Journal of Integer Sequences, Vol. 28 (2025),
Article 25.2.2

Greatest Common Divisors and Lucas's Theorem

John Ferdinands
Department of Mathematics and Statistics
Calvin University
3201 Burton St. SE
Grand Rapids, MI 49546
USA
ferd@calvin.edu

Timothy Ferdinands
Department of Mathematics and Computer Science
Alfred University
One Saxon Dr.
Alfred, NY 14802
USA
ferdinands@alfred.edu

Abstract

We consider a sequence of greatest common divisors of the coefficients of a binomial expansion and use a classical result due to Lucas to show that the greatest common divisor is always 1. Our result generalizes a problem found in the Problem Section of *Mathematics Magazine*.

1 Introduction

The first author of this paper became interested in the following problem in the Problem Section of *Mathematics Magazine* from February 2022 [3].

Problem 1. *For a positive integer n, let a_n and b_n be the unique integers such that*

$$(5+\sqrt{3})^n = a_n + b_n\sqrt{3}.$$

Find $\gcd(a_n, b_n)$ *as a function of* n. *Solve the analogous problem when* $5+\sqrt{3}$ *is replaced by* $3+\sqrt{5}$.

In both cases the greatest common divisor is a power of 2. This led us to speculate about what would happen if the integers 5 and 3 were replaced by distinct positive integers u and v. The second author suggested the following more general question.

Problem 2. *Let p be an odd prime and let u and v be relatively prime positive integers where $v^{1/p}$ is irrational. Let $a_{n,0}, a_{n,1}, \ldots, a_{n,p-1}$ be the unique integers such that*

$$\left(u+v^{1/p}\right)^n = a_{n,0} + a_{n,1}v^{1/p} + a_{n,2}v^{2/p} + \cdots + a_{n,p-1}v^{(p-1)/p}.$$

Find $\gcd(a_{n,0}, a_{n,1}, \ldots, a_{n,p-1})$.

We were able to answer these questions, and the detailed results appear in [4]. The short answer is that the greatest common divisor is either 1 or a power of the prime p. The gcd function depends on the highest nonnegative power of p that divides $u^p+(-1)^p v$. The proof, which uses matrix algebra, is long and messy, since there are several cases that need to be considered. We will state the exact results later.

The obvious follow-up question is to ask what happens when the prime p is replaced by a composite positive integer N. If N is divisible by more than one prime, then the answer is simple. Before we state it, we will state a condition which ensures that the coefficients in the expansion of $(u+v^{1/N})^n$ are unique.

Lemma 3. *Let N be a positive integer that is divisible by at least two distinct primes, and let u and v be relatively prime positive integers. If the polynomial $x^N - v$ is irreducible over the rationals, then the coefficients in the expansion of $(u+v^{1/N})^n$ are unique.*

Proof. Let $(u+v^{1/N})^n = a_{n,0} + a_{n,1}v^{1/N} + a_{n,2}v^{2/N} + \cdots + a_{n,N-1}v^{(N-1)/N}$, using the binomial expansion. Suppose the coefficients $a_{n,0}, a_{n,1}, \ldots, a_{n,N-1}$ are not unique. Then there must be a positive integer $m < N$ such that $v^{m/N} = w$ where w is a positive integer. Let m be the smallest integer with this property. We claim that m divides N. Suppose that this is false; then $N = mq + r$ for some integers m and r with $0 < r < N$. Hence $(v^{1/N})^N = (v^{1/N})^{mq} v^{r/N}$, which implies that $v = w^q v^{r/n}$. But $v^{r/N}$ is irrational so we have a contradiction.

Now we show that $x^m - w$ divides $x^N - v$, so that $x^N - v$ is not irreducible over the rationals. The roots of $x^m - w$ are $w^{1/m}, \alpha w^{1/m}, \alpha^2 w^{1/m}, \ldots, \alpha^{m-1} w^{1/m}$, where α is a primitive m-th root of 1. Observe that for $0 \le i < m-1$ we know that $(\alpha^i w^{1/m})^N = w^{N/m}$, since m divides N, but $w^{1/m} = v^{1/N}$, so $w^{N/m} = v$. Hence every root of $x^m - w$ is also a root of $x^N - v$, which implies that $x^m - w$ divides $x^N - v$. □

Theorem. *Let N be a positive integer that is divisible by at least two distinct primes, and let u and v be relatively prime positive integers such that the polynomial $x^N - v$ is irreducible over the rationals. For any positive integer n, let $a_{n,0}, a_{n,1}, \ldots, a_{n,N-1}$ be the unique integers such that*

$$\left(u + v^{1/N}\right)^n = a_{n,0} + a_{n,1}v^{1/N} + a_{n,2}v^{2/N} + \cdots + \cdots a_{n,N-1}v^{(N-1)/N}.$$

Then $\gcd(a_{n,0}, a_{n,1}, \ldots, a_{n,N-1}) = 1$.

