Journal of Integer Sequences, Vol. 10 (2007),
Article 07.8.6

# Cipolla Pseudoprimes

Y. Hamahata[1] and Y. Kokubun
Department of Mathematics
Tokyo University of Science
Noda, Chiba, 278-8510
Japan
hamahata_yoshinori@ma.noda.tus.ac.jp

**Abstract**

We consider the pseudoprimes that M. Cipolla constructed. We call such pseudoprimes *Cipolla pseudoprimes*. In this paper we find infinitely many Lucas and Lehmer pseudoprimes that are analogous to Cipolla pseudoprimes.

## 1 Introduction

Take an integer $a > 1$. A *pseudoprime to base* $a$ is a composite number $n$ such that $a^{n-1} \equiv 1 \pmod{n}$. In 1904, M. Cipolla [1] found infinitely many pseudoprimes to a given base $a$. To be more precise,

**Theorem 1** (Cipolla [1], cf. Ribenboim [5]). *Let $p$ be a prime such that $p$ does not divide $a(a^2-1)$. Put*

$$n_1 = \frac{a^p - 1}{a - 1}, \quad n_2 = \frac{a^p + 1}{a + 1}, \quad n = n_1 n_2.$$

*Then $n$ is a pseudoprime to base $a$.*

In this paper we call such $n$ a *Cipolla pseudoprime*. In the above theorem, if we set $P = a + 1$, $Q = a$, then $n$ is written as $n = U_{2p}/P$, where $U_{2p}$ is a term in the Lucas sequence with parameters $P$ and $Q$. See the next section for Lucas sequences. From this observation, the following question arises. For given integers $P, Q$, are there infinitely many Lucas pseudoprimes with parameters $P$ and $Q$ of the form $U_{2p}/P$? Here Lucas pseudoprimes will be defined in the next section.

The purpose of the paper is to solve the above question affirmatively under a certain condition. As a corollary to our result, we derive the result of Lehmer [4]. We are also going to consider an analogous question for Lehmer sequences.

[1]Partially supported by Grant-in-Aid for Scientific Research (No. 18540050), Japan Society for the Promotion of Science.

## 2 Cipolla-Lucas pseudoprimes

In this section we consider Lucas pseudoprimes of special type.

Let $P, Q$ be integers such that $D := P^2 - 4Q \neq 0$, and $\alpha, \beta$ the roots of the polynomial $z^2 - Pz + Q$. For a nonnegative integer $n$, put

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad V_n = \alpha^n + \beta^n.$$

For example, we have $U_0 = 1$, $U_1 = 1$, $U_2 = P$, $V_0 = 2$, and $V_1 = P$. One sees that $(U_n)_{n\geq 0}$ and $(V_n)_{n\geq 0}$ are integer sequences. We call the sequences $(U_n)_{n\geq 0}$, $(V_n)_{n\geq 0}$ the *Lucas sequences with parameters P and Q*.

We exhibit some results needed afterwards. One can consult Ribenboim [5, 6] for the basic results.

(I) For a nonnegative integer $n$, $U_{2n} = U_n V_n$.

(II) (a) If $P$ is odd and $Q$ is even, then $U_n$, $V_n$ $(n \geq 1)$ are odd.

(b) If $P$ and $Q$ are odd, then $U_n$, $V_n$ $(3 \nmid n)$ are odd.

(III) (a) When $U_m \neq 1$, $U_m | U_n$ if and only if $m|n$.

(b) When $V_m \neq 1$, $V_m | V_n$ if and only if $m|n$ and $n/m$ is odd.

(IV) For any odd prime $p$,

$$2^{p-1} U_p = \sum_{k=0}^{(p-1)/2} \binom{p}{2k+1} P^{p-(2k+1))} D^k, \tag{1}$$

$$2^{p-1} V_p = \sum_{k=0}^{(p-1)/2} \binom{p}{2k} P^{(p-2k)} D^k. \tag{2}$$

$$U_p \equiv \left(\frac{D}{p}\right) \pmod{p}, \quad V_p \equiv P \pmod{p}.$$

We recall Lucas pseudoprimes. A composite number $n$ is a *Lucas pseudoprime with parameters P and Q* if

$$U_{n-\left(\frac{D}{n}\right)} \equiv 0 \pmod{n}$$

holds. Here $\left(\frac{D}{n}\right)$ is the Jacobi symbol.

