# Some Congruences and Identities for Generalizations of Rédei Functions

PAUL THOMAS YOUNG

ABSTRACT. In a recent article we described various congruences, identities, and factorization results for the generalized Dickson polynomials and Dickson polynomials of the second kind which are obtained by relating their generating functions to differentials on formal group laws. In this note we show that the Rédei functions, as well as generalizations due to W. Nöbauer and to Fried and Lidl, also satisfy congruences which reveal their connection to formal group laws.

## 1. Introduction

Dickson polynomials and Rédei functions have been extensively studied with respect to their permutation behavior on finite fields and Galois rings. In [**7**] we showed that the generalized Dickson polynomials and Dickson polynomials of the second kind arise as the expansion coefficients of invariant differentials on rational formal group laws over polynomial rings. As corollaries we deduced congruences for these polynomials in characteristic zero, which imply various identities and factorization results in positive characteristic. In this note we demonstrate analogous results for the Rédei functions and their various generalizations.

1991 *Mathematics Subject Classification.* Primary 11T06; Secondary 14L05.

This paper is in final form and no version of it will be submitted for publication elsewhere.

## 2. Congruences for the rational Rédei Functions

In this section we give congruence results for the rational Rédei functions which reveal their connection to formal group laws attached to quadratic characters. The Rédei functions $R_n(x,a) \in \mathbf{Q}(x,a)$ are defined as follows (cf. [**3**]): Let $x, a$ be indeterminates and define polynomials $r_n, s_n \in \mathbf{Z}[x,a]$ by the expansion

$$(x+\sqrt{a})^n = r_n(x,a) + s_n(x,a)\sqrt{a}. \tag{2.1}$$

Then set $R_n(x,a) = r_n(x,a)/s_n(x,a)$. (For a power $q$ of a prime $p$, we obtain Rédei functions $R_n(x)$ of the single variable $x$ over $\mathbf{F}_q$ by reducing the coefficients modulo $p$ and specializing $a$ to $\mathbf{F}_q$; generally $a$ is specialized to a nonsquare element of $\mathbf{F}_q^\times$.)

For a fixed odd prime $p$ let "ord" denote the $p$-adic valuation on $\mathbf{Q}$ with ord $p = 1$. If $f = \sum_{i,j} c_{i,j} x^i a^j \in \mathbf{Z}[x,a]$, define ord $f = \min_{i,j}$ 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 ord $h =$ ord $f -$ 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). We give congruences for $R_n(x,a)$ in the ring

$$\mathcal{A} = \{h \in \mathbf{Q}(x,a) : \text{ord } h \geq 0\}. \tag{2.2}$$

THEOREM 2.1. *Let $p$ be an odd prime. Then the formal differential form*

$$\omega = \sum_{n=1}^{\infty} R_n(x,a) T^m \frac{dT}{T}$$

*is an invariant differential on a formal group law over $\mathcal{A}$ isomorphic over $\mathcal{A}[a^{1/2}]$ to the formal group law given by*

$$F(X,Y) = X + Y - a^{-1/2} XY.$$

PROOF. By [**6**, Theorem A8, A9] it suffices to prove the congruences

$$R_{mp^r}(x,a) \equiv a^{(1-p)/2}\, R_{mp^{r-1}}(x^p, a^p) \pmod{p^r \mathcal{A}} \tag{2.3}$$

for all $m, r > 0$; we are using the map $\sigma : \mathcal{A} \to \mathcal{A}$ defined by $h(x,a) \mapsto h(x^p, a^p)$ as our "lifting of Frobenius" in the terminology of that article (cf. also [**2**]). It is well-known and easily verified that

$$R_n(x,a) = \sqrt{a} \cdot \frac{(x+\sqrt{a})^n + (x-\sqrt{a})^n}{(x+\sqrt{a})^n - (x-\sqrt{a})^n} \tag{2.4}$$

[**3**, eq.(2.12)]. From the congruences

$$(x \pm \sqrt{a})^p \equiv x^p \pm \sqrt{a}^{\,p} \pmod{p\mathbf{Z}[x,a]} \tag{2.5}$$

we deduce by induction on $r$ that

$$(x \pm \sqrt{a})^{mp^r} \equiv (x^p \pm \sqrt{a}^{\,p})^{mp^{r-1}} \pmod{p^r\mathbf{Z}[x,a]}. \tag{2.6}$$

