ON MODIFIED DICKSON POLYNOMIALS

Paul Thomas Young
Department of Mathematics, University of Charleston
Charleston, SC 29424
paul@math.cofc.edu

1. INTRODUCTION

The *modified Dickson polynomials*

$$Z_n(y,a) = \sum_{j=0}^{[n/2]} \frac{n}{n-j}\binom{n-j}{j}(-a)^j y^{[n/2]-j} \tag{1.1}$$

were defined and studied by P. Filipponi in the case $a = 1$ in [1], where several identities and congruences were established. In this note we generalize some of those theorems and present some new properties of these polynomials. One basic result is ([1], Proposition 2), which states that if p is an odd prime and k is an integer, then

$$Z_p(k,1) \equiv (k|p) \pmod{p}, \tag{1.2}$$

where $(k|p)$ is the Legendre symbol. The generalization is as follows:

Theorem 1. *If p is an odd prime, a, k are integers, and m, r are positive integers, then*

$$Z_{mp^r}(k,a) \equiv H_m(k) \cdot Z_{mp^{r-1}}(k,a) \pmod{p^r},$$

where

$$H_m(k) = \begin{cases} 1, & \text{if } m \text{ is even,} \\ (k|p), & \text{if } m \text{ is odd.} \end{cases}$$

We will deduce this from a corresponding congruence for these polynomials in the polynomial ring $\mathbb{Z}[y,a]$, and present a few applications thereof in the next section. We give an analogous definition of modified Dickson polynomials of the second kind and give some identities, recurrences, and congruences for them in section 3. We conclude by describing a compositeness test based on Theorem 1 in the last section.

2. CONGRUENCES FOR MODIFIED DICKSON POLYNOMIALS

The (usual) Dickson polynomials $D_n(x,a)$ are defined for $n > 0$ by

$$D_n(x,a) = \sum_{j=0}^{[n/2]} \frac{n}{n-j}\binom{n-j}{j}(-a)^j x^{n-2j} \tag{2.1}$$

(cf. [2]), with the convention that $D_0(x,a) = 2$. They may also be defined as the expansion coefficients of the rational differential form

$$\frac{dP}{P} = -\sum_{n=1}^{\infty} D_n(x,a)T^n \frac{dT}{T} \tag{2.2}$$

where $P(T) = 1 - xT + aT^2$ ([5], eq. (1.6)), and they satisfy the functional equation

$$D_n\left(u + \frac{a}{u}, a\right) = u^n + \left(\frac{a}{u}\right)^n. \tag{2.3}$$

By comparing (1.1), (2.1), we see that as polynomials in y and a,

$$Z_n(y,a) = \begin{cases} D_n(y^{1/2},a), & \text{if } n \text{ is even,} \\ y^{-1/2}D_n(y^{1/2},a), & \text{if } n \text{ is odd} \end{cases} \tag{2.4}$$

(cf. [1], eq. (1.2)). We have the following congruence for the polynomials $Z_n(y,a)$.

Theorem 2. *If p is an odd prime and m, r are positive integers, then the congruence*

$$Z_{mp^r}(y,a) \equiv H_m \cdot Z_{mp^{r-1}}(y^p, a^p) \pmod{p^r\mathbb{Z}[y,a]}$$

holds in the polynomial ring $\mathbb{Z}[y,a]$, where

$$H_m = \begin{cases} 1, & \text{if } m \text{ is even,} \\ y^{(p-1)/2}, & \text{if } m \text{ is odd.} \end{cases}$$