Now let us define an analogue of Cipolla pseudoprimes for Lucas sequences.

**Definition 2.** A composite number $n$ is called a *Cipolla-Lucas pseudoprime with parameters* $P$ and $Q$ if it is a Lucas pseudoprime with parameters $P$ and $Q$ and has the form $U_{2p}/P$ for a certain prime number $p$.

Our first result is as follows.

**Theorem 3.** *Let $P$ be an odd number, and $Q$ a nonzero integer such that* $\gcd(P, Q) = 1$. *Assume that $D = P^2 - 4Q$ is square-free. Then there are infinitely many Cipolla-Lucas pseudoprimes with parameters $P$ and $Q$.*

*Proof.* Let $p$ be an odd prime such that $\gcd(p, 3PD) = 1$ and $\varphi(D)|p-1$. Then we show that $U_{2p}/P$ is a Lucas pseudoprime. From now on we prove the theorem step by step. Put $m = U_{2p}/P$.

First of all, we prove $m|U_{m-\left(\frac{D}{m}\right)}$. Since $p$ is odd, $U_p \equiv \left(\frac{D}{p}\right) \pmod p$, $V_p \equiv P \pmod p$. So that

$$U_{2p} = U_p V_p \equiv P\left(\frac{D}{p}\right) \pmod{p}.$$

Since $P = U_2$, $U_2|U_{2p}$, and $\gcd(p, P) = 1$, we have $m \equiv \left(\frac{D}{p}\right) \pmod p$. We recall that $P$ is odd and $\gcd(p, 3) = 1$. Hence $U_p$ and $V_p$ are odd. We see $2p|m - \left(\frac{D}{p}\right)$. From this, we have $U_{2p}|U_{m-\left(\frac{D}{p}\right)}$. Moreover we have $m|U_{m-\left(\frac{D}{p}\right)}$. We prove $\left(\frac{D}{p}\right) = \left(\frac{D}{m}\right)$. By (1) and (2),

$$\begin{aligned} 2^{p-1}U_p &\equiv pP^{p-1} \pmod{D}, \\ 2^{p-1}V_p &\equiv P^p \pmod{D}. \end{aligned}$$

By $\varphi(D)|p-1$, we have $U_p \equiv p \pmod D$, $V_p \equiv P \pmod D$. Hence $U_{2p} \equiv pP \pmod D$. By $\gcd(P, D) = 1$, it follows that $m = U_{2p}/P \equiv p \pmod D$. Observe that $D \equiv 1 \pmod 4$ because $P$ is odd. Thus we have $\left(\frac{D}{p}\right) = \left(\frac{D}{m}\right)$, which implies $m|U_{m-\left(\frac{D}{m}\right)}$.

We next show that $m$ is a composite number. Since $p$ is odd and $P = U_2 = V_1$, one has $P \nmid U_p$ and $P|V_p$. Now assume that there exists an odd prime $p$ satisfying $V_p = \pm P$. Then one has $V_1|V_p$ and $V_p|V_1$. This implies $p = 1$, which is absurd. Therefore $m$ is a composite number.

Finally, we prove the infinitude of $U_{2p}/P$. By Dirichlet's theorem on primes in arithmetic progression, there are infinitely many primes $p$ such that $\varphi(D)|p-1$. The number of primes $p$ with $\gcd(p, 3PD) > 1$ among them is finite. This proves the claim. □

As a corollary to the last theorem, we can derive a known result. We call the Lucas sequence with parameters 1 and $-1$ the *Fibonacci sequence*. We write $(F_n)_{n\geq 0}$ for it. A composite number $n$ is called a *Fibonacci pseudoprime* if

$$F_{n-\left(\frac{D}{n}\right)} \equiv 0 \pmod{n}$$

is valid. Using the last theorem, we have

**Corollary 4** (Lehmer [4])**.** *There are infinitely many primes $p$ such that $F_{2p}$ is a Fibonacci pseudoprime.*

*Proof.* Since $P = 1$ and $Q = -1$, $U_{2p}/P$ becomes $F_{2p}$. In this case one has $D = 5$. Hence for any prime $p > 5$ with $p \equiv 1 \pmod 4$, the two conditions $\gcd(p, 3PD) = 1$ and $\varphi(D)|p-1$ hold. This yields the result. □

## 3 Cipolla-Lehmer pseudoprimes

In this section we consider Lehmer pseudoprimes. First, we review Lehmer sequences.

