Congruences for Generalized Dickson Polynomials

Paul Thomas Young

University of Charleston, Charleston, SC 29424 USA

1 Introduction

If R is a commutative ring with identity and $a \in R$ the Dickson polynomials $g_n(x,a) \in R[x]$ may be defined explicitly by

$$g_n(x,a) = \sum_{k=0}^{[n/2]} \frac{n}{n-k} \binom{n-k}{k} (-a)^k x^{n-2k}. \tag{1.1}$$

These polynomials play several important roles in the the theory of finite fields, particularly in the study of permutation polynomials (cf. Mullen 1993) and of Kloosterman sums. These applications arise via the well-known functional equation

$$g_n\left(y + \frac{a}{y}, a\right) = y^n + \left(\frac{a}{y}\right)^n. \tag{1.2}$$

In this paper we study similar properties relating to generalizations of the Dickson polynomials, which are defined as the expansion coefficients of certain rational differential forms. We realize these differential forms as invariant differentials on one-dimensional commutative formal group laws (cf. Hazewinkel 1978, §5.8) over polynomial rings and p-adic integer rings. This connection to formal group theory expresses itself in congruences for these expansion coefficients in characteristic zero. By reduction modulo prime powers we obtain identities for the generalized Dickson polynomials over finite fields $R = \mathbf{F}_q$ and over Galois rings $R = GR(p^s, t)$.

In §§2,3 we treat the generalized Dickson polynomials as defined in Lidl and Niederreiter (1983), demonstrating their connection to the formal multiplicative group $\hat{\mathbf{G}}_m$. In §4 we show how the Dickson polynomials of the second kind $h_n(x,a)$ (over a p-adic field) arise from formal group laws attached to the L-series for quadratic characters, and deduce a partial factorization for $h_{mq-1}(x,a)$ over $\mathbf{F}_q$. Finally we combine these two types of results in §5 to demonstrate a formal group interpretation of the rational Rédei functions. In all cases we first obtain congruences in characteristic zero and deduce identities in positive characteristic.

Consider a polynomial

$$P(T) = 1 - x_1 T + x_2 T^2 + \cdots + (-1)^n x_n T^n + (-1)^{n+1} a T^{n+1} \tag{1.3}$$

with integer coefficients $x_1, ..., x_n, a$. Over some extension of $\mathbf{Q}$ this polynomial splits into the product

$$P(T) = \prod_{j=1}^{n+1} (1 - \alpha_j T). \tag{1.4}$$

It follows that $x_j = \sigma_j(\alpha_1, ..., \alpha_{n+1})$ for $1 \le j \le n$ and $a = \sigma_{n+1}(\alpha_1, ..., \alpha_{n+1})$, where σ_j denotes the j-th elementary symmetric function in $n+1$ indeterminates.

For $1 \le i \le n$ let $P^{(i)}(T)$ be the polynomial of degree $k = \binom{n+1}{i}$ with constant term 1 whose reciprocal roots are all products of the form $\alpha_{j_1} \cdots \alpha_{j_i}$ where $1 \le j_1 < \cdots < j_i \le n+1$. The coefficients of $P^{(i)}$ are symmetric functions of $\alpha_1, ..., \alpha_{n+1}$, and therefore there are integral polynomials $y_{j,i}$ in $x_1, ..., x_n, a$ such that

$$P^{(i)}(T) = 1 - y_{1,i} T + y_{2,i} T^2 + \cdots + (-1)^k y_{k,i} T^k, \tag{1.5}$$

with $y_{1,i} = x_i$ and $y_{k,i} = a^i$. If we now view $x_1, ..., x_n, a$ as indeterminates then $P^{(i)}(T) \in \mathbf{Z}[x_1, ..., x_n, a][T]$ for all i. The generalized Dickson polynomials $g_m^{(i)}$ (over $\mathbf{Z}$) are then defined by

$$\frac{dP^{(i)}}{P^{(i)}} = -\sum_{m=1}^{\infty} g_m^{(i)}(x_1, ..., x_n, a) T^m \frac{dT}{T}. \tag{1.6}$$

The usual Dickson polynomials (1.1) are obtained in this way from $P(T) = 1 - xT + aT^2$ with $i = n = 1$. If R is any commutative ring with identity we obtain generalized Dickson polynomials over R by specializing $a \in R$, although in §§3,4 we shall also specialize the x_i to elements of R. For $R = \mathbf{F}_q$ this definition agrees with that given in Lidl and Niederreiter (1983).

2 Polynomial Congruences

We begin these results with a congruence obtained from the functional equations of the generalized Dickson polynomials.

Theorem 1. *Let R be a commutative ring with identity and $a \in R$. Then for all primes p, all integers $m > 0$ and $1 \le i \le n$ we have*

$$g_{mp}^{(i)}(x_1, ..., x_n, a) \equiv g_m^{(i)}(x_1, ..., x_n, a)^p \pmod{pR[x_1, ..., x_n]}.$$

