QUADRATIC RECIPROCITY VIA LUCAS SEQUENCES

Paul Thomas Young
Department of Mathematics, University of Charleston, Charleston, SC 29424

(Submitted June 1993)

1. INTRODUCTION

Given $\lambda, \mu \in \mathbb{Z}$, the associated Lucas sequence $\{\gamma_n\}_{n\geq 0}$ is defined by the binary linear recurrence

$$\gamma_0 = 0, \ \gamma_1 = 1, \ \text{and} \ \gamma_{n+1} = \lambda\gamma_n + \mu\gamma_{n-1} \ \text{for} \ n > 0. \tag{1.1}$$

In this article we will show how these sequences may be used to give new proofs of the quadratic reciprocity theorem. It is well known that these sequences have the ordinary formal power series generating functions

$$P(t)^{-1} = \sum_{n=1}^{\infty} \gamma_n t^{n-1}, \tag{1.2}$$

where $P(t) = 1 - \lambda t - \mu t^2$. The reciprocity law follows from certain integrality relations in the formal power series ring $\mathbb{Q}[\![t]\!]$ between these generating functions and a generating function for the quadratic character modulo the discriminant of $P(t)$. The only other tools needed are the elementary properties of quadratic Gauss sums.

2. LUCAS SEQUENCES AND THE LEGENDRE SYMBOL

The following formal power series identity expresses an interesting relation between the sequences $\{\gamma_n\}$ and the Legendre symbol $(n|q)$, where $|q|$ is the discriminant of $P(t)$.

Theorem: Let q be an odd prime and set $D = (-1|q)q$. Choose any integers λ, μ such that $\lambda^2 + 4\mu = D$, and define the sequence $\{\gamma_n\}$ by the recursion (1.1). Then there is a unique formal power series ϕ with integer coefficients and constant term zero such that

$$\sum_{n=1}^{\infty} \gamma_n \frac{\phi(t)^n}{n} = \sum_{n=1}^{\infty} \left(\frac{n}{q}\right) \frac{t^n}{n} \tag{2.1}$$

holds as an equality of formal power series.

Proof: Let ζ be any fixed primitive q^{th} root of unity. We define the quadratic Gauss sums $\tau(n)$ modulo q by

$$\tau(n) = \sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \zeta^{na}. \tag{2.2}$$

It is an elementary property of these sums ([1], Theorem 9.13) that $\tau(1)^2 = D$ and, therefore, $\tau(1)$ is a square root of D. Hereafter, we dispense with the ambiguity in sign and simply *define* $\sqrt{D}$ to be $\tau(1)$. Now, since $\sum_{a=0}^{q-1} \zeta^a = 0$, we have

$$\frac{1}{2}\sum_{a=1}^{q-1} \left(\left(\frac{a}{q}\right) - 1\right)\zeta^a = \frac{1+\sqrt{D}}{2}, \tag{2.3}$$

which shows that $(1+\sqrt{D})/2$ lies in the ring $\mathbb{Z}[\zeta]$ and, therefore, $\mathcal{O}_D = \mathbb{Z}[(1+\sqrt{D})/2] \subseteq \mathbb{Z}[\zeta]$. We also recall the separability property $\tau(n) = (n|q)\sqrt{D}$ for every integer n ([1], p. 192, eq. (17)).

Define the rational function f by

$$f(t) = \prod_{a=1}^{q-1} (1-\zeta^a t)^{-(a|q)}. \tag{2.4}$$

It is readily seen that as a formal power series in t, the coefficients of f lie in $\mathbb{Z}[\zeta]$. Set $P(t) = 1-\lambda t - \mu t^2 = (1-\alpha t)(1-\beta t)$, where the reciprocal roots α, β are chosen so that $\alpha - \beta = \sqrt{D}$. Then define the rational function ϕ by

$$\phi(t) = \frac{f(t)-1}{\alpha f(t) - \beta}. \tag{2.5}$$

We claim this function ϕ, as a formal power series in t, satisfies the conditions of the theorem.

We first show that ϕ satisfies the equality (2.1). We compute that as formal power series,

$$\begin{aligned} \log f(t) &= \log\left(\prod_{a=1}^{q-1}(1-\zeta^a t)^{-(a|q)}\right) = -\sum_{a=1}^{q-1}\left(\frac{a}{q}\right)\log(1-\zeta^a t) \\ &= \sum_{a=1}^{q-1}\left(\frac{a}{q}\right)\sum_{n=1}^{\infty}\zeta^{an}\frac{t^n}{n} = \sum_{n=1}^{\infty}\tau(n)\frac{t^n}{n} = \sqrt{D}\sum_{n=1}^{\infty}\left(\frac{n}{q}\right)\frac{t^n}{n}. \end{aligned} \tag{2.6}$$