Let $\alpha, \beta$ be distinct roots of the polynomial $f(z) = z^2 - \sqrt{L}z + M$, where $L > 0$ and $M$ are rational integers, and $K := L - 4M$ is the discriminant of $f(z)$. For a nonnegative integer $n$, put

$$D_n = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta) & \text{if } n \text{ is odd} \\ (\alpha^n - \beta^n)/(\alpha^2 - \beta^2) & \text{if } n \text{ is even,} \end{cases}$$

$$E_n = \begin{cases} (\alpha^n + \beta^n)/(\alpha + \beta) & \text{if } n \text{ is odd} \\ \alpha^n + \beta^n & \text{if } n \text{ is even.} \end{cases}$$

For example, we have $D_0 = 0$, $D_1 = D_2 = 1$, $E_0 = 2$, $E_1 = 1$, and $E_2 = L - 2M$. One sees that $(D_n)_{n\geq 0}$ and $(E_n)_{n\geq 0}$ are integer sequences. We call the sequences $(D_n)_{n\geq 0}$ and $(E_n)_{n\geq 0}$ the *the Lehmer sequences with parameters $L$ and $M$*. It should be noticed that we modify the original definition of the Lehmer sequences in order to make them integer sequences.

We exhibit some results needed afterwards. One can consult Lehmer [3] for the basic results.

(I) For a prime $p$, $D_{2p} = D_p E_p$.

(II) $D_n$ is even in the following cases only

(a) $L = 4k$, $M = 2l + 1$, $n = 2h$,

(b) $L = 4k + 2$, $M = 2l + 1$, $n = 4h$,

(c) $L = 4k \pm 1$, $M = 2l + 1$, $n = 3h$.

(III) $E_n$ is even in the following cases only

(a) $L = 4k$, $M = 2l + 1$,

(b) $L = 4k + 2$, $M = 2l + 1$, $n = 2h$,

(c) $L = 4k \pm 1$, $M = 2l + 1$, $n = 3h$.

(IV) If $m|n$, then $D_m|D_n$.

(V) For any odd prime $p$,

$$2^{p-1}D_p = \sum_{k=0}^{(p-1)/2} \binom{p}{2k+1} L^{(p-2k-1)/2}K^k, \tag{3}$$

$$2^{p-1}E_p = \sum_{k=0}^{(p-1)/2} \binom{p}{2k} L^{(p-2k)/2}K^k. \tag{4}$$

$$D_p \equiv \left(\frac{K}{p}\right) \pmod{p}, \quad E_p \equiv \left(\frac{L}{p}\right) \pmod{p}.$$

Next, we review Lehmer pseudoprimes. A composite number $n$ is called a *Lehmer pseudoprime with parameters $L$ and $M$* if

$$D_{n-\left(\frac{KL}{n}\right)} \equiv 0 \pmod{n}$$

holds. Here $\left(\frac{KL}{n}\right)$ denotes the Jacobi symbol.

Any Cipolla pseudoprime is written as $D_{2p}$ for some prime $p$. Hence we define Lehmer pseudoprimes related to Cipolla pseudoprimes as follows.

**Definition 5.** A composite number $n$ is called a *Cipolla-Lehmer pseudoprime with parameters $L$ and $M$* if it is a Lehmer pseudoprime with parameters $L$ and $M$ and has the form $D_{2p}$ for a certain prime $p$

Our second result is as follows.

**Theorem 6.** *Let $L$ be a square-free odd number and $M$ an integer such that* $\gcd(L, M) = 1$. *Assume that $K = L - 4M$ is square-free. Then there are infinitely many Cipolla-Lehmer pseudoprimes with parameters $L$ and $M$.*

*Proof.* The proof is similar to that of Theorem 3. Let $p$ be an odd prime such that $\gcd(p, KL) = 1$ and $\varphi(KL)|p-1$. Then we prove that $D_{2p}$ is a Lehmer pseudoprime. Put $m = D_{2p}$.