Proof. We define an R-algebra homomorphism

$$\varphi : R[x_1, ..., x_n] \longrightarrow R[y_1, ..., y_n, (y_1 \cdots y_n)^{-1}] \tag{2.1}$$

by requiring

$$\varphi(x_j) = \sigma_j(y_1, ..., y_n, a(y_1 \cdots y_n)^{-1}) \tag{2.2}$$

for $1 \leq j \leq n$, where σ_j is the j-th elementary symmetric function in $n+1$ indeterminates, and extending by R-linearity and multiplicativity. Both φ and the reduced map

$$\bar{\varphi} : (R/pR)[x_1, ..., x_n] \longrightarrow (R/pR)[y_1, ..., y_n, (y_1 \cdots y_n)^{-1}] \tag{2.3}$$

are injective. From the definition (1.5) of $P^{(i)}(T)$, we see that extending φ to a map from $R[x_1, ..., x_n][T]$ to $R[y_1, ..., y_n, (y_1 \cdots y_n)^{-1}][T]$ by $T \mapsto T$ yields

$$\varphi(P^{(i)}(T)) = \prod(1 - uT), \tag{2.4}$$

where the product is taken over all products of the form $u = y_{j_1} \cdots y_{j_i}$ where $1 \leq j_1 < \cdots < j_i \leq n+1$, with y_{n+1} taken to mean $a(y_1 \cdots y_n)^{-1}$. Therefore by (1.6) we have

$$\varphi(g_m^{(i)}(x_1, ..., x_n, a)) = \sigma_i(y_1^m, ..., y_n^m, a^m(y_1 \cdots y_n)^{-m}) \tag{2.5}$$

for all i, m (these are the functional equations). Then using the fact that $(\sum_i X_i)^p \equiv \sum_i X_i^p \mod p$ we see that

$$\bar{\varphi}(g_{mp}^{(i)}(x_1, ..., x_n, a)) = \bar{\varphi}(g_m^{(i)}(x_1, ..., x_n, a))^p. \tag{2.6}$$

Since $\bar{\varphi}$ is injective, the congruence follows.

It is well-known that $g_m^{(i)}(x_1, ..., x_n, a)$ is a permutation polynomial in n indeterminates over $\mathbf{F}_q$ if $(m, q^s - 1) = 1$ for $s = 1, 2, ..., n+1$ (cf. Lidl and Niederreiter 1983). As stated below, the above result implies that the set of generalized Dickson polynomials over $\mathbf{F}_q$ of this type is closed under postcomposition with the Frobenius $x \mapsto x^p$, where $q = p^f$.

Corollary 2. *If R has characteristic p then*

$$g_{mp}^{(i)}(x_1, ..., x_n, a) = g_m^{(i)}(x_1, ..., x_n, a)^p$$

in the polynomial ring $R[x_1, ..., x_n]$.

The following congruences express the formal group significance of the generalized Dickson polynomials.

Theorem 3. *Let R be a commutative ring with identity. Then for all primes p, all integers $m, r > 0$ and $1 \le i \le n$ we have*

$$g^{(i)}_{mp^r}(x_1, ..., x_n, a) \equiv g^{(i)}_{mp^{r-1}}(x_1^p, ..., x_n^p, a^p) \pmod{p^r R[x_1, ..., x_n, a]}.$$

Proof. Since the natural homomorphism $\mathbf{Z} \to R$ maps the ideal $p^r\mathbf{Z}$ to $p^r R$, it suffices to prove this when $R = \mathbf{Z}$. By comparing the expansions of $\omega = dP/P$ for the polynomials $P(T)$ and $P(x_1^{-1}T)$ we see that

$$g^{(1)}_m(x_1, ..., x_n, a) = x_1^m g^{(1)}_m(1, x_2x_1^{-2}, x_3x_1^{-3}, ..., x_nx_1^{-n}, ax_1^{-1-n}). \tag{2.7}$$

Now the differential form

$$\omega = \frac{d(1 - P(x_1^{-1}T))}{1 - (1 - P(x_1^{-1}T))} = \sum_{m=1}^{\infty} g^{(1)}_m(1, x_2x_1^{-2}, ..., ax_1^{-1-n})T^n \frac{dT}{T} \tag{2.8}$$

is the canonical invariant differential on a one-dimensional formal group law over the complete ring $\mathbf{Z}_p[x_1^{-1}, x_2, ..., x_n, a]$ which is strictly isomorphic over this ring to the formal multiplicative group $\hat{\mathbf{G}}_m$, whose invariant differential is $dT/(1 - T)$ (with $1 - P(x_1^{-1}T)$ being the isomorphism) (cf. Hazewinkel 1978, §5.8; Stienstra and Beukers 1985, Theorems A8, A9). Using the lifting of Frobenius given by

$$\sigma(h(x_1, ..., x_n, a)) = h(x_1^p, ..., x_n^p, a^p), \tag{2.9}$$

this implies the congruences

$$\begin{aligned} g^{(1)}_{mp^r}(1, x_2x_1^{-2}, ..., ax_1^{-1-n}) &\equiv \sigma(g^{(1)}_{mp^{r-1}}(1, x_2x_1^{-2}, ..., ax_1^{-1-n})) \\ &\pmod{p^r\mathbf{Z}_p[x_1^{-1}, ..., x_n, a]}. \end{aligned} \tag{2.10}$$

Multiplying by $x_1^{mp^r}$ and using (2.7) yields the desired congruence modulo $p^r\mathbf{Z}_p[x_1, ..., x_n, a]$ for $i = 1$, but both sides lie in $\mathbf{Z}[x_1, ..., x_n, a]$, giving the result for $i = 1$.

In general, for $1 \le i \le n$ we write $P^{(i)}(T)$ in the form (1.5). By comparing the expansions of $\omega = dP/P$ for the polynomials $P^{(i)}(T)$ and $P^{(i)}(x_i^{-1}T)$ we see that

$$\begin{aligned} g^{(i)}_m(x_1, ..., x_n, a) &= g^{(1)}_m(y_{1,i}, ..., y_{k-1,i}, a^i) \\ &= y_{1,i}^m g^{(1)}_m(1, y_{2,i}y_{1,i}^{-2}, ..., a^i y_{1,i}^{-k}). \end{aligned} \tag{2.11}$$

Then repeating the above argument with P and x_1 replaced by $P^{(i)}$ and x_i gives the result for general i.