Proof. In ([5], Theorem 2) we showed that the congruence

$$D_{mp^r}(x,a) \equiv D_{mp^{r-1}}(x^p, a^p) \pmod{p^r\mathbb{Z}[x,a]} \tag{2.5}$$

holds in the polynomial ring $\mathbb{Z}[x,a]$. Replacing the indeterminate x with $y^{1/2}$ yields

$$D_{mp^r}(y^{1/2},a) \equiv D_{mp^{r-1}}(y^{p/2}, a^p) \pmod{p^r\mathbb{Z}[y^{1/2},a]}, \tag{2.6}$$

where $y^{p/2}$ is defined to be $(y^{1/2})^p$. By (2.4), this gives the result for even m, since both sides of the congruence (2.6) lie in $\mathbb{Z}[y,a]$ in that case. For odd m, we divide both sides of (2.6) by $y^{1/2}$ to obtain the congruence

$$y^{-1/2}D_{mp^r}(y^{1/2},a) \equiv y^{(p-1)/2}\cdot(y^{-p/2}D_{mp^{r-1}}(y^{p/2},a^p)) \pmod{p^r\mathbb{Z}[y,a]}, \tag{2.7}$$

both sides of which now lie in $\mathbb{Z}[y,a]$. Comparison with (2.4) now gives the result for odd m.

Theorem 1 may be obtained directly from this as follows.

Proof of Theorem 1. Let a, k be integers, and consider them as elements of the ring $\mathbb{Z}_p$ of p-adic integers. For an element u of $\mathbb{Z}_p$, the Teichmüller representative $\hat{u}$ of u is defined to be the unique solution to $x^p = x$ which is congruent to u modulo $p\mathbb{Z}_p$; it is also given by the p-adic limit $\hat{u} = \lim_{r\to\infty} u^{p^r}$. Observing that $\hat{a}^p = \hat{a}$, $\hat{k}^p = \hat{k}$, and $\hat{k}^{(p-1)/2} = (k|p)$, we evaluate the polynomial congruence of Theorem 2 at $y = \hat{k}$, $a = \hat{a}$ to obtain

$$Z_{mp^r}(\hat{k},\hat{a}) \equiv H_m(k)\cdot Z_{mp^{r-1}}(\hat{k},\hat{a}) \pmod{p^r\mathbb{Z}_p}, \tag{2.8}$$

where $H_m(k)$ is as defined in the statement of the theorem.

Now from the second statement of ([5], Theorem 3) applied with $i = 1$, $n = 1$, and $K = \mathbb{Q}_p(\sqrt{k})$, it follows that

$$D_{mp^r}(k^{1/2},a) \equiv D_{mp^r}(\hat{k}^{1/2},\hat{a}) \pmod{\pi p^r\mathfrak{O}_K} \tag{2.9}$$

for all r, where (π) is the maximal ideal in the ring of integers $\mathfrak{O}_K$ of the field K. For m even, comparison of (2.8) and (2.9) yields

$$D_{mp^r}(k^{1/2},a) \equiv D_{mp^{r-1}}(k^{1/2},a) \pmod{\pi p^{r-1}\mathfrak{O}_K}, \tag{2.10}$$

but both sides of this congruence are integers, so it must hold modulo $p^r\mathbb{Z}$. In this case the theorem then follows by comparison with (2.4).

If m is odd and $\hat{k} \neq 0$, multiplying both sides of (2.8) by $\hat{k}^{1/2}$ yields

$$D_{mp^r}(\hat{k}^{1/2}, \hat{a}) \equiv (k|p) \cdot D_{mp^{r-1}}(\hat{k}^{1/2}, \hat{a}) \pmod{p^r \mathfrak{O}_K}. \tag{2.11}$$

Comparison with (2.9) shows that

$$D_{mp^r}(k^{1/2}, a) \equiv (k|p) \cdot D_{mp^{r-1}}(k^{1/2}, a) \pmod{\pi p^{r-1} \mathfrak{O}_K}, \tag{2.12}$$

and then dividing by $k^{1/2}$ yields

$$Z_{mp^r}(k, a) \equiv (k|p) \cdot Z_{mp^{r-1}}(k, a) \pmod{\pi p^{r-1} \mathfrak{O}_K}, \tag{2.13}$$

but again both sides of this congruence are integers, so it holds modulo $p^r \mathbb{Z}$, proving the theorem in that case.

