A SHORT PROOF OF CONGRUENCES FOR LUCAS SEQUENCES

MASAKAZU YAMAGISHI

Abstract. We present a short alternative proof of congruences for Lucas sequences. We also mention a known connection with Honda's work on formal groups.

1. Introduction

Let $D_n(x,y)$ and $E_n(x,y)$ denote the Dickson polynomials of the first and second kind, respectively, as defined in [6]. We adopt Schur's notation $\mathscr{E}_n(x,y) = E_{n-1}(x,y)$. The values of Dickson polynomials at integers are called Lucas sequences. For a prime number p, let ν_p denote the additive p-adic valuation. The purpose of this note is to give a short and elementary proof of the following congruences for Lucas sequences.

Theorem 1.1. *Let p be a prime number, $a, b \in \mathbb{Z}$, and $n \geq 1$.*

(i) We have

$$D_{pn}(a,b) \equiv D_n(a,b) \pmod{p^{1+\nu_p(n)}}.$$

(ii) We have

$$\mathscr{E}_{pn}(a,b) \equiv \left(\frac{D}{p}\right) \mathscr{E}_n(a,b) \pmod{p^{1+\nu_p(n)}},$$

where $D = a^2 - 4b$ and $\left(\frac{D}{p}\right)$ is the Kronecker symbol (cf. [5]).

These congruences are due to Robbins [7]. Robbins' proof is elementary, but rather long. Young [11] utilized p-adic methods to obtain (ii). In [10], Young interpreted generalized Dickson polynomials as coefficients of the canonical invariant differential of a certain formal group. That the formal group is strongly isomorphic over an appropriate ring to the formal multiplicative group then yields congruences for generalized Dickson polynomials (Theorem 3 and Corollary C in [10]), of which (i) and (ii) are special cases.

Our method is different from previous ones. We use polynomial properties of Dickson polynomials (Lemma 2.1) to derive integer congruences for the values of those polynomials. This makes the proof of Theorem 1.1 efficient.

2. Dickson Polynomials

Dickson polynomials of the first and second kind, respectively, are defined by recurrence formulas

$$\begin{aligned} D_n(x,y) &= xD_{n-1}(x,y) - yD_{n-2}(x,y) \ (n \geq 2), \\ E_n(x,y) &= xE_{n-1}(x,y) - yE_{n-2}(x,y) \ (n \geq 2), \end{aligned} \tag{2.1}$$

This work was supported by JSPS KAKENHI Grant Number JP17K05168.

with $D_0(x,y)=2$, $D_1(x,y)=x$, $E_0(x,y)=1$, and $E_1(x,y)=x$. They are characterized by the identities

$$D_n(u_1+u_2,u_1u_2)=u_1^n+u_2^n, \tag{2.2}$$
$$E_n(u_1+u_2,u_1u_2)=\frac{u_1^{n+1}-u_2^{n+1}}{u_1-u_2}$$

for indeterminates u_1 and u_2. Moreover, they have explicit expressions

$$D_n(x,y)=\sum_{j=0}^{\lfloor n/2\rfloor}\frac{n}{n-j}\binom{n-j}{j}(-y)^j x^{n-2j}, \tag{2.3}$$
$$E_n(x,y)=\sum_{j=0}^{\lfloor n/2\rfloor}\binom{n-j}{j}(-y)^j x^{n-2j}$$

for $n\geq 1$. Recall that we adopt Schur's notation

$$\mathscr{E}_n(x,y)=E_{n-1}(x,y)\quad(n\geq 1).$$

The following identities are easily shown.

Lemma 2.1.

$$D_{mn}(x,y)=D_m(D_n(x,y),y^n), \tag{2.4}$$
$$\mathscr{E}_{mn}(x,y)=\mathscr{E}_m(D_n(x,y),y^n)\mathscr{E}_n(x,y). \tag{2.5}$$
$$D_n(x,y)^2-(x^2-4y)\mathscr{E}_n(x,y)^2=4y^n. \tag{2.6}$$
$$\frac{\partial}{\partial x}D_n(x,y)=n\mathscr{E}_n(x,y)\quad(n\geq 1), \tag{2.7}$$
$$\frac{\partial}{\partial y}D_n(x,y)=-n\mathscr{E}_{n-1}(x,y)\quad(n\geq 2).$$

3. Congruences

Let p be a fixed prime number. We start with polynomial congruences.

