Alabama Journal of Mathematics

Alabama Journal of Mathematics
Volume 46 (1) (2023), 12 – 25

Original Article

A Sequence of Greatest Common Divisors

John Ferdinands[1], Timothy Ferdinands[2]

[1] *Department of Mathematics and Statistics*
Calvin University
Grand Rapids, MI
USA

2*Department of Mathematics and Computer Science*
Alfred University
Alfred, NY
USA

Abstract

Let u, v and p be positive integers such that u and v are relatively prime, p is prime, and $v^{1/p}$ is an irrational number. Then for each positive integer n, the greatest common divisor of the integer coefficients in the expansion of $\left(u + v^{1/p}\right)^n$ is the n-th term of a sequence of positive integers. We show that the greatest common divisor is a nonnegative power of p as well as finding this greatest common divisor as an explicit function of n.

Mathematics Subject Classification (2020). 11B50, 11B65

Keywords. Sequence, greatest common divisor, nullspace of a matrix

1. Introduction

The Problems Section of Mathematics Magazine for February 2022 [2] contained the following proposal:

Proposal 1.1. *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 $3+\sqrt{5}$.*

It turns out that in both cases the greatest common divisor is either 1 or a power of 2. It is natural to try to generalize these results. If u and v are positive integers and v is not a square, then $(u+\sqrt{v})^n = a_n + b_n\sqrt{v}$ for some integers a_n and b_n. If u and v had a common factor, it could be factored out of the parentheses; hence if we are interested in finding $\gcd(a_n, b_n)$ we may assume that u and v are relatively prime. We could also consider the analogous problem for $(u + v^{1/p})^n$ where p is an odd prime.

Email address: john.ferdinands@calvin.edu
Email address: ferdinands@alfred.edu

Here are the problems, stated precisely:

Problem 1.2. *(1) Let u and v be relatively prime positive integers with v not a square number. For each positive integer n, let*

$$(u+\sqrt{v})^n = a_n + b_n\sqrt{v}$$

for some integers a_n and b_n.

Find $\gcd(a_n, b_n)$ as a function of n.

(2) Let p be an odd prime, and let u and v be relatively prime positive integers with $v^{1/p}$ not an integer. For each positive integer n, let

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

for some integers $a_{n,0}, a_{n,1}, \ldots, a_{n,p-1}$.

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

In Section 2 of this paper we show that $\gcd(a_n, b_n)$ is either 1 or a power of 2, and that $\gcd(a_{n,0}, a_{n,1}, \ldots, a_{n,p-1})$ is either 1 or a power of p. In Section 3 we will find $\gcd(a_n, b_n)$ as an explicit function of n. Finally in Section 4 we give the explicit function for $\gcd(a_{n,0}, a_{n,1}, \ldots, a_{n,p-1})$. We only use elementary methods: divisibility of integers congruence modulo a prime, and a little matrix algebra.

2. The GCD is either 1 or a Prime Power

Using the notation of Section 1 we have that

$$\begin{aligned} a_{n+1} + b_{n+1}\sqrt{v} &= (u+\sqrt{v})^{n+1} = (u+\sqrt{v})(u+\sqrt{v})^n \\ &= (u+\sqrt{v})(a_n + b_n\sqrt{v}) = ua_n + vb_n + (a_n + ub_n)\sqrt{v} \end{aligned}$$

which gives the following recurrence relations:

$$\begin{aligned} a_{n+1} &= ua_n + vb_n \\ b_{n+1} &= a_n + ub_n \end{aligned} \tag{2.1}$$

We begin with three lemmas. The first two are straightforward and the third is the key to the proof of the main result.

Lemma 2.1. *Let $D_n = \gcd(a_n, b_n)$. Then D_n divides D_{n+1} for all n.*

Proof. Since D_n divides a_n and b_n it follows from (2.1) that D_n divides a_{n+1} and b_{n+1}, and hence divides D_{n+1}. □

Lemma 2.2. $\gcd(u^2 - v, u) = \gcd(u^2 - v, v) = 1$.