To illustrate this theorem, let $u = 3, v = 2$ and $N = 6$. Then

$$\left(3 + 2^{1/6}\right)^8 = 7065 + (17544)2^{1/6} + (20414)2^{2/6} + (13608)2^{3/6} + (5670)2^{4/6} + (1512)2^{5/6}$$

and

$$\gcd(7065, 17544, 20414, 13608, 5670, 1512) = 1.$$

This theorem is the main result of this paper. Compared to the proofs for the case where N is prime, the proof of this result is gratifyingly quick and easy.

2 Some lemmas

From now on the reader may assume unless told otherwise that N is a positive integer such that $N \geq 4$, and the polynomial $x^N - v$ is irreducible over the rationals. Additionally let $D_n = \gcd(a_{n,0}, a_{n,1}, \ldots, a_{n,N-1})$. We begin with two easy lemmas.

Lemma 4. *For all positive integers n, the value of D_n divides D_{n+1}.*

Proof. Observe that $\left(u + v^{1/N}\right)^{n+1} = \left(u + v^{1/N}\right)\left(u + v^{1/N}\right)^n$. It follows that

$$\begin{aligned} &a_{n+1,0} + a_{n+1,1}v^{1/N} + \cdots + a_{n+1,N-1}v^{(N-1)/N} \\ &= \left(u + v^{1/N}\right)\left(a_{n,0} + a_{n,1}v^{1/N} + \cdots + a_{n,N-1}v^{(N-1)/N}\right). \end{aligned}$$

By equating the coefficients of $v^{i/n}$ for $0 \leq i \leq N-1$ we see that

$$\begin{aligned} a_{n+1,0} &= ua_{n,0} + va_{n,N-1} \\ a_{n+1,1} &= a_{n,0} + ua_{n,1} \\ a_{n+1,2} &= a_{n,1} + ua_{n,2} \\ &\vdots \\ a_{n+1,N-1} &= a_{n,N-2} + ua_{n,N-1}. \end{aligned} \tag{1}$$

Since D_n divides each of the coefficients $a_{n,0}, a_{n,1}, \ldots, a_{n,N-1}$, it must also divide each of the coefficients $a_{n+1,0}, a_{n+1,1}, \ldots, a_{n+1,N-1}$, and hence it divides D_{n+1}.

□

Lemma 5. *If u and v are relatively prime positive integers, then*

$$\gcd(u^N + (-1)^{N+1}v, u) = \gcd(u^N + (-1)^{N+1}v, v) = 1.$$

Proof. This follows from the fact that u and v are relatively prime. □

Our next lemma shows why the expression $u^N + (-1)^{N+1}v$ is important.

Lemma 6. *For every positive integer n it is the case that either $\gcd(u^N+(-1)^{N+1}v, D_n) = 1$, or the $\gcd(u^N + (-1)^{N+1}v, D_n)$ is a product of powers of primes that divides N.*

Proof. We proceed by induction on n. For $1 \leq n \leq N-1$ it follows from the binomial formula that the coefficient $a_{n,n}$ of $v^{n/N}$ is 1, and hence $D_n = 1$ for $1 \leq n \leq N-1$.

Suppose that the result is true for some $n \geq N-1$ and false for $n+1$. Then the $\gcd(u^N + (-1)^{N+1}v, D_n)$ is either 1 or a product of primes that divide N, and thus the $\gcd(u^N + (-1)^{N+1}v, D_{n+1})$ is divisible by a prime p that does not divide N. Hence p divides both $u^N + (-1)^{N+1}v$ and D_{n+1}, but does not divide either N or D_n.