We remark that if $q = p^f$, then f-fold iteration of these congruences yields

$$g^{(i)}_{mq^r}(x_1, ..., x_n, a) \equiv g^{(i)}_{mq^{r-1}}(x_1^q, ..., x_n^q, a^q) \pmod{pq^{r-1}R[x_1, ..., x_n, a]}. \tag{2.12}$$

Such congruences become identities in any ring R of characteristic dividing pq^{r-1}; in particular this is the case for the Galois ring $R = GR(p^s, t)$ whenever $r \geq 1 + (s-1)/t$.

3 Congruences for Values of Generalized Dickson Polynomials

In this section we let K be a finite extension of $\mathbf{Q}_p$ having uniformizing parameter π_K, residue-class field of cardinality $q = p^f$, and ramification index $e = e_K$ over $\mathbf{Q}_p$ defined by $(p) = (\pi_K)^e$. We assume also that the characteristic polynomial $P(T)$ has coefficients in the ring of integers $\mathcal{O}_K$ of K.

Theorem 4. *If $e \leq p-1$ then for all $x_1, ..., x_n, a \in \mathcal{O}_K$, all $m, r > 0$ and $1 \leq i \leq n$ we have*

$$g^{(i)}_{mq^r}(x_1, ..., x_n, a) \equiv g^{(i)}_{mq^{r-1}}(x_1, ..., x_n, a) \pmod{\pi_K q^{r-1}\mathcal{O}_K}.$$

Furthermore there exists an algebraic integer $H^{(i)}_m \in \mathcal{O}_K$, depending only on $x_1, ..., x_n, a \pmod{\pi_K \mathcal{O}_K}$, m, and i, and satisfying $|H^{(i)}_m|_\infty \leq \binom{n+1}{i}$ in every complex embedding, such that

$$g^{(i)}_{mq^r}(x_1, ..., x_n, a) \equiv H^{(i)}_m \pmod{\pi_K q^r \mathcal{O}_K}.$$

Proof. Let us first assume that x_1 is a unit in $\mathcal{O}_K$. In this case the differential form

$$\omega = \frac{d(1 - P(x_1^{-1}T))}{1 - (1 - P(x_1^{-1}T))} = \sum_{m=1}^{\infty} g^{(1)}_m(1, x_2x_1^{-2}, ..., ax_1^{-1-n})T^n \frac{dT}{T} \tag{3.1}$$

is the canonical invariant differential on a one-dimensional formal group law over $\mathcal{O}_K$ which is strictly isomorphic over $\mathcal{O}_K$ to $\hat{\mathbf{G}}_m$. We take the identity map $\sigma : K \to K$ as our lifting of Frobenius, and deduce the congruences

$$g^{(1)}_{mq^r}(1, x_2x_1^{-2}, ..., ax_1^{-1-n}) \equiv g^{(1)}_{mq^{r-1}}(1, x_2x_1^{-2}, ..., ax_1^{-1-n}) \pmod{\pi_K q^{r-1}\mathcal{O}_K}. \tag{3.2}$$

Multiplying by $x_1^{mq^r}$ and using (2.7) then yields

$$g^{(1)}_{mq^r}(x_1,...,x_n,a) \equiv x_1^{mq^{r-1}(q-1)}\, g^{(1)}_{mq^{r-1}}(x_1,...,x_n,a) \pmod{\pi_K q^{r-1}\mathcal{O}_K}. \tag{3.3}$$

Since the residue-class field $\bar{K}$ has cardinality q, we have $x_1^{m(q-1)} \equiv 1 \pmod{\pi_K\mathcal{O}_K}$, and since $\operatorname{ord}\pi_K \geq 1/(p-1)$ we find by induction that $x_1^{mq^{r-1}(q-1)} \equiv 1 \pmod{\pi_K q^{r-1}\mathcal{O}_K}$, giving the result for $i=1$ in this case.

Now suppose that $x_1 \in \pi_K\mathcal{O}_K$. Note that $\tilde{P}(T) = (1-T)P(T)$ is a polynomial of degree $n+2$ in $\mathcal{O}_K[T]$ whose coefficient of $-T$ is $\tilde{x}_1 = 1+x_1$, which is a unit in $\mathcal{O}_K$. Let $\tilde{g}^{(1)}_m$ denote the coefficient of $T^m dT/T$ in the expansion of $d\tilde{P}/\tilde{P}$; then from the above result applied to $\tilde{P}$ we have

$$\tilde{g}^{(1)}_{mq^r} \equiv \tilde{g}^{(1)}_{mq^{r-1}} \pmod{\pi_K q^{r-1}\mathcal{O}_K}. \tag{3.4}$$

Since $\tilde{g}^{(1)}_m = 1 + g^{(1)}_m(x_1,...,x_n,a)$ for all m, the desired congruence follows for the sequence $g^{(1)}_m(x_1,...,x_n,a)$. This completes the proof of the first statement in the case $i=1$.

Repeating the above argument with P and x_1 replaced by $P^{(i)}$ and x_i proves the first statement for general i.

For the second statement, we note that $\{g^{(i)}_{mq^r}(x_1,...,x_n,a)\}_{r=0}^{\infty}$ is a Cauchy sequence in the complete ring $\mathcal{O}_K$, demonstrating the existence of $H^{(i)}_m$ satisfying the stated congruence. Factor $P(T)$ over $\mathcal{O}_L$ as in (1.4), where L is the splitting field of P over K, and suppose L has residue-class field $\bar{L}$ of cardinality q^b. Since $\lim_{r\to\infty}\alpha_i^{mq^{br}} = \hat{\alpha}_i^m$ (where $\hat{x}$ is the Teichmüller representative of x) and $g^{(i)}_m = \sigma_i(\alpha_1^m,...,\alpha_{n+1}^m)$, we can evaluate the limit as $r\to\infty$ of the subsequence $\{g^{(i)}_{mq^{br}}(x_1,...,x_n,a)\}$ as the algebraic integer

$$H^{(i)}_m = \sigma_i(\hat{\alpha}_1^m,...,\hat{\alpha}_{n+1}^m). \tag{3.5}$$

Noting that Teichmüller representatives $\hat{\alpha}_j$ depend only on $P(T) \pmod{\pi_K\mathcal{O}_K[T]}$ and are either zero or roots of unity, and that the elementary symmetric function $\sigma_i(u_1,...,u_{n+1})$ has $\binom{n+1}{i}$ terms completes the proof.

