $(p, d) = 1$.

Example 5.1. Let $Q(x) = x^3 + x + 1$, the irreducible over $\mathrm{GF}(2)$. Let $r = 4$. Here $(r, s) = 2$; in fact $s|r$ so that $s' = 1$ and

$$\sum_{j=0}^{s'-1} a^{q^{tj}} = a$$

where $a \neq 0$. Thus the hypothesis $Q(x) \nmid \varrho_{s'}(x)$ of Theorem 5.2 is satisfied, and we have $k = 1$, $l = 1$ and $d = 2$. Theorem 5.2 predicts $[N(1, 2) + N(2, 2) + N(4, 2)]/4 = 4$ irreducibles of degree 8 in the factorization of $Q(x^{16} - x)$ over $\mathrm{GF}(2)$. We find that

$$Q(x^{16} - x) = (x^8 + x^5 + x^3 + x + 1)(x^8 + x^5 + x^4 + x^3 + x^2 + x + 1) \times \\ \times (x^8 + x^6 + x^5 + x + 1)(x^8 + x^6 + x^5 + x^2 + 1).$$

Remark. The hypotheses $(r', d) = 1$ in Theorem 5.1 and $(l, d) = 1$ in Theorem 5.2 prevent these theorems from describing the most general case of unrestricted values of r. An examination of the proofs shows however that even if $(l, d) \neq 1$, irreducibles of the minimum degree must occur. That the formulas counting irreducibles in the preceding theorems are not correct for $(l, d) \neq 1$ is shown by the following problem:

Let $Q(x) = x^3 + x + 1$, an irreducible over $\mathrm{GF}(2)$. Thus $q = p = 2$ and $s = 3$. Let $r = 9$. Then $d = 3$, $k = 0$, and $l = 3$ so that $(l, d) = 3$. $Q(x) \nmid \varrho_3(x)$. For $t = 1$, the formula of Theorem 5.2 yields $[N(1, 2) + N(3, 2)]/2 = 4$ irreducibles of degree 6. For $t = 3$, the formula yields $[N(3, 2) + N(9, 2)]/6 = 85$ irreducibles of degree 18. The irreducibles of degree 6 and 18 in this count contribute a total degree of 1554 in the factorization of $Q(x^{2^9} - x)$. But $2^9 \cdot 3 = 1536$ is the correct degree of $Q(x^{2^9} - x)$.

Now $Q(x^{2^9} - x) \equiv Q(x^{2^3} - x) \bmod P$ when P is an irreducible of degree 6 over $\mathrm{GF}(2)$. All the sextic factors of $Q(x^{2^9} - x)$ are contained in the factorization of $Q(x^{2^3} - x)$. By Theorem 2.7, $Q(x^{2^3} - x)$ is the product of 4 irreducibles of degree 6. The remaining factors of $Q(x^{2^9} - x)$, which are of degree 18 by the proof of Theorem 5.2, must number 84. The counting formula gave 85, and it is easy to observe the reason for the inconsistency. $N(3, 2)$ appears in both the count for $t = 1$ and $t = 3$. It obviously belongs in the count for $t = 1$, and therefore should not be included in the count for $t = 3$. With the removal of the term $N(3, 2)$, we find that $N(9, 2)/6 = 84$, the correct number of irreducible factors of degree 18.

Theorem 5.3. *Let $Q(x)$ be irreducible of degree s over $\mathrm{GF}(q)$. Let $(r, s) = d$, and let $s/d = s'$ and $r/d = r'$. If $Q(x)|\varrho_{s'}(x)$, then $Q(x^{q^r} - x)$ is the product over $\mathrm{GF}(q)$ of irreducibles of degree st, $t|r'$. For each $t|r'$ the number of irreducibles of degree st is*

$$\sum_{\substack{v|d \\ (t, d/v)=1}} N(vt, q)/t. \tag{5.9}$$

Proof. This theorem is the same as Theorem 5.1 with the restriction $(r', d) = 1$ removed. An inspection of the proof of Theorem 5.1 reveals that $(r', d) = 1$ was used to obtain the condition $(t, d/v) = 1$ so that the degree of $\lambda_1^{q^j} + \gamma$ could be specified. But by Lemma 3.4 all divisors vt of r are included exactly once in the set

$$\left\{vt: t|r', v|d, \left(t, \frac{d}{v}\right) = 1\right\}.$$

Thus

$$s \sum_{t|r'} \sum_{\substack{v|d \\ (t, d/v)=1}} N(vt, q) = sq^r$$

accounts for all the linear factors of $Q(x^{q^r} - x)$. By the argument in the proof of Theorem 5.1, we find that the number of irreducibles of degree st, $t|r'$, is given by (5.9).