By (1) we know that

$$\begin{aligned} a_{n+1,0} &= ua_{n,0} + va_{n,N-1} \\ a_{n+1,1} &= a_{n,0} + ua_{n,1} \\ a_{n+1,2} &= a_{n,1} + ua_{n,2} \\ &\vdots \\ a_{n+1,N-1} &= a_{n,N-2} + ua_{n,N-1}. \end{aligned}$$

Since p divides D_{n+1}, it divides each of $a_{n+1,0}, a_{n+1,1}, \ldots, a_{n+1,N-1}$. Hence

$$a_{n,N-2} \equiv -ua_{n,N-1} \pmod{p}.$$

Also

$$a_{n,N-3} \equiv -ua_{n,N-2} \equiv u^2 a_{n,N-1} \pmod{p}.$$

Proceeding thus, we can show that

$$a_{n,i} \equiv (-1)^{N-i-1}u^{N-i-1}a_{n,N-1} \pmod{p}. \tag{2}$$

By (1) again we see that

$$\begin{aligned} a_{n,0} &= ua_{n-1,0} + va_{n-1,N-1} \\ a_{n,1} &= a_{n-1,0} + ua_{n-1,1} \\ a_{n,2} &= a_{n-1,1} + ua_{n-1,2} \\ &\vdots \\ a_{n,N-1} &= a_{n-1,N-2} + ua_{n-1,N-1}. \end{aligned} \tag{3}$$

This implies that

$$\sum_{i=0}^{N-1}(-1)^i u^i a_{n,i} = ua_{n-1,0} + va_{n-1,N-1} - u(a_{n-1,0} + ua_{n-1,1}) \\ + u^2(a_{n-1,1} + ua_{n-1,2}) - \cdots + (-1)^{N-1}u^{N-1}(a_{n-1,N-2} + ua_{n-1,N-1}).$$

The right-hand side reduces to

$$(v + (-1)^{N-1}u^N)a_{n-1,N-1} = (-1)^{N-1}(u^N + (-1)^{N+1}v)a_{n-1,N-1}.$$

But $u^N + (-1)^{N+1}v$ is divisible by p. Hence p divides $\sum_{i=0}^{N-1}(-1)^i u^i a_{n,i}$.

By (2), $a_{n,i} \equiv (-1)^{N-i-1}u^{N-i-1}a_{n,N-1} \pmod{p}$. Therefore

$$\begin{aligned}\sum_{i=0}^{N-1}(-1)^i u^i a_{n,i} &\equiv \sum_{i=0}^{N-1}(-1)^i u^i (-1)^{N-i-1}u^{N-i-1}a_{n,N-1} \pmod{p} \\ &\equiv \sum_{i=0}^{N-1}(-1)^{N-1}u^{N-1}a_{n,N-1} \pmod{p} \\ &\equiv (-1)^{N-1}Nu^{N-1}a_{n,N-1} \pmod{p}.\end{aligned}$$

Since p divides $\sum_{i=0}^{N-1}(-1)^i u^i a_{n,i}$, it follows that p divides $(-1)^{N-1}Nu^{N-1}a_{n,N-1}$. By hypothesis p does not divide N. Since p divides $u^N + (-1)^{N+1}v$, Lemma 5 implies that p does not divide u. Therefore p divides $a_{n,N-1}$. But then it follows from (2) that p divides $a_{n,i}$ for all $0 \le i \le N-1$, and hence p divides D_n, which contradicts our hypothesis.

□

Lemma 7. *Let p be a prime that divides D_n for some n. Then p divides $u^N + (-1)^{N+1}v$.*

Proof. We saw in the proof of Lemma 6 that $D_i = 1$ for $1 \le i \le N-1$. Let n be the smallest positive integer such that p divides D_n. Then p does not divide D_{n-1}. (Note that $n \ge N \ge 4$, so $n-1$ must be a positive integer.)

Equation (1) can be written in matrix form as

$$\begin{pmatrix} a_{n,0} \\ a_{n,1} \\ \vdots \\ a_{n,N-1} \end{pmatrix} = T \begin{pmatrix} a_{n-1,0} \\ a_{n-1,1} \\ \vdots \\ a_{n-1,N-1} \end{pmatrix}$$

where

$$T = \begin{pmatrix} u & 0 & 0 & \cdots & 0 & 0 & v \\ 1 & u & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & u & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 & u \end{pmatrix}$$

is an $N \times N$ matrix.