As a corollary to this theorem we find a condition under which distinct generalized Dickson polynomials agree identically over Galois rings.

Corollary 5. *For any values $x_1,...,x_n,a$ in the Galois ring $R = GR(p^s,t)$ we have the identities*

$$g^{(i)}_{mq^r}(x_1,...,x_n,a) = g^{(i)}_{mq^{r-1}}(x_1,...,x_n,a)$$

for $1 \leq i \leq n$, where $q = p^t$ and $r \geq 1 + (s-1)/t$.

Proof. Take $K = \mathbf{Q}_p(\zeta_{q-1})$ and observe that there is an isomorphism $\mathcal{O}_K/p^s\mathcal{O}_K \cong GR(p^s,t)$. Given $x_1,...,x_n,a \in GR(p^s,t)$, define $P(T)$ as in (1.3) and choose a polynomial $\hat{P} \in \mathcal{O}_K[T]$ whose reduction modulo p^s is P. Let $\hat{g}_m^{(i)}$ denote the coefficient of $T^m dT/T$ in the expansion of $d\hat{P}^{(i)}/\hat{P}^{(i)}$; then from Theorem 4 applied to $\hat{P}$ we have

$$\hat{g}_{mq^r}^{(i)} \equiv \hat{g}_{mq^{r-1}}^{(i)} \pmod{pq^{r-1}\mathcal{O}_K}. \tag{3.6}$$

The corollary then follows by reduction modulo p^s.

It is possible for certain polynomials P to twist these congruences by multiplicative characters. Keeping the notation of Theorem 4 and its proof, let $\bar{P}$ be the image of P in the residue class field $\bar{L}$, and suppose that the set of reciprocal roots of $\bar{P}(T)$ in $\mathbf{F}_q$ (counted with multiplicity) is $S = \{\bar{\alpha}_1,...,\bar{\alpha}_{n+1}\}$. We require that the Frobenius $\sigma : x \mapsto x^q$ acts as a power of a $(n+1)$-cycle on S, i.e., we may write $\sigma = \tau^i$, where $\tau = (\bar{\alpha}_1, \bar{\alpha}_2, ..., \bar{\alpha}_{n+1})$. For $j \in \mathbf{Z}$ set $\varepsilon(j) = \zeta^j$ where ζ is a (not necessarily primitive) $(n+1)$-st root of unity, and define a formal power series

$$Q(T) = \prod_{j=1}^{n+1} (1-\alpha_j T)^{-\varepsilon(j)}. \tag{3.7}$$

Consider the sequence $\{f_m(x_1,...,x_n,a)\}$ defined by expansion of the differential

$$\omega = \frac{dQ}{Q} = \sum_{m=1}^{\infty} f_m(x_1,...,x_n,a)T^m \frac{dT}{T}. \tag{3.8}$$

Then we have the following result.

Theorem 6. *With notation as above,*

i. The sequence $\{f_m(x_1,...,x_n,a)\}$ satisfies the same linear $(n+1)$-st order recursion as does $\{g_m^{(1)}(x_1,...,x_n,a)\}$.

ii. Suppose that the ramification index e_L of L over $\mathbf{Q}_p$ satisfies $e_L \leq p-1$. Then for all $m, r > 0$ we have the congruences

$$f_{mq^r}(x_1,...,x_n,a) \equiv \zeta^i f_{mq^{r-1}}(x_1,...,x_n,a) \pmod{\pi_L q^{r-1}\mathcal{O}_L[\zeta]}.$$

Proof. We compute directly from (3.7) that

$$\frac{dQ}{Q} = \sum_{j=1}^{n+1} \frac{\varepsilon(j)\alpha_j}{1-\alpha_j T}\, dT = \frac{B(T)}{P(T)}\, dT \tag{3.9}$$

for some polynomial $B \in \mathcal{O}_L[\zeta][T]$ of degree at most n, from which the first statement follows. We further note by comparing (3.8), (3.9) that

$$f_m(x_1, ..., x_n, a) = \sum_{j=1}^{n+1} \varepsilon(j)\alpha_j^m, \tag{3.10}$$

so the congruences in (ii) follow from the congruences $\alpha_j^{q^r} \equiv \alpha_{j+i}^{q^{r-1}} \pmod{\pi_L q^{r-1}\mathcal{O}_L}$, where $j+i$ is interpreted as the element of $\{1, 2, ..., n+1\}$ congruent to $j+i$ modulo $n+1$. For $r = 1$ these congruences are evident from our hypothesis on σ. Assuming that $e_L \leq p-1$, the general case is proved by induction on r.

The condition on σ in this theorem is unfortunately rather restrictive, in that it requires $\bar{P}$ to split over $\mathbf{F}_q$ into irreducible factors which all have the same degree. This is satisfied for all P only when $n = 0, 1$. Furthermore, the f_n do not usually have coefficients in $\mathcal{O}_K$, but in $\mathcal{O}_L[\zeta]$. However, when $n = 0, 1$ they can be normalized to lie in $\mathcal{O}_K$.