Theorem 5.4. *Let $Q(x)$ be irreducible of degree s over $\mathrm{GF}(q)$. Let $(r, s) = d$, and let $s/d = s'$ and $r/d = r'$. Let $r' = p^k l$, $(p, l) = 1$ and $k \geqslant 0$. If $Q(x) \nmid \varrho_{s'}(x)$, then $Q(x^{q^r} - x)$ is the product over $\mathrm{GF}(q)$ of irreducibles of degree $p^{k+1}st$, $t|l$. For each $t|l$ the number of irreducibles of degree $p^{k+1}st$ is*

$$\sum_{\substack{v|D \\ (t, D/v)=1}} N(vt, q)/p^{k+1}t, \tag{5.10}$$

where $D = p^k d$.

Proof. This theorem is the same as Theorem 5.2 with the restriction $(l, d) = 1$ removed. In the proof of Theorem 5.2 we used the condition $(l, d) = 1$ to imply that $(t, d/v') = 1$ in (5.8):

$$t | p^{k+1-u} t' s' \frac{d}{v'}.$$

Since $d/v' | D/v$, the condition $(t, D/v) = 1$ now implies $(t, d/v') = 1$. Thus we know as before that the degree of $\lambda + \gamma$ is $p^{k+1} st$. But by Lemma 3.5 all divisors vt of r are included exactly once in the set

$$\left\{ vt\colon\ t|l,\ v|D,\ \left(t, \frac{D}{v}\right) = 1 \right\}.$$

Thus by an argument similar to the proof of Theorem 5.2, we obtain (5.10) as the formula for the number of irreducibles of degree $p^{k+1} st$, $t|l$.

Remark. We note that if $(p, d) = 1$, (5.10) becomes

$$\sum_{u=0}^{k} \sum_{\substack{v|d \\ (t, \frac{d}{v}) = 1}} N(p^u vt, q)/p^{k+1} t.$$

As in the proof of Theorem 5.4, the condition $(t, d/v) = 1$ may be applied to

$$t | p^{k+1-u} s' t' \frac{d}{v} \qquad (v|d,\ t|l)$$

to conclude that $t' = t$. In the count of irreducibles of degree $p^{k+1} st$, Lemma 3.4 can then be applied to the divisors of ld without regard to the powers of p since $(d, p) = (l, p) = 1$ implies that $(ld, p) = 1$.

Corollary 5.1. *Let $Q(x)$ be irreducible of degree s over $\mathrm{GF}(q)$ with the coefficient β of x^{s-1} satisfying $\beta \neq 0$. Let $r|s$. Then $Q(x^{q^r} - x)$ is the product over $\mathrm{GF}(q)$ of irreducibles of degree ps. The number of irreducibles of degree ps is*

$$\sum_{v|r} N(v, q)/p.$$

Proof. Using the notation of Theorem 5.4, we see that $d = r$, $s = rs'$ and $r' = 1$. Now if α is a root of $Q(x)$,

$$-\beta = \sum_{j=0}^{s-1} \alpha^{q^j}.$$

The hypothesis $\beta \neq 0$ implies

$$\sum_{j=0}^{s'-1} \alpha^{q^{rj}} \neq 0, \tag{5.11}$$

for otherwise

$$-\beta = \sum_{j=0}^{s-1} \alpha^{q^j} = \sum_{i=0}^{r-1} \Big(\sum_{j=0}^{s'-1} \alpha^{q^{rj}} \Big)^{q^i} = 0.$$

By Theorem 2.6, (5.11) is equivalent to $Q(x) \nmid \varrho_{s'}(x)$ and the hypotheses of Theorem 5.4 are satisfied.

Remark. If $\beta = 0$ replaces $\beta \neq 0$ in Corollary 5.1, the hypotheses for either Theorem 5.3 or Theorem 5.4 may be satisfied. In particular if $\beta = 0$ and $s = s'$ (i.e. $r = 1$), then Theorem 5.3 applies. Example 5.2 shows however that the simultaneous conditions $\beta = 0$ and $Q(x) \nmid \varrho_{s'}(x)$ are possible.

Example 5.2. Let $Q(x) = x^4 + x + 1$, an irreducible over GF(2). Note that $\beta = 0$. Let $r = 2$.

$$Q(x^4 - x) = (x^8 + x^6 + x^5 + x^3 + 1)(x^8 + x^6 + x^5 + x^4 + x^3 + x + 1),$$

a product of two irreducibles of degree 8 over GF(2). Since this result is consistent with Theorem 5.4, but inconsistent with Theorem 5.3, we conclude that $Q(x) \nmid \varrho_{s'}(x)$ here.

Example 5.3. Let $Q(x) = x^4 + x^3 + 1$, an irreducible over GF(2). Here $\beta \neq 0$. Let $r = 2$. Corollary 5.1 predicts $[N(1, 2) + N(2, 2)]/2 = 2$ irreducibles of degree 8 in the factorization of $Q(x^4 - x)$ over GF(2). We find that

$$Q(x^4 - x) = (x^8 + x^5 + x^3 + x + 1)(x^8 + x^5 + x^4 + x^3 + x^2 + x + 1).$$

Corollary 5.2. *Let $Q(x)$ be irreducible of degree s over $\mathrm{GF}(q)$. Let $s|r$ so that $r = sr'$ with $r' = p^k l$, $(l, p) = 1$ and $k \geqslant 0$. Then $Q(x^{q^r} - x)$ is the product of irreducibles of degree $p^{k+1} st$, $t|l$. The number of irreducibles of degree $p^{k+1} st$ is*

$$\sum_{\substack{v|D \\ (t, D/v) = 1}} N(vt, q)/p^{k+1} t,$$

where $D = p^k s$.