Note that $\det(T) = u^N + (-1)^{N+1}v$, which is nonzero since $v^{1/N}$ is irrational. This means that T is invertible. It follows that

$$\begin{pmatrix} a_{n-1,0} \\ a_{n-1,1} \\ \vdots \\ a_{n-1,N-1} \end{pmatrix} = T^{-1} \begin{pmatrix} a_{n,0} \\ a_{n,1} \\ \vdots \\ a_{n,N-1} \end{pmatrix} = \frac{1}{u^N + (-1)^{N+1}v} B \begin{pmatrix} a_{n,0} \\ a_{n,1} \\ \vdots \\ a_{n,N-1} \end{pmatrix},$$

where B is a matrix with integer entries. (See, for instance [5, p. 219]). Therefore

$$(u^N + (-1)^{N+1}v) \begin{pmatrix} a_{n-1,0} \\ a_{n-1,1} \\ \vdots \\ a_{n-1,N-1} \end{pmatrix} = B \begin{pmatrix} a_{n,0} \\ a_{n,1} \\ \vdots \\ a_{n,N-1} \end{pmatrix}.$$

Since p divides $a_{n,i}$ for $0 \leq i \leq N-1$, we have that p divides $(u^N + (-1)^{N+1}v)a_{n-1,i}$ for $0 \leq i \leq N-1$.

If p does not divide $u^N + (-1)^{N+1}v$, then p divides $a_{n-1,i}$ for $0 \leq i \leq N-1$, and hence p divides D_{n-1}. This contradicts the hypothesis. Therefore p divides $u^N + (-1)^{N+1}v$. □

Lemma 8. *For all positive integers n, either $D_n = 1$ or D_n is a product of powers of primes that divide N.*

Proof. Suppose there is a positive integer n and a prime p such that p divides D_n. Then p divides $u^N + (-1)^{N+1}v$ by Lemma 7. Therefore p divides $\gcd(u^N + (-1)^{N+1}v, D_n)$. Then Lemma 6 implies that p divides N, and the result follows. □

These lemmas imply the following corollary.

Corollary 9. *If $u^N + (-1)^{N+1}v$ and N are relatively prime, then $D_n = 1$ for all positive integers n.*

We leave the proof of this corollary to the reader.

3 Lucas's theorem

To complete the proof of our main result we need a classical result due to the 19th century mathematician Édouard Lucas [1], together with four corollaries.

Lucas (1842–1891) was a French mathematician who is best known for his work in number theory [6]. He studied the Fibonacci sequence and the associated Lucas sequence is named after him. Additionally he proved that the Mersenne number $2^{127}-1$ is prime. This is, and surely will always be, the largest prime number found by hand calculations [2].

Theorem 10 (Lucas's theorem)**.** *Let p be a prime, and let n and k have notation in base p of $n=\sum_{i\geq 0} a_i p^i$ and $k=\sum_{i\geq 0} b_i p^i$ respectively. Then*

$$\binom{n}{k} \equiv \prod_{i\geq 0} \binom{a_i}{b_i} \pmod{p}.$$

(Note that this uses the convention that if $a<b$, then $\binom{a}{b}=0$.)

For the purposes of this paper we only need the following weaker version of Lucas's theorem, which was proved in [1], and from which the more general result follows by induction.

Theorem 11 (Lucas's theorem, weaker version)**.** *Let p be a prime and let a and b be nonnegative integers. Let $c,d\in\{0,1,2,\ldots,p-1\}$. Then*

$$\binom{ap+c}{bp+d} \equiv \binom{a}{b}\binom{c}{d} \pmod{p}.$$

For convenience we will denote the weaker version of Lucas's theorem by LTWV. From LTWV we see the following corollaries.

Corollary 12. *Let p be prime and let a and b be nonnegative integers. If p divides a and p does not divide b, then p divides $\binom{a}{b}$.*

Proof. Suppose p divides a and p does not divide b. This means that $a=lp$ and $b=mp+r$ for some integers l and r where $r\in\{1,2,\ldots,p-1\}$. By the LTWV

$$\binom{a}{b} = \binom{lp+0}{mp+r} \equiv \binom{l}{m}\binom{0}{r} \equiv 0 \pmod{p}.$$

Note that since $0<r$, $\binom{0}{r}=0$. Thus we see that p divides $\binom{a}{b}$. □

Corollary 13. *Let p be prime, and let a and b be nonnegative integers. Then*

$$\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p}.$$

Proof. The result follows immediately when we apply LTWV with $c = 0$ and $d = 0$. □