Proof. Suppose there is a prime p that divides $u^2 - v$ and u. Then p divides $u^2 - (u^2 - v) = v$. But this contradicts the hypothesis that u and v are relatively prime. If there is a prime p that divides $u^2 - v$ and v, then p must divide $u^2 - v + v = u^2$, and hence p divides u, which again is a contradiction. □

Lemma 2.3. *For all n, $\gcd(u^2 - v, D_n) = 1$ or a power of 2.*

Proof. First note that $D_1 = \gcd(u, 1) = 1$, so the statement is true for $n = 1$. Since $(u+\sqrt{v})^2 = u^2 + v + 2u\sqrt{v}$, $D_2 = \gcd(u^2 + v, 2u)$. Suppose there is a prime $p \neq 2$ that divides $u^2 + v$ and $2u$. Then p divides u and $u^2 + v$, which means that p must divide $u^2 + v - u^2 = v$. This contradicts the hypothesis that u and v are relatively prime. Thus 2 is the only prime that can divide D_2, so the result is true for $n = 2$.

Assume that the result is true for $1 \leq i \leq n$ for some $n \geq 2$, but false for $i = n + 1$. Then there is a prime $p \neq 2$ such that p divides $u^2 - v$ and D_{n+1}, but p does not divide D_n.

Writing (2.1) in matrix form gives $\begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix} = \begin{pmatrix} u & v \\ 1 & u \end{pmatrix} \begin{pmatrix} a_n \\ b_n \end{pmatrix}$. Since v is not a perfect square, $u^2 - v \neq 0$. It follows that:

$$\begin{pmatrix} a_n \\ b_n \end{pmatrix} = \begin{pmatrix} u & v \\ 1 & u \end{pmatrix}^{-1} \begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix} = \frac{1}{u^2 - v} \begin{pmatrix} u & -v \\ -1 & u \end{pmatrix} \begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix}$$

which gives

$$(u^2 - v)a_n = ua_{n+1} - vb_{n+1}$$
$$(u^2 - v)b_n = -a_{n+1} + ub_{n+1}.$$

Since $n \geq 2$, this implies that $(u^2-v)b_{n-1} = -a_n+ub_n$. Since p divides (u^2-v), p divides $(-a_n + ub_n)$. Furthermore, since p divides D_{n+1}, p divides b_{n+1}. Since $b_{n+1} = a_n + ub_n$, p divides $(a_n + ub_n)$. Therefore p divides both $(a_n + ub_n) - (-a_n + ub_n) = 2a_n$ and $(a_n + ub_n) + (-a_n + ub_n) = 2ub_n$. Since $\gcd(u^2 - v, u) = 1$, p does not divide u, and also $p \neq 2$. Therefore p divides both a_n and b_n, and hence p divides D_n as well, which contradicts the hypothesis that $D_n = 1$ or a power of 2.

□

Now we are ready to prove the first of the two main results of this section.

Theorem 2.1. *Let $(u+\sqrt{v})^n = a_n + b_n\sqrt{v}$ where u, v, a_n and b_n are positive integers with u and v relatively prime. Then $\gcd(a_n, b_n) = 1$ or a power of 2.*

Proof. We saw in the proof of Lemma 2.3 that the statement is true for $n = 1$ and $n = 2$. Suppose it is true for some $n \geq 2$. In the proof of Lemma 2.3 we showed that:

$$(u^2 - v)a_n = ua_{n+1} - vb_{n+1}$$
$$(u^2 - v)b_n = -a_{n+1} + ub_{n+1}.$$

Suppose that the result is false for $n + 1$. Then there is a prime $p \neq 2$ that divides $D_{n+1} = \gcd(a_{n+1}, b_{n+1})$. Hence p divides both a_{n+1} and b_{n+1}, and thus p divides $(u^2-v)a_n$ and $(u^2 - v)b_n$. But by Lemma 2.3, p does not divide $u^2 - v$. Therefore p divides a_n and b_n and therefore p divides D_n, contrary to our hypothesis that the statement is true for n. The statement of the theorem follows. □