Finally, when $\hat{k} = 0$ and n is odd we have the identity $Z_n(0, a) = (-a)^{(n-1)/2} \cdot n$ (cf. [1], eq. (2.7)), so that $Z_{mp^r}(0, a) \equiv 0 \pmod{p^r}$ when m is odd. Combining this with (2.9), we see that in this case we also have

$$Z_{mp^r}(k, a) \equiv H_m(k) \cdot Z_{mp^{r-1}}(k, a) \pmod{\pi p^{r-1} \mathfrak{O}_K}, \tag{2.14}$$

but again both sides are integers, proving the theorem.

Remarks. Perhaps the most interesting feature of these theorems is that while the "special element" H_m depends on y and on the parity of m, it does not depend on a. For example, taking $m = 1$, $r = 1$ in Theorem 1 and observing that $Z_1(y, a) = 1$ yields

$$Z_p(k, a) \equiv (k|p) \pmod{p}, \tag{2.15}$$

of which Filipponi's result (1.2) is a special case; indeed it is evident from (1.1) that $Z_p(k, a) \equiv k^{(p-1)/2} \pmod{p}$ for all a. In section 4 below we propose a compositeness test based on (2.15).

One also obtains interesting congruences by combining Theorem 1 above with Filipponi's multiplication formula ([1], eq. (3.6)). For example, for n even the $h = 3$ case of Filipponi's result is the identity

$$Z_{3n} = Z_n^3 - 3Z_n \tag{2.16}$$

(cf. [1], eq. (3.5)), where $Z_n = Z_n(k,1)$. Putting $n = m \cdot 3^r$ with m even, from Theorem 1.1 we obtain $Z_{3n} \equiv Z_n \pmod{3^{r+1}}$; combining this with (2.16) yields $Z_n(Z_n^2 - 4) \equiv 0 \pmod{3^{r+1}}$. It follows that if n is even and divisible by 3^r, then Z_n is congruent to either -2, 0, or 2 modulo 3^{r+1}. A similar but slightly more complicated result holds for n odd. Many other such results may be similarly obtained.

We conclude this section with a generating form and recurrence for the $Z_n(y,a)$, which provides an efficient means for generating the sequence and for obtaining identities.

Theorem 3. *For $n > 0$ the polynomials $Z_n(y,a)$ may be obtained as the expansion coefficients of the rational differential form*

$$\sum_{n=1}^{\infty} Z_n(y,a)T^n \frac{dT}{T} = \frac{(1-(2a-y)T - aT^2 - 2a^2T^3)\,dT}{1+(2a-y)T^2 + a^2T^4}.$$

Consequently, the sequence $Z_n = Z_n(y,a)$ is given by the recurrence

$$Z_0 = 2, \quad Z_1 = 1, \quad Z_2 = y - 2a, \quad Z_3 = y - 3a, \quad \text{and} \quad Z_{n+2} = (y-2a)Z_n - a^2 Z_{n-2}.$$

Proof. Use (2.4) to write the power series

$$\begin{aligned}\sum_{n=1}^{\infty} Z_n T^{n-1} = \frac{1}{2}y^{-1/2}\sum_{n=1}^{\infty} D_n(y^{1/2},a)(T^{n-1} + (-T)^{n-1}) \\ + \frac{1}{2}\sum_{n=1}^{\infty} D_n(y^{1/2},a)(T^{n-1} - (-T)^{n-1})\end{aligned} \tag{2.17}$$

as the sum of an even function of T and an odd function of T. Then from (2.2) we obtain

$$-\sum_{n=1}^{\infty} Z_n(y,a)T^n \frac{dT}{T} = \frac{1}{2}\left((1+y^{-1/2})\frac{dP(T)}{P(T)} + (1-y^{-1/2})\frac{dP(-T)}{P(-T)}\right), \tag{2.18}$$

where $P(T) = 1 - y^{1/2}T + aT^2$. Expanding and simplifying (2.18) yields the first statement of the theorem. The recurrence follows by multiplying both sides by $1+(2a-y)T^2 + a^2T^4$ and equating coefficients of $T^n\,dT$.