Corollary 14. *Let p be prime and let a and b be nonnegative integers. If $r > s$ and p does not divide either a or b, then p divides $\binom{p^r a}{p^s b}$.*

Proof. By Corollary 13, we see that

$$\binom{p^r a}{p^s b} \equiv \binom{p^{r-1} a}{p^{s-1} b} \equiv \binom{p^{r-2} a}{p^{s-2} b} \equiv \cdots \equiv \binom{p^{r-s} a}{b} \pmod{p}.$$

From Corollary 12 we see that p divides $\binom{p^{r-s} a}{b}$. Therefore we get that p divides $\binom{p^r a}{p^s b}$. □

Corollary 15. *Suppose p is prime and a and b are nonnegative integers. If r is a positive integer and p does not divide either a or b, then*

$$\binom{p^r a}{p^r b} \equiv \binom{a}{b} \pmod{p}.$$

Proof. This result follows from repeatedly applying the result of Corollary 13, in the same manner as we did for the proof of Corollary 14. □

4 Proof of the main theorem

We are now ready to prove the main result of this paper.

Theorem 16. *Let N be a positive integer that is divisible by at least two distinct primes and let u and v be relatively prime positive integers such that the polynomial $x^N - v$ is irreducible over the rationals. For any positive integer n, let $a_{n,0}, a_{n,1}, \ldots, a_{n,N-1}$ be the unique integers such that*

$$\left(u + v^{1/N}\right)^n = a_{n,0} + a_{n,1} v^{1/N} + a_{n,2} v^{2/n} + \cdots + a_{n,N-1} v^{(N-1)/N}.$$

Then $\gcd(a_{n,0}, a_{n,1}, \ldots, a_{n,N-1}) = 1$.

Proof. We begin with a brief sketch of the argument. We suppose there is some n such that $D_n \neq 1$. Then there is a prime p that divides D_n. We will then show that there exists an integer m where $m > n$ such that p does not divide D_m. But from Lemma 4 we know that D_n must divide D_m, which will give us a contradiction.

Accordingly, suppose $D_n \neq 1$ for some n, and let p be a prime that divides D_n. Since p divides D_n, we see from Lemma 8 that p divides N. This means that $N = p^a s$ for some positive integer a and and integer $s > 1$ that is not divisible by p. (Recall that N is divisible

by at least two distinct primes.) Thus we can choose a positive integer r such that we have both $Np^r > n$ and $p^{a+r} > N$.

Note that $p^{a+r} = kN + t$ for some positive integers k and t, where $1 \leq t \leq N-1$. Since $t \leq N-1$ we know that $t+N \leq 2N-1 < 2N < Np^r$. Thus we can repeatedly add positive integer multiples of N to t until the sum first exceeds Np^r. In other words, there exists a positive integer l such that $t + lN < Np^r < t + (l+1)N$. (Note that if $t + lN = Np^r$ it is the case that N divides t, which is impossible since $t < N$.) It follows that in the expansion of $\left(u + v^{1/N}\right)^{Np^r}$, the coefficient of $v^{t/N}$ is

$$a_{Np^r,t} = \sum_{i=0}^{l} \binom{Np^r}{t+iN} u^{Np^r - t - iN} v^i.$$

Now we will show that $a_{Np^r,t}$ is not divisible by p. Since p divides D_n, we see from Lemma 7 that p divides $u^N + (-1)^{N+1} v$. Thus Lemma 5 tells us that p does not divide either u or v.

When $i = k$ we see from Corollary 15 that

$$\binom{Np^r}{t+kN} \equiv \binom{p^{a+r}s}{p^{a+r}} \equiv \binom{s}{1} \pmod{p}.$$

Since p does not divide s, we see that p does not divide $\binom{Np^r}{t+kN}$. We will show that when i is unequal to k, $\binom{Np^r}{t+iN}$ is divisible by p. Thus it follows that p does not divide

$$a_{Np^r,t} = \sum_{i=0}^{l} \binom{Np^r}{t+iN} u^{Np^r - t - iN} v^i.$$

Suppose $0 \leq i \leq k-1$. Then $t + iN < t + kN = p^{a+r}$. Hence the highest power of p that divides $t + iN$ is smaller than $a + r$. By Corollary 14 we know that $\binom{Np^r}{t+iN} = \binom{p^{a+r}s}{t+iN}$ is divisible by p.