Now we turn to the case of $\left(u + v^{1/p}\right)^n$ where p is an odd prime, u and v are relatively prime positive integers with $v^{1/p}$ not an integer. Recall that

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

for some integers $a_{n,0}, a_{n,1}, \ldots, a_{n,p-1}$. Then

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

By equating the coefficients of $v^0, v^{1/p}, v^{2/p}, \ldots, v^{(p-1)/p}$ we see that

$$\begin{aligned} a_{n+1,0} &= ua_{n,0} + va_{n,p-1} \\ a_{n+1,1} &= a_{n,0} + ua_{n,1} \\ a_{n+1,2} &= a_{n,1} + ua_{n,2} \\ &\vdots \\ a_{n+1,p-1} &= ua_{n,p-2} + a_{n,p-1} \end{aligned} \tag{2.2}$$

Next we state three lemmas which are analogous to Lemmas 2.1, 2.2 and 2.3. We omit the proofs of the first two, since they are similar to the proofs of Lemmas 2.1 and 2.2.

Lemma 2.4. *Let $D_n = \gcd(a_{n,0}, a_{n,1}, \ldots, a_{n,p-1})$. Then D_n divides D_{n+1} for all n.*

Lemma 2.5. $\gcd(u^p + v, u) = \gcd(u^p + v, v) = 1$

Lemma 2.6. *For all positive integers* n, $\gcd(u^p + v, D_n) = 1$ *or a power of* p.

Proof. From the binomial expansion of $(u + v^{1/p})^n$, we can show that $D_n = 1$ for $1 \leq n \leq p-1$. The binomial expansion together with Lemma 2.5 give us that either $D_p = p$ or $D_p = 1$. Hence the statement is true for $1 \leq n \leq p$.

Assume that the statement is true for some $n \geq p$, but false for $n+1$. Then there is a prime $q \neq p$ such that q divides $u^p + v$ and D_{n+1}, but q does not divide D_n.

Since q divides D_{n+1}, q divides $a_{n+1,i}$ for $0 \leq i \leq p-1$. It follows from (2.2) that $a_{n,p-2} + ua_{n,p-1} \equiv 0 \pmod{q}$, and hence $a_{n,p-2} \equiv -ua_{n,p-1} \pmod{q}$. Similarly we see that $a_{n,p-3} \equiv -ua_{n,p-2} \equiv u^2 a_{n,p-1} \pmod{q}$. By repeatedly applying (2.2) we see that

$$a_{n,r} \equiv (-1)^r u^{p-r-1} a_{n,p-1} \pmod{q} \tag{2.3}$$

for $0 \leq r \leq p-1$.

Since $n \geq p > 1$, equation (2.2) implies that

$$\begin{aligned} a_{n,0} &= ua_{n-1,0} + va_{n-1,p-1} \\ a_{n,1} &= a_{n-1,0} + ua_{n-1,1} \\ a_{n,2} &= a_{n-1,1} + ua_{n-1,2} \\ &\vdots \\ a_{n,p-1} &= a_{n-1,p-2} + ua_{n-1,p-1} \end{aligned} \tag{2.4}$$

Hence

$$\begin{aligned} \sum_{r=0}^{p-1} (-1)^r u^r a_{n,r} =& (au_{n-1,0} + va_{n-1,p-1}) - u(a_{n-1,0} + ua_{n-1,1}) + \\ & u^2(a_{n-1,1} + ua_{n-1,2}) - \cdots + u^{p-1}(a_{n-1,p-2} + ua_{n-1,p-1}) \\ =& (u^p + v)a_{n-1,p-1}. \end{aligned} \tag{2.5}$$