Now when $m$ is odd, the polynomial $(x+\sqrt{a})^{mp^r} - (x-\sqrt{a})^{mp^r}$ contains the monomial $2\sqrt{a}^{\,mp^r}$, and when $m$ is even it contains the monomial $2\binom{mp^r}{p^r}x^{(m-1)p^r}\sqrt{a}^{\,p^r}$, showing that in either case this polynomial is a unit in $\mathcal{A}$. It follows that

$$\begin{aligned}&\frac{(x+\sqrt{a})^{mp^r} + (x-\sqrt{a})^{mp^r}}{(x+\sqrt{a})^{mp^r} - (x-\sqrt{a})^{mp^r}}\\ &\equiv \frac{(x^p+\sqrt{a}^{\,p})^{mp^{r-1}} + (x^p-\sqrt{a}^{\,p})^{mp^{r-1}}}{(x^p+\sqrt{a}^{\,p})^{mp^{r-1}} - (x^p-\sqrt{a}^{\,p})^{mp^{r-1}}} \pmod{p^r\mathcal{A}}\end{aligned} \tag{2.7}$$

and therefore (2.3) holds, as desired.

**Remarks.** One deduces identities in Galois rings from these congruences as follows. If $q = p^t$, view the $R_n(x,a)$ as defined over the ring of integers $\mathcal{O}_K$ of the unramified extension $K$ of $\mathbf{Q}_p$ of degree $t$, and note that (2.3) implies

$$R_{mq^r}(x,a) \equiv a^{(1-q)/2}\, R_{mq^{r-1}}(x^q, a^q) \pmod{pq^{r-1}\mathcal{A}}. \tag{2.8}$$

By specializing $a$ to a $(q-1)$-st root of unity in $K$ which is not a $((q-1)/2)$-th root of unity, these congruences become

$$R_{mq^r}(x) \equiv -\,R_{mq^{r-1}}(x^q) \pmod{pq^{r-1}\mathcal{A}_K}, \tag{2.9}$$

where

$$\mathcal{A}_K = \{h \in K(x) : \operatorname{ord} h \geq 0\}, \tag{2.10}$$

$\operatorname{ord}(f/g) = \operatorname{ord} f - \operatorname{ord} g$ and $\operatorname{ord}(\sum_i c_i x^i) = \min_i \operatorname{ord} c_i$. Noting that $\mathcal{O}_K/p^s\mathcal{O}_K$ is isomorphic to the Galois ring $R = GR(p^s,t)$, reduction modulo $p^s$ yields identities

$$R_{mq^r}(x) = -\,R_{mq^{r-1}}(x^q) \quad \text{in } R(x) \tag{2.11}$$

whenever $r \geq 1 + (s-1)/t$. In particular we have

$$R_{mq}(x) = -\,R_m(x^q) \quad \text{in } \mathbf{F}_q(x). \tag{2.12}$$

The same method may be applied to give congruences for W. Nöbauer's generalization of the Rédei functions, which are defined as follows (cf. [**5, 3**]): Choose a quadratic polynomial $t(x) = x^2 - \lambda x + \mu \in \mathbf{Z}[\lambda, \mu][x]$, and let $\xi$ denote the residue class of $x$ in the ring $\mathbf{Z}[\lambda, \mu][x]/(t(x))$. Each element of this ring has a unique representation of the form $a + b\xi$ with $a, b \in \mathbf{Z}[\lambda, \mu]$. Define polynomials $g_n, h_n \in \mathbf{Z}[\lambda, \mu][x]$ by the expansion

$$(x + \xi)^n = g_n(x) + h_n(x)\xi \quad in \quad \mathbf{Z}[\lambda, \mu][x]/(t(x)). \tag{2.13}$$

Then set

$$R_n^*(x) = g_n(x)/h_n(x) = R_n^*(x, a, \sqrt{D}), \tag{2.14}$$

where $D = a^2 + 4b$, and set $\alpha, \beta = \dfrac{a \pm \sqrt{D}}{2}$. We obtain congruences in the ring

$$\mathcal{A} = \{h \in \mathbf{Q}(x, a, D) : \text{ord } h \geq 0\}, \tag{2.15}$$

where ord $(f/g) =$ ord $f -$ ord $g$ and

$$\text{ord } (\sum c_{ijk} x^i a^j D^k) = \min \text{ ord } \ c_{ijk}. \tag{2.16}$$

PROPOSITION 2.2. *If $q$ is a power of an odd prime $p$, then for all $m, r > 0$ we have*

$$2R_{mq^r}^*(x, a, \sqrt{D}) - a \equiv D^{(1-q)/2}(2R_{mq^{r-1}}^*(x^q, a^q, \sqrt{D}^{\,q}) - a^q) \pmod{pq^{r-1}\mathcal{A}}.$$

SKETCH OF PROOF. Begin with the identity

$$\frac{(x + \alpha)^n}{(x + \beta)^n} = \frac{R_n^*(x) + \alpha}{R_n^*(x) + \beta} \tag{2.17}$$

[**3**, p. 24] and repeat the proof of Theorem 2.1 *mutatis mutandis*.