We first show $m|D_{m-\left(\frac{KL}{m}\right)}$. Since $p$ is odd, $D_p \equiv \left(\frac{K}{p}\right) \pmod p$, $E_p \equiv \left(\frac{L}{p}\right) \pmod p$. Hence

$$m = D_{2p} = D_p E_p \equiv \left(\frac{KL}{p}\right) \quad (\text{mod } p).$$

That is to say, $p|m - \left(\frac{KL}{p}\right)$. Since $L$ is odd, $D_p$ and $E_p$ are odd. Hence $m$ is odd. We find that $m-\left(\frac{KL}{p}\right)$ is even. Thus $2p|m-\left(\frac{KL}{p}\right)$. Using this, we have $D_{2p}|D_{m-\left(\frac{KL}{p}\right)}$, which shows $m|D_{m-\left(\frac{KL}{p}\right)}$. We must prove $\left(\frac{KL}{p}\right) = \left(\frac{KL}{m}\right)$. Since $K$ is odd, by (3) and (4),

$$\begin{aligned} 2^{p-1}D_p &\equiv pL^{\frac{p-1}{2}} + K^{\frac{p-1}{2}} \quad (\text{mod } KL), \\ 2^{p-1}E_p &\equiv L^{\frac{p-1}{2}} + pK^{\frac{p-1}{2}} \quad (\text{mod } KL). \end{aligned}$$

Since $\varphi(KL)|p-1$ and $2 \nmid KL$ hold, $2^{p-1} \equiv 1 \pmod{KL}$. Hence we have

$$m = D_p E_p \equiv p\left(K^{p-1} + L^{p-1}\right) \quad (\text{mod } KL).$$

It should be noted that $K^{p-1} + L^{p-1} \equiv 1 \pmod{KL}$. Indeed, because of $\gcd(K, L) = 1$, the condition $\varphi(K)\varphi(L)|p-1$ implies $L^{p-1} \equiv 1 \pmod K$ and $K^{p-1} \equiv 1 \pmod L$. For any prime divisor $l$ of $K$, $l|K^{p-1} + L^{p-1} - 1$. Hence we have $K^{p-1} + L^{p-1} - 1 \equiv 0 \pmod K$. In the same way, we have $K^{p-1} + L^{p-1} - 1 \equiv 0 \pmod L$. Therefore our claim is proven. Using this observation, we obtain $m \equiv p \pmod{KL}$. By the way, we see $KL = L^2 - 4ML \equiv L^2 \equiv 1 \pmod 4$. Thus we conclude that $\left(\frac{KL}{p}\right) = \left(\frac{KL}{m}\right)$. We get $m|D_{m-\left(\frac{KL}{m}\right)}$.

Clearly $m = D_p E_p$ is a composite number.

Finally we show the infinitude of $D_{2p}$. By Dirichlet's theorem on primes in arithmetic progression, there are infinitely many primes $p$ such that $\varphi(KL)|p-1$. The number of primes $p$ with $\gcd(p, KL) > 1$ among them is finite. This proves the claim. □

# References


[1] M. Cipolla, Sui numeri composti $P$, che verificanola congruenza di Fermat $a^{P-1} \equiv 1 \pmod P$. *Annali di Matematica* **9** (1904), 139–160.

[2] N. Koblitz, *A Course in Number Theory and Cryptography.* Springer-Verlag, 1994.

[3] D. H. Lehmer, An extended theory of Lucas' functions. *Annals of Math.* **31** (1930), 419–448.

[4] E. Lehmer, On the infinitude of Fibonacci pseudo-primes. *Fibonacci Quart.* **2** (1964), 229–230.

[5] P. Ribenboim, *The Book of Prime Number Records.* Springer-Verlag, 1989.

[6] P. Ribenboim, *My Numbers, My Friends – Popular Lectures on Number Theory.* Springer-Verlag, 2003.

[7] A. Rotkiewicz, Lucas pseudoprimes. *Functiones et Approximatio* **XXVIII** (2000), 97–104.

[8] A. Rotkiewicz, Arithmetic progressions formed by pseudoprimes. *Acta Mathematica et Informatica Universitatis Ostraviensis* **8** (2000) 61–74.

[9] J.-P. Serre, *Cours d'arithmétique.* Presses Universitaires de France, 1970.

---

2000 *Mathematics Subject Classification*: Primary 11A51; Secondary 11B39.

*Keywords:* pseudoprime, Lucas sequence, Lucas pseudoprime, Lehmer sequence, Lehmer pseudoprime.

---

Received July 17 2007; revised version received August 1 2007. Published in *Journal of Integer Sequences*, August 14 2007.

---

Return to Journal of Integer Sequences home page.