Finally suppose that $k+1 \leq i \leq l$. Then $t + iN \leq t + lN < Np^r$. But we see that

$$t + iN = p^{a+r} - kN + iN = p^{a+r} + (i-k)N.$$

Hence $(i-k)N < Np^r$, so $i - k < p^r$.

Therefore the highest power of p that divides $(i-k)N = (i-k)p^a s$ is smaller than $a+r$. It follows that the same must be true for $t + iN = p^{a+r} + (i-k)N$. Again by Corollary 14 we see that $\binom{Np^r}{t+iN} = \binom{p^{a+r}s}{t+iN}$ is divisible by p. This completes the proof that $a_{Np^r,t}$ is not divisible by p. Hence D_{Np^r} is not divisible by p, which gives us our contradiction.

□

5 When N is prime

These results depend on whether N is equal to 2 or an odd prime. The proofs of the following theorems are found in [4].

Theorem 17. *For any positive integer n, let $(u+\sqrt{v})^n = a_n + b_n\sqrt{v}$ where u and v are relatively prime positive integers, $\sqrt{v}$ is irrational, and a_n and b_n are integers. Let $D_n = \gcd(a_n, b_n)$.*

(a) If $u^2 - v$ is odd, then $D_n = 1$ for all $n \geq 1$.

(b) If $u^2 - v \equiv 2 \pmod 4$, then $D_{2n-1} = 2^{n-1}$ and $D_{2n} = 2^n$ for all $n \geq 1$.

(c) If $u^2 - v \equiv 4 \pmod 8$, then $D_{3n-2} = 2^{3n-3}$, $D_{3n-1} = 2^{3n-2}$ and $D_{3n} = 2^{3n}$ for all $n \geq 1$.

(d) If $u^2 - v \equiv 0 \pmod 8$, then $D_n = 2^{n-1}$ for all $n \geq 1$.

Theorem 18. *For any positive integer n, let*

$$\left(u + v^{1/p}\right)^n = a_{n,0} + a_{n,1}v^{1/p} + a_2 v^{2/p} + \cdots + a_{n,p-1}v^{(p-1)/p}$$

for some integers $a_{n,0}, a_{n,1}, \ldots, a_{n,p-1}$, where p is an odd prime, u and v are relatively prime positive integers and $v^{1/p}$ is irrational. Let $D_n = \gcd(a_{n,0}, a_{n,1}, a_{n,2}, \ldots, a_{n,p-1})$.

(a) If $u^p + v$ is not divisible by p, then $D_n = 1$ for all $n \geq 1$.

(b) If $u^p + v = mp$ where p does not divide m, then $D_{np+i} = p^n$ for all $n \geq 0$ and $0 \leq i \leq p-1$.

(c) If $u^p + v$ is divisible by p^2, then $D_{n(p-1)+i} = p^n$ when $n \geq 0$ and $1 \leq i \leq p-1$.

6 When N is a power of a prime

This is the one remaining case. This remains an open problem. While we do not have definite answers at this time, we strongly suspect that this case is quite similar to the results of Theorem 17 and Theorem 18. This is a problem for further investigation.

References

[1] P. Anderson, A. Benjamin, and J. Rouse, Combinatorial proofs of Fermat's, Lucas's, and Wilson's theorems, *Amer. Math. Monthly* **112** (2005), 266–268.

[2] C. Caldwell, The largest known prime by year: A brief history, 2024, https://t5k.org/notes/by_year.html.

[3] Columbus State University Problem Solving Group, Proposal 2137. Problems and solutions. *Math. Mag.* **95** (2022), 73–82.

[4] J. Ferdinands and T. Ferdinands, A sequence of greatest common divisors, *Alabama J. Math.* **46** (2023), 12–25.

[5] S. Friedberg, A. Insel, and L. Spence, *Linear Algebra*, 3rd edition, Prentice-Hall, 1997.

[6] J. J. O'Connor and E. F. Robertson, François Édouard Anatole Lucas, 1996. Available at https://mathshistory.st-andrews.ac.uk/Biographies/Lucas/.

2020 *Mathematics Subject Classification*: Primary 11B50; Secondary 11B65.
Keywords: Greatest common divisor, Lucas's theorem.

(Concerned with sequence A007318.)

Received June 11 2024; revised versions received June 20 2024; June 21 2024; January 15 2025; March 4 2025. Published in *Journal of Integer Sequences*, March 10 2025.

Return to Journal of Integer Sequences home page.