## 3. Congruences for Fried and Lidl's Multivariate Generalization of Rédei Functions

Let $K$ be the unramified extension of $\mathbf{Q}_p$ of degree $t$, $q = p^t$, and let $\theta$ be a $(q^{k+1} - 1)$-st root of unity in the algebraic closure of $\mathbf{Q}_p$ which is not a $(q^j - 1)$-st root of unity for any $j$, $1 \leq j \leq k$. Following the construction

of generalized Rédei function vectors given by Matthews and Lidl [**4**], we define

$$A = A(\theta) = \begin{pmatrix} 1 & \theta & \theta^2 & \cdots & \theta^k \\ 1 & \theta^q & \theta^{2q} & \cdots & \theta^{kq} \\ 1 & \theta^{q^2} & \theta^{2q^2} & \cdots & \theta^{kq^2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \theta^{q^k} & \theta^{2q^k} & \cdots & \theta^{kq^k} \end{pmatrix}. \tag{3.1}$$

For a vector $\underline{\mathbf{v}} = (v_1, ..., v_{k+1})$ write $\underline{\mathbf{v}}^{(n)} = (v_1^n, ..., v_{k+1}^n)$, and define

$$R_n(\underline{\mathbf{x}}, \theta) = A^{-1}(A\underline{\mathbf{x}})^{(n)}. \tag{3.2}$$

Fried and Lidl's generalization of the Rédei functions [**1, 3**] may be obtained by reducing the coefficients of the vectors $R_n(\underline{\mathbf{x}}, \theta)$ to the residue-class field of $K$, which is isomorphic to $\mathbf{F}_q$.

THEOREM 3.1. *For $m, r > 0$,*

$$R_{mq^r}(\underline{\mathbf{x}}, \theta) \equiv A^{-1}EA \cdot R_{mq^{r-1}}(\underline{\mathbf{x}}^{(q)}, \theta^q) \pmod{pq^{r-1}\mathcal{O}_K[\underline{\mathbf{x}}]^{k+1}},$$

*where*

$$E = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

PROOF. Observe that for all $m > 0$,

$$(A\underline{\mathbf{x}})^{(mq)} \equiv (EA\underline{\mathbf{x}}^{(q)})^{(m)} \pmod{p\mathcal{O}_L[\underline{\mathbf{x}}]^{k+1}} \tag{3.3}$$

where $L = K(\theta)$. By induction on $r$, we find that for all $m, r > 0$,

$$(A\underline{\mathbf{x}})^{(mq^r)} \equiv (EA\underline{\mathbf{x}}^{(q)})^{(mq^{r-1})} \pmod{pq^{r-1}\mathcal{O}_L[\underline{\mathbf{x}}]^{k+1}}. \tag{3.4}$$

Premultiplication by $A^{-1}$ yields

$$\begin{aligned} A^{-1}(A\underline{\mathbf{x}})^{(mq^r)} &\equiv A^{-1}(EA\underline{\mathbf{x}}^{(q)})^{(mq^{r-1})} \\ &= (A^{-1}EA)(EA)^{-1}(EA\underline{\mathbf{x}}^{(q)})^{(mq^{r-1})} \\ &\qquad \pmod{pq^{r-1}\mathcal{O}_K[\underline{\mathbf{x}}]^{k+1}}. \end{aligned} \tag{3.5}$$

Now note that $EA(\theta) = A(\theta^q)$; thus (3.5) is equivalent to

$$R_{mq^r}(\underline{\mathbf{x}}, \theta) \equiv A^{-1}EA \cdot R_{mq^{r-1}}(\underline{\mathbf{x}}^{(q)}, \theta^q) \pmod{pq^{r-1}\mathcal{O}_K[\underline{\mathbf{x}}]^{k+1}}, \tag{3.6}$$

as desired.

**Remarks.** In the case $k = 1$ and $\theta = \sqrt{a}$ where $a$ is a primitive $(q-1)$-st root of unity in $K$, the vector $R_n(\underline{\mathbf{x}}, \theta)$ has the form $(r_n(x_1, x_2), s_n(x_1, x_2))$ with the property that $r_n(x, 1)/s_n(x, 1)$ is the usual one-variable Rédei function $R_n(x, a)$ [**1,3**]. We note that the special element $A^{-1}EA$ in these congruences has multiplicative order $k + 1$, in direct analogy to the element $a^{(1-q)/2}$ of order 2 in the congruences for one-variable Rédei functions.