3. MODIFIED DICKSON POLYNOMIALS OF THE SECOND KIND.

The Dickson polynomials of the second kind $E_n(x,a)$ are defined for $n \geq 0$ by

$$E_n(x,a) = \sum_{j=0}^{[n/2]} \binom{n-j}{j} (-a)^j x^{n-2j} \tag{3.1}$$

(cf. [2]). They may also be defined as the expansion coefficients of the rational differential form

$$\frac{dT}{P(T)} = \sum_{n=0}^{\infty} E_n(x,a) T^n \, dT \tag{3.2}$$

where $P(T) = 1 - xT + aT^2$ ([5], eq. (4.4)). By way of analogy with (1.1) we define the *modified Dickson polynomials of the second kind* $Y_n(y,a)$ by

$$Y_n(y,a) = \sum_{j=0}^{[n/2]} \binom{n-j}{j} (-a)^j y^{[n/2]-j}. \tag{3.3}$$

Comparison of (3.1), (3.3) shows that as polynomials in y and a,

$$Y_n(y,a) = \begin{cases} E_n(y^{1/2}, a), & \text{if } n \text{ is even,} \\ y^{-1/2} E_n(y^{1/2}, a), & \text{if } n \text{ is odd.} \end{cases} \tag{3.4}$$

From this definition we deduce the following generating form for the polynomials $Y_n(y,a)$.

Theorem 4. *The polynomials $Y_n(y,a)$ may be obtained as the expansion coefficients of the rational differential form*

$$\sum_{n=0}^{\infty} Y_n(y,a)\, T^n \, dT = \frac{(1 + T + aT^2)\, dT}{1 + (2a - y)T^2 + a^2 T^4}.$$

Consequently, the sequence $Y_n = Y_n(y,a)$ is given by the recurrence

$$Y_0 = 1, \quad Y_1 = 1, \quad Y_2 = y - a, \quad Y_3 = y - 2a, \quad \text{and} \quad Y_{n+2} = (y - 2a)Y_n - a^2 Y_{n-2}.$$

Proof. Use (3.4) to write the power series $\sum_n Y_n(y,a)T^n$ as the sum of an even function of T and an odd function of T. Then from (3.2) we obtain

$$\sum_{n=0}^{\infty} Y_n(y,a) T^n \, dT = \frac{1}{2} \left((1 + y^{-1/2}) \frac{dT}{P(T)} + (1 - y^{-1/2}) \frac{dT}{P(-T)} \right), \tag{3.5}$$

where $P(T) = 1 - y^{1/2}T + aT^2$. Expanding and simplifying (3.5) yields the first statement of the theorem. The recurrence follows by multiplying both sides by $1 + (2a - y)T^2 + a^2T^4$ and equating coefficients of $T^n\,dT$.

The generating functions for Y_n and Z_n may be used directly to deduce several identities relating them to D_n and E_n, some of which we record here.

Theorem 5. *In the polynomial ring $\mathbb{Z}[y, a]$ we have the identities*

$$(i) \qquad Y_{2m-1}(y, a) = E_{m-1}(y - 2a, a^2) \qquad \text{for } m > 0,$$

$$(ii) \qquad Z_{2m}(y, a) = D_m(y - 2a, a^2) \qquad \text{for } m \geq 0,$$

$$(iii) \qquad Y_{2m}(y, a) + Z_{2m+1}(y, a) = 2E_m(y - 2a, a^2) \qquad \text{for } m \geq 0,$$

$$(iv) \qquad Y_{2m}(y, a) - Z_{2m+1}(y, a) = 2aE_{m-1}(y - 2a, a^2) \qquad \text{for } m > 0.$$

Proof. For (iii), use Theorems 3 and 4 and equation (3.2) to write

$$\begin{aligned} \sum_{n=0}^{\infty} (Y_n + Z_{n+1})T^n\,dT &= \frac{2\,dT}{1 + (2a - y)T^2 + a^2T^4} + (\text{odd function of } T)\,dT \\ &= 2\sum_{m=0}^{\infty} E_m(y - 2a, a^2)T^{2m}\,dT + (\text{odd function of } T)\,dT. \end{aligned} \tag{3.6}$$

Equating coefficients of $T^{2m}\,dT$ gives the result. The other parts are similarly obtained.