Lemma 3.1. *In the ring $\mathbb{Z}[x,y]$, we have the following congruences:*

$$D_p(x,y)\equiv x^p\pmod p, \tag{3.1}$$
$$\mathscr{E}_p(x,y)\equiv(x^2-4y)^{(p-1)/2}\pmod p. \tag{3.2}$$

Note that (3.2) *makes sense even for $p=2$.*

Proof. The congruence (3.1) follows from (2.3). The congruence (3.2) for $p=2$ is clear. If p is odd, then

$$\mathscr{E}_p(u_1+u_2,u_1u_2)=\frac{u_1^p-u_2^p}{u_1-u_2}\equiv(u_1-u_2)^{p-1}=\left((u_1+u_2)^2-4u_1u_2\right)^{(p-1)/2},$$

which implies (3.2). □

Let ν_p denote the additive p-adic valuation, extended to $f\in\mathbb{Z}[x]$:

$$\nu_p(f)=\max\{k\,;f\equiv 0\pmod{p^k}\}.$$

The following Lemma is essentially the "lifting the exponent" lemma in [8], where $\nu_p(\mathscr{E}_n(a,b))$ is investigated.

Lemma 3.2. *Let $f, g, h \in \mathbb{Z}[x]$ and put $k = \nu_p(g-h)$. If $k \geq 1$, then*

$$\nu_p(f(g) - f(h)) \geq k + \nu_p(df/dx).$$

Proof. Let $n \geq 1$. It follows from

$$g^n - h^n = \sum_{j=1}^{n} \binom{n}{j} (g-h)^j h^{n-j} = \sum_{j=1}^{n} \frac{n}{j} \binom{n-1}{j-1} (g-h)^j h^{n-j}$$

that $\nu_p(g^n - h^n) \geq \nu_p(n) - \nu_p(j) + kj$ for some $j \geq 1$. Since

$$j \geq p^{\nu_p(j)} \geq 1 + (p-1)\nu_p(j) \geq 1 + \nu_p(j),$$

we find that

$$\nu_p(g^n - h^n) \geq \nu_p(n) - \nu_p(j) + kj \geq k + \nu_p(n).$$

If $f(x) = \sum_n a_n x^n$, then we have

$$\nu_p(f(g) - f(h)) \geq k + \min\{\nu_p(a_n) + \nu_p(n); n \geq 1\} = k + \nu_p(df/dx)$$

as desired. □

Now, we are ready to prove Theorem 1.1.

Proof of Theorem 1.1. (i) Applying Lemma 3.2 to $(f, g, h) = (D_n(x, b^p), D_p(a, b), a^p)$ and using (2.4), we obtain

$$D_{pn}(a, b) = f(g) \equiv f(h) = D_n(a^p, b^p) \pmod{p^{1+\nu_p(n)}},$$

since we have $\nu_p(g-h) \geq 1$ by (3.1) and $\nu_p(df/dx) \geq \nu_p(n)$ by (2.7). Applying Lemma 3.2 to $(f, g, h) = (D_n(a^p, x), b^p, b)$ and then to $(f, g, h) = (D_n(x, b), a^p, a)$, we obtain similarly

$$D_n(a^p, b^p) \equiv D_n(a^p, b) \equiv D_n(a, b) \pmod{p^{1+\nu_p(n)}}.$$

(ii) First, we notice the congruence

$$\mathscr{E}_p(D_n(a, b), b^n) \equiv \left((a^2 - 4b)\mathscr{E}_n(a, b)^2\right)^{(p-1)/2} \pmod{p}, \tag{3.3}$$

which follows from (2.6) and (3.2) and makes sense even for $p = 2$. Using (2.5) and (3.3) one deduces, by induction on $\nu_p(n)$, that $\nu_p(\mathscr{E}_n(a, b)) \geq \nu_p(n)$ if $p | D = a^2 - 4b$, and that $\nu_p(\mathscr{E}_n(a, b)) \geq 1 + \nu_p(n)$ if $p | \mathscr{E}_n(a, b)$. So, the claimed congruence holds true if $p | D\mathscr{E}_n(a, b)$, both sides being zero.

Suppose $p \geq 3$ and $p \nmid D\mathscr{E}_n(a, b)$. By (2.6), Theorem 1.1 (i), and that $b^{pn} \equiv b^n \pmod{p^{1+\nu_p(n)}}$, we obtain

$$\mathscr{E}_{pn}(a, b)^2 - \mathscr{E}_n(a, b)^2 \equiv 0 \pmod{p^{1+\nu_p(n)}}. \tag{3.4}$$

On the other hand, it follows from (2.5) and (3.3) that

$$\mathscr{E}_{pn}(a, b) \equiv \left(\frac{D}{p}\right) \mathscr{E}_n(a, b) \pmod{p},$$

so the desired congruence follows from (3.4).