On the other hand, solving (2.5) for f yields

$$f(t) = \frac{1-\beta\phi(t)}{1-\alpha\phi(t)}. \tag{2.7}$$

Since $f(0) = 1$, we have $\phi(0) = 0$; therefore, we may also compute that as formal power series,

$$\begin{aligned} \log f(t) &= \log\left(\frac{1-\beta\phi(t)}{1-\alpha\phi(t)}\right) = \log(1-\beta\phi(t)) - \log(1-\alpha\phi(t)) \\ &= \sum_{n=1}^{\infty}(\alpha^n - \beta^n)\frac{\phi(t)^n}{n} = \sqrt{D}\sum_{n=1}^{\infty}\gamma_n\frac{\phi(t)^n}{n}, \end{aligned} \tag{2.8}$$

using the well-known Binet formula

$$\gamma_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}. \tag{2.9}$$

(Note that expressions such as $\sum \gamma_n \phi^n / n$ make sense as formal power series in t, since the constant term of ϕ is zero.) Now, comparing the two expressions (2.6) and (2.8) shows that ϕ satisfies (2.1).

Turning now to the coefficients of ϕ, we write $\phi(t) = \sum_{n=1}^{\infty} a_n t^n$. Equating coefficients of t in (2.1) yields $a_1 = 1$; equating coefficients of t^n yields a recursion for a_n in terms of $a_1, \ldots, a_{n-1}$, demonstrating the uniqueness of ϕ. We first show that the coefficients of ϕ are rational: Suppose not, and let k be minimal such that $a_k \notin \mathbb{Q}$. For $1 \le j \le k$, let b_j denote the coefficient of t^k in $\phi(t)^j$; then $b_1 = a_k \notin \mathbb{Q}$, while $b_j \in \mathbb{Q}$ for $1 < j \le k$. Equating coefficients of t^k in (2.1) yields

$$b_1+\sum_{j=2}^{k}\gamma_j\frac{b_j}{j}=\left(\frac{k}{q}\right)\frac{1}{k}, \tag{2.10}$$

which is impossible, since $b_1\notin\mathbb{Q}$ while all other terms in (2.10) lie in $\mathbb{Q}$.

Now we show that the coefficients of ϕ are integers: Suppose not, and let k be minimal such that $a_k\notin\mathbb{Z}$. Again let b_j denote the coefficient of t^k in $\phi(t)^j$ for $1\le j\le k$; then $b_j\in\mathbb{Z}$ for $1<j\le k$, while $b_1=a_k=r/s$ for some coprime integers r, s with $|s|>1$. Expanding (2.7) formally yields

$$f(t)=(1-\beta\phi(t))\left(\sum_{n=0}^{\infty}\alpha^n\phi(t)^n\right)=1+\sqrt{D}\sum_{n=1}^{\infty}\alpha^{n-1}\phi(t)^n, \tag{2.11}$$

and therefore the coefficient of t^k in f is

$$\sqrt{D}(b_1+\alpha b_2+\cdots+\alpha^{k-1}b_k). \tag{2.12}$$

We know from (2.4) that this coefficient lies in $\mathbb{Z}[\zeta]$, and we observe that $\sqrt{D}(\alpha b_2+\cdots+\alpha^{k-1}b_k)$ lies in the subring $\mathbb{O}_D$, since $\alpha=(\lambda+\sqrt{D})/2$. So we must have $b_1\sqrt{D}\in\mathbb{Z}[\zeta]$, and therefore $(b_1\sqrt{D})^2=r^2D/s^2\in\mathbb{Z}[\zeta]$. This is a contradiction, since $r^2D/s^2\in\mathbb{Q}\setminus\mathbb{Z}$, whereas $\mathbb{Z}[\zeta]\cap\mathbb{Q}=\mathbb{Z}$. This proves the theorem, and in passing also shows via (2.12) that f has coefficients in $\mathbb{O}_D$.

3. THE LAW OF QUADRATIC RECIPROCITY

Theorem (Gauss): Let p and q be distinct odd primes, and set $D=(-1|q)q$. Then

$$\left(\frac{p}{q}\right)=\left(\frac{D}{p}\right). \tag{3.1}$$

Proof: Choose any integers λ,μ that satisfy $\lambda^2+4\mu=D$, and let $P(t)=1-\lambda t-\mu t^2=(1-\alpha t)(1-\beta t)$ and ϕ be as in the above theorem. For $1\le k\le p$, let b_k denote the coefficient of t^p in $\phi(t)^k$. Equating the coefficients of t^p in (2.1) yields

$$\frac{\gamma_p}{p}+\sum_{k=1}^{p-1}\gamma_k\frac{b_k}{k}=\frac{\left(\frac{p}{q}\right)}{p}, \tag{3.2}$$

so that

$$\left(\frac{p}{q}\right)-\gamma_p=p\sum_{k=1}^{p-1}\gamma_k\frac{b_k}{k}. \tag{3.3}$$