Remarks. Replacing y with y^2 in (ii) and using (2.4) yields the $n = 2$ case of the familiar composition formula

$$D_{mn}(y, a) = D_m(D_n(y, a), a^n) \tag{3.7}$$

for the usual Dickson polynomials. An analogous formula

$$E_{2m-1}(y, a) = y \cdot E_{m-1}(D_2(y, a), a^2) \tag{3.8}$$

is similarly obtained from (i). Similar composition formulae for E_{2m} and D_{2m+1} may be obtained by combining (iii) and (iv) and replacing y with y^2.

Another set of identities relating the polynomials Y_n and Z_n may be obtained from the observation that the characteristic polynomial $1+(2a-y)T^2+a^2T^4$ is invariant under the transformation $a \mapsto -a$, $y \mapsto y-4a$, as follows.

Theorem 6. *If m is a nonnegative integer we have, as identities in the polynomial ring $\mathbb{Z}[y,a]$,*

$$(i) \qquad Z_{2m+1}(y-4a,-a) = Y_{2m}(y,a),$$

$$(ii) \qquad Z_{2m}(y-4a,-a) = Z_{2m}(y,a),$$

$$(iii) \qquad Y_{2m}(y-4a,-a) = Z_{2m+1}(y,a),$$

$$(iv) \qquad Y_{2m+1}(y-4a,-a) = Y_{2m+1}(y,a).$$

Proof. Using the generating form from Theorem 3, we compute

$$\begin{aligned}\sum_{n=1}^{\infty} Z_n(y-4a,-a)T^n\frac{dT}{T} &= \frac{(1-(2a-y)T+aT^2-2a^2T^3)\,dT}{1+(2a-y)T^2+a^2T^4} \\ &= \frac{(-(2a-y)T-2a^2T^3)\,dT}{1+(2a-y)T^2+a^2T^4} + \frac{(1+aT^2)\,dT}{1+(2a-y)T^2+a^2T^4}.\end{aligned} \tag{3.9}$$

Noting that the even part of this form agrees with the even part of the generating form for Y_n from Theorem 4, and the odd part of (3.9) agrees with the odd part of the generating form for Z_n from Theorem 3, gives results (i), (ii). Repeating the argument starting from the generating form for Y_n from Theorem 4 gives (iii), (iv).

Remark. Parts (i) and (iii) of this theorem are equivalent.

Finally, we will use the results of Theorems 5 and 6 to give an analogue of Theorem 1 for the values of the polynomials Y_n.

Theorem 7. *If p is an odd prime, a, k are integers, and m, r are positive integers, then*

$$Y_{mp^r-1}(k,a) \equiv G_m(k) \cdot Y_{mp^{r-1}-1}(k,a) \pmod{p^r},$$

where

$$G_m(k) = \begin{cases} (k(k-4a)|p), & \text{if } m \text{ is even,} \\ (k-4a|p), & \text{if } m \text{ is odd.} \end{cases}$$

Proof. First suppose $m = 2j$ is even. From Theorem 5(i), we have $Y_{mp^r-1}(k,a) = E_{jp^r-1}(k-2a, a^2)$ for all $r \geq 0$. Using the congruence

$$E_{jp^r-1}(x,a) \equiv (x^2 - 4a|p) \cdot E_{jp^{r-1}-1}(x,a) \pmod{p^r} \tag{3.10}$$

([5], Corollary C; [4], Corollary 1(i)) with $x = k - 2a$ and a replaced with a^2 yields the result for even m.

If m is odd, then $mp^r - 1$ is even for all $r \geq 0$, and from Theorem 6(i) we have $Y_{mp^r-1}(y,a) = Z_{mp^r}(y-4a, -a)$. The result in this case then follows from the odd m case of Theorem 1.