4 Congruences for Dickson Polynomials of the Second Kind

For example, take $P(T) = 1 - xT + aT^2 \in \mathcal{O}_K[T]$ and take $\zeta = -1$ in Theorem 6. If the discriminant $D = x^2 - 4a$ is a square in $\mathcal{O}_K^\times$ then we have $i = 2$ in the congruences, whereas if D is a nonsquare in $\mathcal{O}_K^\times$ then $i = 1$. In this case the $f_m(x, a)$ can be normalized to give the *Dickson polynomials of the second kind* $h_m(x, a)$ over $\mathcal{O}_K$ by

$$(\alpha_2 - \alpha_1)h_{m-1}(x, a) = f_m(x, a), \tag{4.1}$$

and we have the following result, which generalizes (Young 1994, Corollary 1).

Corollary 7. *If the ramification index e_L of $L = K(\sqrt{D})$ satisfies $e_L \leq p-1$, then for all $x, a \in \mathcal{O}_K$ we have*

$$h_{mq^r-1}(x, a) \equiv \left(\frac{D}{\pi_K}\right) h_{mq^{r-1}-1}(x, a) \pmod{\pi_K q^{r-1}\mathcal{O}_K},$$

where $(D|\pi_K)$ is the quadratic Legendre symbol in $\mathcal{O}_K$, defined by $(D|\pi_K) = 1$ (resp. -1; resp. 0) if $D \in (\mathcal{O}_K^\times)^2$ (resp. $\mathcal{O}_K^\times \setminus (\mathcal{O}_K^\times)^2$; resp. $\pi_K\mathcal{O}_K$). These congruences also hold when $p = 2$, $D \in \pi_K\mathcal{O}_K$, and $e_L \leq 2$.

Proof. If D is a unit in $\mathcal{O}_K^\times$, the congruence holds modulo $\pi_L q^{r-1}\mathcal{O}_L$ by Theorem 6, (4.1), and the above remarks, but it is easy to see that both sides lie in $\mathcal{O}_K$, giving the result.

If $D \in \pi_K \mathcal{O}_K$, we can write $\alpha_2 - \alpha_1 = \pm\sqrt{D}$ with $\sqrt{D} \in \pi_L^N \mathcal{O}_L$, $z \notin \pi_L^{N+1} \mathcal{O}_L$. Note that if $p = 2$ then $D = x^2 - 4a \in \pi_K^2 \mathcal{O}_K$ and therefore $N \geq 2$. By induction on r using the hypothesis $e_L \leq N(p-1)$ one has

$$f_{mq^r}(x,a) = \alpha_2^{mq^r} - \alpha_1^{mq^r} \equiv 0 \pmod{\pi_L^N q^r \mathcal{O}_L}, \tag{4.2}$$

which yields

$$h_{mq^r-1}(x,a) \equiv 0 \pmod{q^r \mathcal{O}_L}. \tag{4.3}$$

Again, this last congruence holds modulo $q^r \mathcal{O}_K$ since all $h_n(x,a) \in \mathcal{O}_K$, completing the proof.

Corollary 8. *For any values x, a in the Galois ring $R = GR(p^s, t)$ we have the identity*

$$h_{mq^r-1}(x,a) = \chi(D) h_{mq^{r-1}-1}(x,a),$$

where $q = p^t$ and $r \geq 1 + (s-1)/t$, and

$$\chi(D) = \begin{cases} 1, & \text{if } D \text{ is a square in } R^\times; \\ -1, & \text{if } D \text{ is a nonsquare in } R^\times; \\ 0, & \text{if } D \text{ is a nonunit in } R. \end{cases}$$

Proof. Take $K = \mathbf{Q}_p(\zeta_{q-1})$ in Corollary 7 and note that $e_L = 1$ when $D \in \mathcal{O}_K^\times$ and $e_L \leq 2$ when $D \in \pi_K \mathcal{O}_K$. Then proceed as in the proof of Corollary 5.

By comparing (3.8), (3.9), (4.1) we see that the Dickson polynomials of the second kind $h_m(x,a)$ can be defined by the expansion

$$\omega = \omega(T) = \frac{dT}{P(T)} = \sum_{m=1}^{\infty} h_{m-1}(x,a) T^m \frac{dT}{T} \tag{4.4}$$

where $P(T) = 1 - xT + aT^2$. Here we relate this differential to a formal group law and deduce congruences in polynomial rings $R[x,a]$ related to Corollary 7. These congruences in turn give a partial factorization of $h_{mq-1}(x,a)$ over the finite field $\mathbf{F}_q$.

Theorem 9. *Let R be a commutative ring with identity. Then for any power $q = p^f$ of an odd prime p and for all $m > 0$ we have*

$$h_{mq-1}(x,a) \equiv (x^2 - 4a)^{(q-1)/2} h_{m-1}(x^q, a^q) \pmod{pR[x,a]}.$$

It follows that for $a \in \mathbf{F}_q$ we have the factorization

$$h_{mq-1}(x,a) = (x^2 - 4a)^{(q-1)/2} h_{m-1}(x^q, a) \quad \text{in} \quad \mathbf{F}_q[x].$$

Proof. Again it suffices to prove this for $R = \mathbf{Z}$. We first consider the case $q = p$. Let $\varphi \in T + T^2\mathbf{Z}[x,a][[T]]$ be the formal power series given by $\varphi = T/P(T)$. Considering x, a as constants and taking total derivatives in $P(T)\varphi = T$ yields

$$\omega = \frac{dT}{P(T)} = \frac{d\varphi}{1 - P'(T)\varphi} = \frac{d\varphi}{1 - (-x + 2aT)\varphi}. \tag{4.5}$$

Since $\varphi - (1 + x\varphi)T + a\varphi T^2 = 0$ we have

$$T = \frac{1 + x\varphi - ((1 + x\varphi)^2 - 4a\varphi^2)^{1/2}}{2a\varphi}, \tag{4.6}$$

yielding

$$\omega = \omega(\varphi) = \frac{d\varphi}{\sqrt{1 + 2x\varphi + (x^2 - 4a)\varphi^2}}. \tag{4.7}$$

Here $f^{1/2}$ and $\sqrt{f}$ refer to the power series in $1 + \varphi\mathbf{Z}[1/2][x,a][[\varphi]]$ whose square is f.