Although defined *a priori* over $K(\theta)$, we note that the vectors $R_n(\underline{\mathbf{x}}, \theta)$ and the matrix $A^{-1}EA$ are in fact defined over $K$, justifying the congruences (3.5), (3.6).

PROPOSITION 3.2. *The coefficients of the entries of* $R_n(\underline{\mathbf{x}}, \theta)$ *and of* $A^{-1}EA$ *lie in* $K$.

PROOF. We must show that $R_n(\underline{\mathbf{x}}, \theta)$ and $A^{-1}EA$ are invariant under the map $\sigma$ which sends $\theta$ to $\theta^q$. We write $A$ for $A(\theta)$ and recall that $EA = A(\theta^q)$ to compute

$$\begin{aligned} \sigma(R_n(\underline{\mathbf{x}}, \theta)) &= A(\theta^q)^{-1}(A(\theta^q)\underline{\mathbf{x}})^{(n)} \\ &= (EA)^{-1}(EA\underline{\mathbf{x}})^{(n)} = A^{-1}E^{-1}(EA\underline{\mathbf{x}})^{(n)}. \end{aligned} \tag{3.7}$$

Since $E\underline{\mathbf{v}}$ consists of a permutation of the entries of $\underline{\mathbf{v}}$, it is clear that $E^{-1}(E\underline{\mathbf{v}})^{(n)} = \underline{\mathbf{v}}^{(n)}$. Hence $\sigma(R_n(\underline{\mathbf{x}}, \theta)) = R_n(\underline{\mathbf{x}}, \theta)$.

Similarly, we compute

$$\begin{aligned} \sigma(A^{-1}EA) &= A(\theta^q)^{-1}EA(\theta^q) \\ &= (EA)^{-1}EEA = A^{-1}E^{-1}EEA = A^{-1}EA. \end{aligned} \tag{3.8}$$

We conclude by noting that these congruences also imply identities in Galois rings $GR(p^s, t)$. Let $L = K(\theta)$ and note that $\mathcal{O}_K/p^s\mathcal{O}_K$ is isomorphic to $GR(p^s, t)$ while $\mathcal{O}_L/p^s\mathcal{O}_L$ is isomorphic to $GR(p^s, (k+1)t)$. Reduction modulo $p^s$ then yields identities

$$R_{mq^r}(\underline{\mathbf{x}}, \theta) = A^{-1}EA \cdot R_{mq^{r-1}}(\underline{\mathbf{x}}^{(q)}, \theta^q) \quad \text{in } GR(p^s, t)[\underline{\mathbf{x}}]^{k+1} \tag{3.9}$$

whenever $r \geq 1 + (s-1)/t$; in particular

$$R_{mq}(\underline{\mathbf{x}}, \theta) = A^{-1}EA \cdot R_m(\underline{\mathbf{x}}^{(q)}, \theta^q) \quad \text{in } \mathbf{F}_q[\underline{\mathbf{x}}]^{k+1}. \tag{3.10}$$

## REFERENCES


1. M. Fried and R. Lidl, *On Dickson polynomials and Rédei functions*, Contributions to General Algebra 5: Proceedings of Salzburg Conference, Verlag B. G. Teubner, Stuttgart, 1987, pp. 139–149.
2. M. Hazewinkel, *Formal Groups and Applications*, Academic Press, New York, 1978.

3. R. Lidl, G. Mullen, and G. Turnwald, *Dickson Polynomials*, John Wiley & Sons, New York, 1993.
4. R. Matthews and R. Lidl, *On generalized Rédei functions*, International J. Math. & Math. Sci. **11** (1988), 625–634.
5. W. Nöbauer, *Rédei-Funktionen für Zweierpotenzen*, Periodica Math. Hungarica **17** (1986), 37–44.
6. J. Stienstra and F. Beukers, *On the Picard-Fuchs equation and the formal Brauer group of certain elliptic $K3$-surfaces*, Math. Annalen **271** (1985), 269–304.
7. P. T. Young, *Congruences for generalised Dickson polynomials*, Proceedings of the IMA Conference on Applications of Finite Fields, Oxford University Press (to appear).

Department of Mathematics, University of Charleston, Charleston, SC 29424

*E-mail address*: paul@math.cofc.edu