Remarks. While it is possible to prove a polynomial congruence which holds modulo $p^r\mathbb{Z}[y,a]$ (analogous to Theorem 2) for the Y_n, the resulting congruence is rather inelegant due to the cumbersome "lifting of Frobenius" involved (cf. [5], Remark A.2, p.43). However, the "mod p" case of this congruence may be stated rather simply: If p is an odd prime and m is a positive integer, then the congruence

$$Y_{mp-1}(y,a) \equiv G_m \cdot Y_{m-1}(y^p, a^p) \pmod{p\mathbb{Z}[y,a]} \tag{3.11}$$

holds in the polynomial ring $\mathbb{Z}[y,a]$, where

$$G_m = \begin{cases} (y(y-4a))^{(p-1)/2}, & \text{if } m \text{ is even,} \\ (y-4a)^{(p-1)/2}, & \text{if } m \text{ is odd.} \end{cases} \tag{3.12}$$

For m even, this follows from Theorem 5(i) and ([5], Theorem 5); for m odd it follows from Theorem 6(i) and the odd m case of Theorem 2. In particular, the special case $m = 1$ yields the congruence

$$Y_{p-1}(y,a) \equiv (y-4a)^{(p-1)/2} \pmod{p\mathbb{Z}[y,a]}, \tag{3.12}$$

and the case $m = 2$ yields

$$Y_{2p-1}(y,a) \equiv (y(y-4a))^{(p-1)/2} \pmod{p\mathbb{Z}[y,a]}. \tag{3.13}$$

4. A COMPOSITENESS TEST.

The congruence (2.15) furnishes a compositeness test which contains the usual Dickson polynomial test and the Solovay-Strassen test as special cases. If n is a prime then for all integers k and a we have

$$Z_n(k,a) \equiv (k|n) \pmod{n} \tag{4.1}$$

by (2.15), where $(k|n)$ now (and throughout this section) denotes the Jacobi symbol. If n is odd then in the special case where $a = 0$ the congruence (4.1) becomes

$$k^{(n-1)/2} \equiv (k|n) \pmod{n}, \tag{4.2}$$

which is the basis for the Solovay-Strassen test. On the other hand, suppose n is odd and k is a quadratic residue modulo n. Writing $k \equiv b^2 \pmod{n}$ and using (2.4) we have

$$bZ_n(k,a) \equiv bZ_n(b^2,a) = D_n(b,a) \pmod{n}, \tag{4.3}$$

whereas $(k|n) = 1$. So in the case where k is a quadratic residue modulo n the congruence (4.1) is equivalent to the congruence

$$D_n(b,a) \equiv b \pmod{n}, \tag{4.4}$$

which is the basis of the usual Dickson polynomial compositeness test.

If n is a prime, it is clear that (4.4) is satisfied for all integers a and b from (2.5) with $m = r = 1$ and $p = n$; and (4.2) is likewise satisfied for all integers k. However, if n is an odd composite number then there exist values of k with $(k,n) = 1$ for which (4.2) holds; in this case n is said to be an *Euler pseudoprime* to the base k. Furthermore, if n is an odd composite it may happen that (4.4) is satisfied for all integers b and a fixed integer

a, in which case n is said to be a *strong Dickson pseudoprime* to the base a (cf. [2]). It is even possible that n may be a strong Dickson pseudoprime to every base; that is, (4.4) may hold for all integers a and b, although n is not prime.

It is quite easy to see that the compositeness test we propose based on the congruence (4.1) admits no "strong pseudoprimes" to any given base a; in fact, if n is not prime then for any a the congruence (4.1) fails at least half the time, as we now record.