The remaining case is where $p = 2$ and a and $\mathscr{E}_n(a, b)$ are odd. We note that $\left(\frac{D}{2}\right) = (-1)^b$ in this case. Since $\mathscr{E}_{2n}(a, b) = D_n(a, b)\mathscr{E}_n(a, b)$, what we have to show is

$$D_n(a, b) \equiv (-1)^b \pmod{2^{1+\nu_2(n)}}. \tag{3.5}$$

As shown in the proof of (i), the left side of (3.5) remains unchanged if a or b is replaced by its square. The proof of (3.5) is therefore reduced to the case $(a, b) = (1, 0)$ or $(1, 1)$. By (2.2) we have $D_n(1, 0) = 1$, so (3.5) holds true if $(a, b) = (1, 0)$. By the recurrence (2.1), we see that the sequence $\{D_n(1, 1)\}_{n \geq 0}$ is 6-periodic, starting with $2, 1, -1, -2, -1, 1$. Because we

are assuming $\mathscr{E}_n(1,1)$ is odd, $D_n(1,1)$ is also odd by (2.6). Putting these together, we have $D_n(1,1) \equiv -1 \pmod{2^{1+\nu_2(n)}}$, so (3.5) holds true if $(a,b) = (1,1)$.

This completes the proof. □

4. Concluding Remark

We mention a connection with Honda's work on formal groups. Coleman and McGuinness [2] showed that, over a field K of characteristic zero, any formal group that is a rational function is of the form

$$F(X,Y) = \frac{X+Y-aXY}{1-bXY} \tag{4.1}$$

for some $a, b \in K$ (see also Bismuth [1], Walker [9]).

Proposition 4.1. *Let $a, b \in \mathbb{Z}$ and $D = a^2 - 4b$. The formal group (4.1) is strongly isomorphic over $\mathbb{Z}$ to the formal group G, which is obtained from the Dirichlet L-function $\sum_{n=1}^{\infty} \left(\frac{D}{n}\right) n^{-s}$ (cf. Honda* [3, Theorem 4]*).*

Proof. We follow the terminology of Honda [4]. One sees that the invariant differential of F is

$$\omega = \frac{dX}{1-aX+bX^2},$$

and the transformer

$$f(X) = \int \omega = \sum_{n=1}^{\infty} \mathscr{E}_n(a,b) \frac{X^n}{n}.$$

By Theorem 1.1 (ii), we have

$$pf(X) - \left(\frac{D}{p}\right) f(X^p) \in p\mathbb{Z}_p[[X]],$$

which means that the transformer f is of type $p - \left(\frac{D}{p}\right) T$, the same type as the formal group G in [3, Theorem 4]. Because this holds for all primes p, and because the type of a formal group determines its strong isomorphism class over $\mathbb{Z}_p$ ([4, Theorem 2]), we complete the proof. □

We remark that this is known. In [12], Young constructed the isomorphism between F and G directly and used it to prove quadratic reciprocity.

Acknowledgment

The author thanks the referee for informing him of the works of Robbins [7] and of Young [12].

References

[1] R. Bismuth, *Rational Formal Group Laws*, Master's thesis, McMaster University, 1976, `http://hdl.handle.net/11375/9845`.
[2] R. F. Coleman and F. O. McGuinness, *Rational formal group laws*, Pacific J. Math., **147** (1991), no. 1, 25–27.
[3] T. Honda, *Formal groups and zeta-functions*, Osaka J. Math., **5** (1968), 199–213.
[4] T. Honda, *On the theory of commutative formal groups*, J. Math. Soc. Japan, **22** (1970), 213–246.
[5] F. Lemmermeyer, *Reciprocity Laws. From Euler to Eisenstein*, Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000.
[6] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics, 65, Longman Scientific & Technical, Harlow; copublished in the United States with John Wiley & Sons, Inc., New York, 1993.

[7] N. Robbins, *Some congruence properties of binomial coefficients and linear second order recurrences*, Internat. J. Math. Math. Sci., **11** (1988), no. 4, 743–750.
[8] C. Sanna, *The p-adic valuation of Lucas sequences*, The Fibonacci Quarterly, **54.2** (2016), 118–124.
[9] A. Walker, *Formal groups and where to find them*, Feb. 5, 2017, `https://awwalker.com/2017/02/05/formal-groups-and-where-to-find-them`.
[10] P. T. Young, *Congruences for generalised Dickson polynomials*, Applications of Finite Fields (Egham, 1994), 33–46, Inst. Math. Appl. Conf. Ser. New Ser., 59, Oxford Univ. Press, New York, 1996.
[11] P. T. Young, *p-Adic congruences for generalized Fibonacci sequences*, The Fibonacci Quarterly, **32.1** (1994), 2–10.
[12] P. T. Young, *Quadratic reciprocity via Lucas sequences*, The Fibonacci Quarterly, **33.1** (1995), 78–81.

MSC2010: 11B39, 12E10, 14L05

Department of Mathematics, Nagoya Institute of Technology, Gokiso-cho, Showa-ku, Nagoya, Aichi 466-8555, Japan
Email address: `yamagishi.masakazu@nitech.ac.jp`