We recall that the Legendre polynomials $P_n(z) \in \mathbf{Z}[1/2][z]$ are defined by

$$(1 - 2zt + t^2)^{-1/2} = \sum_{n=0}^{\infty} P_n(z)t^n, \tag{4.8}$$

and substitute $u = (x^2 - 4a)^{1/2}\varphi$ to give the expansion

$$\omega(\varphi) = \sum_{n=1}^{\infty} P_{n-1}\left(\frac{-x}{\sqrt{x^2 - 4a}}\right)(x^2 - 4a)^{(n-1)/2}\varphi^n \frac{d\varphi}{\varphi}. \tag{4.9}$$

Note that each coefficient $\gamma_{n-1}(x,a) = P_{n-1}(\frac{-x}{\sqrt{x^2-4a}})(x^2 - 4a)^{(n-1)/2}$ lies in $\mathbf{Z}[1/2][x,a]$ since $P_n(z)$ is an even (resp. odd) polynomial of degree n when n is even (resp. odd).

Consider the lifting of Frobenius σ on $\mathbf{Z}_p[x,a]$ induced by $\sigma(x) = x^p$,

$$\sigma(a) = 4^{p-1}a^p - \frac{1}{4}\sum_{k=1}^{p-1}\binom{p}{k}x^{2k}(-4a)^{p-k}, \tag{4.10}$$

and $\sigma(h(x,a)) = h(\sigma(x), \sigma(a))$, and note that $\sigma(x^2 - 4a) = (x^2 - 4a)^p$. By a theorem of Honda (1976),

$$P_{mp^r-1}(z) \equiv P_{mp^{r-1}-1}(z^p) \pmod{p^r\mathbf{Z}_p[z]}, \tag{4.11}$$

which implies that

$$P_{mp^r-1}\left(\frac{-x}{\sqrt{x^2 - 4a}}\right) \equiv P_{mp^{r-1}-1}\left(\frac{-x^p}{(x^2 - 4a)^{p/2}}\right) \pmod{p^r\mathbf{Z}_p[x, (x^2 - 4a)^{-1/2}]}. \tag{4.12}$$

Multiplying both sides by $(x^2-4a)^{(mp^r-1)/2}$ gives

$$\begin{aligned} & P_{mp^r-1}\left(\tfrac{-x}{\sqrt{x^2-4a}}\right)(x^2-4a)^{(mp^r-1)/2} \\ & \equiv (x^2-4a)^{(p-1)/2} P_{mp^{r-1}-1}\left(\tfrac{-x^p}{(x^2-4a)^{p/2}}\right)((x^2-4a)^p)^{(mp^{r-1}-1)/2} \\ & \qquad (\mathrm{mod}\, p^r \mathbf{Z}_p[x,(x^2-4a)^{1/2}]), \end{aligned} \tag{4.13}$$

which shows that

$$\begin{aligned} \gamma_{mp^r-1}(x,a) \quad &\equiv \quad (x^2-4a)^{(p-1)/2}\,\sigma(\gamma_{mp^{r-1}-1}(x,a)) \\ & \qquad (\mathrm{mod}\, p^r \mathbf{Z}_p[x,a]), \end{aligned} \tag{4.14}$$

since both members of these congruences lie in $\mathbf{Z}_p[x,a]$. We have therefore shown (cf. Stienstra and Beukers 1985, Theorem A8) that $\omega(\varphi)$ is the canonical invariant differential on a formal group law over $\mathbf{Z}_p[x,a]$ (and in fact over $\mathbf{Z}[1/2][x,a]$), and it follows that the power series $T \in \varphi + \varphi^2\mathbf{Z}[x,a][[\varphi]]$ defined by (4.6) is a strict isomorphism from this formal group law to a formal group law over $\mathbf{Z}_p[x,a]$ whose canonical invariant differential is $\omega(T)$. Therefore we have congruences (Stienstra and Beukers 1985, Theorem A8)

$$\begin{aligned} h_{mp^r-1}(x,a) \quad &\equiv \quad (x^2-4a)^{(p-1)/2} h_{mp^{r-1}-1}(x^p,\sigma(a)) \\ & \qquad (\mathrm{mod}\, p^r \mathbf{Z}_p[x,a]) \end{aligned} \tag{4.15}$$

where $\sigma(a)$ is given by (4.10). Taking $r=1$ and noting that $\sigma(a) \equiv a^p \pmod{p\mathbf{Z}[x,a]}$ gives the result for $q=p$.

For the general case where $q=p^f$, we apply the result for $q=p$ recursively with $h_{mp-1}(x,a)$ replaced by $h_{mp^{f-i}-1}(x^{p^i},a^{p^i})$ for $i=0,1,\ldots,f-1$.

Remarks. 1. The equation $P(T)\varphi = T$ may be viewed as the affine equation of a family of cubic curves (parametrized by x,a) which are singular at the point at infinity. The reductions modulo p are cuspidal when $(D|p)=0$ and are nodal with tangents rational (resp. irrational) over $\mathbf{F}_p$ when $(D|p)=1$ (resp. $(D|p)=-1$). By (4.5) we may view ω as a differential on these curves, and this theorem (and Corollary 7) may thus be interpreted as degenerate cases of a result on elliptic curves (cf. Hazewinkel 1978, §33).