Theorem 8. *Let n be an odd composite integer, and let U_n denote the group of units in the ring $\mathbb{Z}/n\mathbb{Z}$. Then for any integer a, the congruence* (4.1) *fails for at least half the elements k of U_n.*

Proof. First suppose that n is a non-square, and write $n = p^e m$ with p prime, e odd, and $(m, p) = 1$. Suppose (4.1) holds for $k = b$. Using the Chinese remainder theorem, choose an integer c such that $c \equiv b \pmod{m}$ and $(c|p) = -(b|p)$. It follows that $(c|n) = -(b|n)$ but $Z_n(c, a) \equiv Z_n(b, a) \pmod{m}$; hence (4.1) cannot hold for $k = c$. Using the isomorphism $U_n \cong U_m \times U_{p^e}$ we see that in fact half the integers c congruent to b modulo m have $(c|p) = -(b|p)$. Therefore in any congruence class modulo m at most half the elements k can satisfy (4.1). The theorem then follows in this case.

Now suppose that n is a square, and write $n = p^2 m$ with p prime. Since n is a square we have $(k|n) = 1$ for all integers k. Suppose then that (4.1) holds for $k = b$; then evaluating the polynomial congruence of Theorem 2 with $r = 2$ at $a = a$, $y = b$ yields

$$1 \equiv Z_{mp^2}(b, a) \equiv b^{(p-1)/2} Z_{mp}(b^p, a^p) \pmod{p^2}. \tag{4.5}$$

Now if c is any integer congruent to b modulo p, then $c^p \equiv b^p \pmod{p^2}$ and therefore $Z_{mp}(c^p, a^p) \equiv Z_{mp}(b^p, a^p) \pmod{p^2}$. However, if $c \equiv b \pmod{p}$ then $c^{(p-1)/2} \not\equiv b^{(p-1)/2} \pmod{p^2}$ unless $c \equiv b \pmod{p^2}$. Thus if $c \equiv b \pmod{p}$ but $c \not\equiv b \pmod{p^2}$ then (4.1) cannot hold for $k = c$. Rewriting n as $n = p^e m'$ with e even and $(p, m') = 1$, and using the isomorphism $U_n \cong U_{m'} \times U_{p^e}$ shows that more than half the integers $c \in U_n$ which are congruent to b modulo p are not congruent to b modulo p^2. The theorem then follows in this case.

The test described here may be implemented in time commensurate with that required for other well-known tests. Using the identities

$$Z_{2n}(k,a) = \begin{cases} Z_n(k,a)^2 - 2a^n, & \text{if } n \text{ is even,} \\ kZ_n(k,a)^2 - 2a^n, & \text{if } n \text{ is odd,} \end{cases} \tag{4.6}$$

$$Z_{2n+1}(k,a) = Z_{n+1}(k,a)Z_n(k,a) - a^n \tag{4.7}$$

and the recursion

$$Z_{n+1}(k,a) = \begin{cases} Z_n(k,a) - aZ_{n-1}(k,a), & \text{if } n \text{ is even,} \\ kZ_n(k,a) - aZ_{n-1}(k,a), & \text{if } n \text{ is odd,} \end{cases} \tag{4.8}$$

one may compute $Z_n(k,a)$ with $O(\log n)$ multiplications, as outlined in ([2], Lemma 2.5) for $D_n(k,a)$. The identities (4.6)-(4.8) were given in the case $a = 1$ in ([1], equations (3.2)-(3.4)), and are proved for general a in the same manner.

REFERENCES

1. P. Filipponi. "Modified Dickson Polynomials", *The Fibonacci Quarterly* **35.1** (1997), 11-18.
2. R. Lidl, G. Mullen, and G. Turnwald. *Dickson Polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics, Vol. 65 (1993), Longman Scientific and Technical, Essex, England.
3. H. Wilf. *Generatingfunctionology*, Academic Press, Boston-San Diego-New York, 1990.
4. P. T. Young. "p-adic Congruences for Generalized Fibonacci Sequences", *The Fibonacci Quarterly* **32.1** (1994), 2-10.
5. P. T. Young. "Congruences for Generalised Dickson Polynomials", *in* Applications of Finite Fields, IMA Conference Series, Vol. 59 (1996), D. Gollman, ed., Oxford University Press, 33-46.

AMS Classification Numbers: 11B39, 11A07