Proof. Using the notation of Theorem 5.4, we have $d = s$ and $s' = 1$. Thus if α is a root of $Q(x)$

$$\sum_{j=0}^{s'-1} \alpha^{q^{sj}} = \alpha.$$

Since $\alpha \neq 0$, Theorem 2.6 indicates that the hypothesis $Q(x) \nmid \varrho_{s'}(x)$ of Theorem 5.4 is satisfied.

Remark. If $r = s$ in Corollary 5.2, Theorem 2.7 is obtained.

Note that Example 5.3 is an illustration of Corollary 5.2. As another illustration we have

Example 5.4. Let $Q(x) = x^9 + x + 1$, an irreducible of degree $s = 9$ over GF(2). Let $r = 135$. Then $d = 9$, $s' = 1$, and $l = 15$.

For $t = 1$, there are $[N(1, 2) + N(3, 2) + N(9, 2)]/2$ irreducible factors of $Q(x^{2^{135}} - x)$ of degree 18. For $t = 3$, there are $N(27, 2)/6$ irreducibles of degree 54. For $t = 5$, there are $[N(5, 2) + N(15, 2) + N(45, 2)]/10$ irreducibles of degree 90, and for $t = 15$, there are $N(135, 2)/30$ irreducibles of degree 270. Since

$$s \sum_{t \mid 15} \sum_{\substack{n \mid 9 \\ (t, \frac{9}{n}) = 1}} N(nt, 2) = 9 \cdot 2^{135}$$

we see that all the irreducible factors are accounted for.

References

[1] L. Carlitz, Unpublished notes for a course in Arithmetic of Polynomials.

[2] R. Church, *Tables of irreducible polynomials for the first four prime moduli*, Ann. of Math. 36 (1935), pp. 198–209.

[3] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Leipzig 1901.

[4] A. F. Long, *Classification of irreducible factorable polynomials over a finite field*, Acta Arith. 12(1967), pp. 301–313.

[5] O. Ore, *Contributions to the theory of finite fields*, Trans. Amer. Math. Soc. 36 (1934), pp. 243–274.

UNIVERSITY OF NORTH CAROLINA
Greensboro, North Carolina

Received on 24. 8. 1972 (318)

ACTA ARITHMETICA
XXV (1973)

Über die arithmetische Natur der Werte der Lösungen einer Funktionalgleichung von H. Poincaré

von

R. Wallisser (Freiburg i. Br.)

1. Einleitung. In seiner Arbeit *Sur une classe nouvelle de transcendants uniformes* betrachtet Poincaré [6] Funktionen $f_1, \ldots, f_n$, die einem Multiplikationstheorem genügen: Es gibt eine komplexe Zahl m mit $|m| > 1$ und rationale Funktionen $R_i(x_1, \ldots, x_{n+1})$, $1 \leqslant i \leqslant n$, so daß

$$f_i(mz) = R_i\big(z, f_1(z), \ldots, f_n(z)\big) \tag{1}$$

gilt. Sind die Funktionen R_i Polynome, so sind die Lösungen eines solchen Systems ganze Funktionen und im allgemeinen ganz transzendent. Spezialfälle solcher Systeme sind Gleichungen der Form

$$f(m^p z) = R\big(z, f(z), f(mz), \ldots, f(m^{p-1}z)\big). \tag{2}$$

Insbesondere gehören die Lösungen der linearen Funktionalgleichung

$$f(m^p z) = P_0(z) f(m^{p-1}z) + \ldots + P_{p-1}(z) f(z) + P_p(z) \tag{3}$$

zu den Funktionen dieser Art. Dabei sind $P_0, \ldots, P_p$ Polynome.

Es fehlt nicht an Untersuchungen arithmetischer Eigenschaften von Funktionen, die einer linearen homogenen Gleichung der Form (3) genügen. Am umfassendsten dürfte die Arbeit von Osgood [4] sein, der im Falle von Polynomen aus dem Gaußschen Zahlkörper die simultane diophantische Approximation gewisser Funktionswerte von Lösungen einer Gleichung (3) untersucht. Hier soleen mit derselben Methode, mit der Gelfond [3] die Transzendenz von e^π bewies, die Werte gewisser Lösungen der Funktionalgleichung

$$f(mz) = P(z) f(z) + Q(z) \tag{4}$$

untersucht werden. Dabei seien P und Q Polynome mit Koeffizienten aus einem imaginär quadratischen Zahlkörper K. Die Methode besteht darin, f in eine geeignete Interpolationsreihe zu entwickeln und die Interpolationskoeffizienten zu analysieren. Es wird sich zeigen, daß man bei linearem P Irrationalitätsaussagen für die Werte der Lösungen solcher Gleichungen machen kann. Bei nichtlinearem P lassen sich jedoch nur