2. The congruences (4.15) are stronger than those stated in the theorem, but appear cumbersome due to the lifting of Frobenius σ. If instead we choose the lifting of Frobenius given by $h(x,a) \mapsto h(x^p,a^p)$, we find that there also exists an element $H(x,a) \in \mathbf{Z}_p[[x,a]]$ such that

$$\begin{aligned} h_{mp^r-1}(x,a) \quad &\equiv \quad H(x,a)\cdot h_{mp^{r-1}-1}(x^p,a^p) \\ & \qquad (\mathrm{mod}\, p^r \mathbf{Z}_p[[x,a]]) \end{aligned} \tag{4.16}$$

and satisfying

$$H(x,a) \equiv (x^2-4a)^{(p-1)/2} \pmod{p\mathbf{Z}_p[[x,a]]}. \tag{4.17}$$

Furthermore for $q=p^f$ we have

$$\begin{aligned} h_{mq^r-1}(x,a) &\equiv H^{(f)}(x,a)\cdot h_{mq^{r-1}-1}(x^q,a^q) \\ &\pmod{pq^{r-1}\mathbf{Z}_p[[x,a]]} \end{aligned} \tag{4.18}$$

where $H^{(f)}(x,a) = H(x,a)H(x^p,a^p)\cdots H(x^{p^{f-1}},a^{p^{f-1}})$.

3. Although the method used in the proof of this result does not apply for $p=2$, the reader may easily verify the following analogous result for $p=2$.

Proposition 10. *Let R be a commutative ring with identity. If $q=2^f$, then for all $m>0$ we have*

$$h_{mq-1}(x,a) \equiv x^{q-1}\, h_{m-1}(x^q,a^q) \pmod{2R[x,a]}.$$

It follows that for $a\in\mathbf{F}_q$ we have the factorization

$$h_{mq-1}(x,a) = x^{q-1}\, h_{m-1}(x^q,a) \quad \textit{in} \quad \mathbf{F}_q[x].$$

Proof. As in Theorem 4.3 it suffices to prove this with $R=\mathbf{Z}$ and $q=2$, that is,

$$h_{2m-1}(x,a) \equiv x\, h_{m-1}(x^2,a^2) \pmod{2\mathbf{Z}[x,a]}, \tag{4.19}$$

which may be verified directly from the explicit formula

$$h_n(x,a) = \sum_{k=0}^{[n/2]} \binom{n-k}{k} (-a)^k x^{n-2k}. \tag{4.20}$$

5 Congruences for the Rational Rédei Functions

As a final application we obtain congruence results for the rational Rédei functions $R_n(x,a)\in\mathbf{Q}(x,a)$, which are defined as follows (cf. Mullen 1993): Let x,a be indeterminates and define polynomials $r_n, s_n\in\mathbf{Z}[x,a]$ by the expansion

$$(x+\sqrt{a})^n = r_n(x,a) + s_n(x,a)\sqrt{a}. \tag{5.1}$$

Then set $R_n(x,a) = r_n(x,a)/s_n(x,a)$.

For a fixed odd prime p let "ord" denote the p-adic valuation on $\mathbf{Q}$ with $\operatorname{ord} p = 1$. If $f=\sum_{i,j} c_{i,j}x^ia^j\in\mathbf{Z}[x,a]$, define $\operatorname{ord} f = \min_{i,j}\operatorname{ord} c_{i,j}$, and extend this definition to rational functions $h\in\mathbf{Q}(x,a)$ by writing $h=f/g$

with $f, g \in \mathbf{Z}[x, a]$ and defining $\operatorname{ord} h = \operatorname{ord} f - \operatorname{ord} g$. This definition is independent of the choice of f, g and gives a non-archimedean valuation on $\mathbf{Q}(x, a)$ (called the Gauss norm). Let E denote the completion of $\mathbf{Q}(x, a)$ under this valuation, and define

$$\mathcal{A} = \{h \in \mathbf{Q}(x, a) : \operatorname{ord} h \geq 0\}, \tag{5.2}$$

$$\mathcal{A}^c = \{h \in E : \operatorname{ord} h \geq 0\}. \tag{5.3}$$

Theorem 11. *Let q be a power of an odd prime p.*

i. Suppose that K is as in §3, with uniformizing parameter π_K, residue-class field of cardinality q and ramification index $e \leq p-1$. If $x, a \in \mathcal{O}_K$ with $a \in \mathcal{O}_K^\times$ such that $R_m(x, a) \in \mathcal{O}_K$ for some m, then in fact $R_{mq^r}(x, a) \in \mathcal{O}_K$ for all $r > 0$ and we have

$$R_{mq^r}(x, a) \equiv \left(\frac{a}{\pi_K}\right) R_{mq^{r-1}}(x, a) \pmod{\pi_K q^{r-1} \mathcal{O}_K}.$$

ii. There exists an element $H(x, a) \in \mathcal{A}^c$ satisfying

$$H(x, a) \equiv a^{(1-q)/2} \pmod{p\mathcal{A}^c}$$

such that for all $m, r > 0$ we have

$$R_{mq^r}(x, a) \equiv H(x, a)\, R_{mq^{r-1}}(x^q, a^q) \pmod{pq^{r-1}\mathcal{A}^c}.$$

iii. In particular, for all $m > 0$ we have

$$R_{mq}(x, a) \equiv a^{(1-q)/2}\, R_m(x^q, a^q) \pmod{p\mathcal{A}}.$$

Proof. From the definition of r_n, s_n we see that $2r_n(x, a) = g_n^{(1)}(2x, x^2 - a)$ and $s_n(x, a) = h_{n-1}(2x, x^2 - a)$, and note that the characteristic polynomial $P(T) = 1 - 2xT + (x^2 - a)T^2$ has discriminant $D = 4a$. The results essentially follow from Theorems 3,4,9, and Corollary 7.