Therefore, the sum $\sum_{k=1}^{p-1}\gamma_k b_k/k$ lies in $(1/p)\mathbb{Z}$; but the least common denominator of the terms is relatively prime to p, since each γ_k and b_k lies in $\mathbb{Z}$. So this sum must be an integer; thus

$$\gamma_p\equiv\left(\frac{p}{q}\right)\pmod{p\mathbb{Z}}. \tag{3.4}$$

On the other hand, we may easily compute (cf. [5], Corollary 1(i) with $m=r=1$)

$$\gamma_p=\frac{\alpha^p-\beta^p}{\alpha-\beta}\equiv\frac{(\alpha-\beta)^p}{\alpha-\beta}=(\sqrt{D})^{p-1}=D^{(p-1)/2}\equiv\left(\frac{D}{p}\right)\pmod{p\mathbb{Z}}; \tag{3.5}$$

the first congruence holds modulo $p\mathcal{O}_D$, but both members are integers, so it holds modulo $p\mathbb{Z}$. Thus, $(p|q) \equiv (D|p) \pmod{p}$, but both are ±1, so they must be equal.

4. CONCLUDING REMARKS

The quadratic Gauss sums have played a role in many quadratic reciprocity proofs, reaching back to Gauss's sixth proof published in 1818 (cf. [3]). Although our approach has features in common with other proofs of the reciprocity law, it does exhibit an unusual flexibility by giving, for fixed p and q, an infinite family of proofs corresponding to the variety of choices for λ and μ.

In [5], we employed elementary p-adic methods to prove congruences relating the ratios $\gamma_{mp^r}/\gamma_{mp^{r-1}}$ to the Legendre symbol $(D|p)$. In the language of formal group laws, these congruences imply that the formal differential $\omega = P(t)^{-1}\,dt$ is the canonical invariant differential on a formal group law defined over $\mathbb{Z}$, which is isomorphic over $\mathbb{Z}$ to the formal group law attached to the Dirichlet L-series $L(s, \chi)$ for the Dirichlet character χ of conductor $|D|$ associated to the quadratic field $K = \mathbb{Q}(\sqrt{D})$. Formally differentiating both sides of (2.1) and using (1.2) gives

$$P(\phi)^{-1}d\phi = \sum_{n=1}^{\infty}\left(\frac{n}{q}\right)t^n\frac{dt}{t}, \tag{4.1}$$

which implies that the power series ϕ defined in §2 actually *is* the isomorphism between these two formal group laws; however, we have used no formal group techniques in the construction of ϕ. The above theorem says that the differential equation (4.1) has a rather surprising property, namely, that of possessing a solution $\phi(t)$ at $t = 0$, which is a rational function whose Maclaurin series has integer coefficients. It may be interesting to know the coefficients of ϕ more explicitly.

The use of formal group techniques to prove reciprocity laws originated with T. Honda [2], who gave a proof of quadratic reciprocity using formal group laws and Gauss sums. However, Honda used a formal group law defined over $\mathcal{O}_D$ rather than over $\mathbb{Z}$, and used the Galois theory of the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{D}) \subseteq \mathbb{Q}(\zeta)$ to prove $\mathcal{O}_D$-integrality, whereas the present argument requires no such techniques.

It does not appear that our method readily proves the auxiliary result $(2|q) = (-1)^{(q^2-1)/8}$, which amounts to a congruence for q modulo 8. But it is easy to determine from (2.1) that $a_2 = ((2|q) - \lambda)/2$, and one may also note that

$$\left(\frac{2}{q}\right) = 1 \Leftrightarrow q \equiv \pm 1 \pmod{8} \Leftrightarrow D \equiv 1 \pmod{8} \Leftrightarrow \mu \equiv 0 \pmod{2}. \tag{4.2}$$

REFERENCES

1. T. Apostol. *Introduction to Analytic Number Theory.* New York: Springer-Verlag, 1976.
2. T. Honda. "Invariant Differentials and L-Functions: Reciprocity Law for Quadratic Fields and Elliptic Curves over $\mathbb{Q}$." *Rend. Sem. Math. Univ. Padova* **49** (1973):323-35.
3. A. Weil. "La Cyclotomie Jadis et Naguère." *Enseign. Math.* **20** (1974):248-63.
4. H. Wilf. *Generatingfunctionology.* Boston-San Diego-New York: Academic Press, 1990.
5. P. T. Young. "p-Adic Congruences for Generalized Fibonacci Sequences." *The Fibonacci Quarterly* **32.1** (1994):2-10.

AMS Classification Numbers: 11A15, 11B39