Let us write $P(T) = (1 - \alpha T)(1 - \beta T)$ with $\alpha, \beta = x \pm \sqrt{a}$. Suppose that $x, a \in \mathcal{O}_K$ with $a \in \mathcal{O}_K^\times$ such that $s_m(x, a) = (\alpha^m - \beta^m)/(\alpha - \beta) \in \pi_K \mathcal{O}_K$. Then we have $\alpha^m - \beta^m \equiv 0 \pmod{\pi_K \mathcal{O}_K[\sqrt{a}]}$. Since $p \neq 2$, it follows that $r_m(x, a) = (\alpha^m + \beta^m)/2 \in \mathcal{O}_K^\times$, so that $R_m(x, a)$ does not lie in $\mathcal{O}_K$. So if $R_m(x, a) \in \mathcal{O}_K$, then $s_m(x, a) \in \mathcal{O}_K^\times$. By Corollary 7 we know that

$$s_{mq^r}(x, a) \equiv \left(\frac{4a}{\pi_K}\right) s_{mq^{r-1}}(x, a) \pmod{\pi_K q^{r-1} \mathcal{O}_K} \tag{5.4}$$

for all r, so if $s_m(x,a) \in \mathcal{O}_K^\times$ then $s_{mq^r}(x,a) \in \mathcal{O}_K^\times$ for all r. By Theorem 4 we know that

$$r_{mq^r}(x,a) \equiv r_{mq^{r-1}}(x,a) \pmod{\pi_K q^{r-1}\mathcal{O}_K} \tag{5.5}$$

for all r. Part (i) follows by dividing the members of the congruences (5.5) by the corresponding members of (5.4) and noting that $(4a|\pi_K) = (a|\pi_K)$.

For (ii), we compute from (5.1) that when m is odd, the polynomial $s_{mq^r}(x,a)$ has the term $a^{(mq^r-1)/2}$, and when m is even $s_{mq^r}(x,a)$ contains the term $\binom{mq^r}{q^r}x^{(m-1)q^r}a^{(q^r-1)/2}$, showing that for all $m, r > 0$ we have $\operatorname{ord} s_{mq^r} = 0$, and thus s_{mq^r} is a unit in $\mathcal{A}$. We define a lifting of Frobenius σ on $\mathcal{A}^c$ by $\sigma(x) = x^p$,

$$\sigma(a) = a^p - \sum_{k=1}^{p-1} \binom{p}{k} x^{2k}(-a)^{p-k}, \tag{5.6}$$

and $\sigma(h(x,a)) = h(\sigma(x), \sigma(a))$, and note that $\sigma(x^2-a) = (x^2-a)^p$. Noting that $\mathbf{Z}[x,a] \subset \mathcal{A}$ and repeating the proof of Theorem 3 with a different lifting of Frobenius we find that

$$r_{mq^r}(x,a) \equiv r_{mq^{r-1}}(x^q, a^q) \pmod{pq^{r-1}\mathcal{A}}, \tag{5.7}$$

and as in the remark (2) following Theorem 9 there is an element $G(x,a) \in \mathcal{A}^c$ satisfying $G(x,a) \equiv (4a)^{(q-1)/2} \pmod{p\mathcal{A}^c}$ such that

$$s_{mq^r}(x,a) \equiv G(x,a)\, s_{mq^{r-1}}(x^q, a^q) \pmod{pq^{r-1}\mathcal{A}^c}. \tag{5.8}$$

Now we note that $G(x,a)$ is also a unit in $\mathcal{A}^c$ and $H(x,a) = G(x,a)^{-1} \equiv a^{(1-q)/2} \pmod{p\mathcal{A}^c}$, and obtain the result by dividing the terms in (5.7) by the corresponding terms in (5.8).

Part (iii) follows by taking $r = 1$ in (ii), using $H(x,a) \equiv a^{(1-q)/2} \pmod{p\mathcal{A}^c}$, and noting that both sides lie in $\mathcal{A}$. This completes the proof.

Remarks. 1. The congruences in (ii) imply that the differential form

$$\omega = \sum_{m=1}^{\infty} R_m(x,a)T^m \frac{dT}{T} \tag{5.9}$$

is an invariant differential on a one-dimensional commutative formal group law over $\mathcal{A}$ (cf. Stienstra and Beukers 1985, Theorem A8; the canonical such differential is $x^{-1}\omega$).

2. The rational Rédei functions over $\mathbf{F}_q$ usually appear as functions $R_m(x)$ of the single variable x, obtained by choosing a specific non-square value of $a \in \mathbf{F}_q^\times$ (cf. Mullen 1993). In this case we have the following result.

Corollary 12. *If q is a power of an odd prime, then for all $m > 0$ we have the identity*

$$R_{mq}(x) = -R_m(x^q)$$

in the rational function field $\mathbf{F}_q(x)$.

Proof. We note that Theorem 11(iii) directly implies the identity

$$R_{mq}(x, a) = a^{(1-q)/2} R_m(x^q, a^q) \tag{5.10}$$

in the rational function field $\mathbf{F}_q(x, a)$ by reduction modulo p. Therefore specializing a to a nonsquare element of $\mathbf{F}_q^\times$ yields the stated identity.

Bibliography

1. M. Hazewinkel (1978), *Formal Groups and Applications*, Academic Press, New York.

2. T. Honda (1976), Two congruence properties of Legendre polynomials, *Osaka J. Math.*, **13**, 131-133.

3. R. Lidl and H. Niederreiter (1983), *Finite Fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley.

4. G. Mullen (1993), Permutation polynomials over finite fields, in *Finite Fields, Coding Theory, and Advances in Communications and Computing*, Lecture Notes in Pure and Applied Mathematics, vol. 141, Marcel Dekker, New York.

5. J. Stienstra and F. Beukers (1985), On the Picard-Fuchs equation and the formal Brauer group of certain elliptic $K3$-surfaces, *Math. Annalen*, **271**, 269-304.

6. P. T. Young (1994), Congruences for generalized Fibonacci sequences, *The Fibonacci Quarterly*, **32.1**, 2-10.