Since q divides $(u^p + v)$, we know that q divides $\sum_{r=0}^{p-1} (-1)^r u^r a_{n,r}$, and hence $\sum_{r=0}^{p-1} (-1)^r u^r a_{n,r} \equiv 0 \pmod{q}$. By (2.3), we see that $a_{n,r} \equiv (-1)^r u^{p-r-1} a_{n,p-1} \pmod{q}$ for $0 \leq r \leq p-1$, so

$$\sum_{r=0}^{p-1} (-1)^r u^r (-1)^r u^{p-r-1} a_{n,p-1} \equiv \sum_{r=0}^{p-1} u^{p-1} a_{n,p-1} \pmod{q}.$$

This implies that $pu^{p-1} a_{n,p-1} \equiv 0 \pmod{q}$, and that q divides $pu^{p-1} a_{n-1,p}$. Since q divides $u^p + v$, Lemma 2.5 implies that q does not divide u^p. Also $q \neq p$. Hence q divides $a_{n,p-1}$, so $a_{n,p-1} \equiv 0 \pmod{q}$. It follows from (2.3) that $a_{n,r} \equiv 0 \pmod{q}$ for $0 \leq r \leq p-1$, and therefore q divides D_n, contrary to the induction hypothesis. □

Theorem 2.7. *Let* $\left(u + v^{1/p}\right) = a_{n,0} + a_{n,1} v^{1/p} + a_{n,2} v^{2/p} + \cdots + a_{n,p-1} v^{(p-1)/p}$ *for some integers* $a_{n,0}, a_{n,1}, \ldots, a_{n,p-1}$, *where* p *is an odd pirme,* u *and* v *are relatively prime positive integers and* v^p *is not an integer. Then either* $D_n = 1$ *or* D_n *is a power of* p.

Proof. We showed in the proof of Lemma 2.6 that the statement is true for $1 \leq n \leq p$. Assume it is true for some $n \geq p$, but false for $n+1$. Then there is a prime $q \neq p$ such that q divides D_{n+1} but q does not divide D_n. By Lemma 2.6, q does not divide $u^p + v$.

Let $A = \begin{pmatrix} u & 0 & 0 & \cdots & 0 & 0 & v \\ 1 & u & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & u & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & & & \cdots & 1 & u & 0 \\ 0 & & & \cdots & 0 & 1 & u \end{pmatrix}$. Then (2.2) can be written in matrix form as $\begin{pmatrix} a_{n+1,0} \\ a_{n+1,1} \\ a_{n+1,2} \\ \vdots \\ a_{n+1,p-2} \\ a_{n+1,p-1} \end{pmatrix} = A \begin{pmatrix} a_{n,0} \\ a_{n,1} \\ a_{n,2} \\ \vdots \\ a_{n,p-2} \\ a_{n,p-1} \end{pmatrix}$. It can be shown using elementary properties of determinants that $\det(A) = u^p + v$. It follows that $A^{-1} = \frac{1}{(u^p+v)}B$, where B is a matrix with integer entries. (See, for instance [3, p.219]).

Hence

$$\begin{pmatrix} a_{n,0} \\ a_{n,1} \\ a_{n,2} \\ \vdots \\ a_{n,p-2} \\ a_{n,p-1} \end{pmatrix} = A^{-1} \begin{pmatrix} a_{n+1,0} \\ a_{n+1,1} \\ a_{n+1,2} \\ \vdots \\ a_{n+1,p-2} \\ a_{n+1,p-2} \end{pmatrix} = \frac{1}{(u^p+v)} B \begin{pmatrix} a_{n+1,0} \\ a_{n+1,1} \\ a_{n+1,2} \\ \vdots \\ a_{n+1,p-2} \\ a_{n+1,p-1} \end{pmatrix}.$$

Thus for each i, $0 \le i \le p-1$, $(u^p+v)a_{n,i}$ is equal to a linear combination of $a_{n+1}, a_{n+1,1}, \ldots, a_{n+1,p-1}$ with integer coefficients. Since q divides D_{n+1}, q divides each of $a_{n+1,0}, a_{n+1,1}, \ldots, a_{n+1,p-1}$, and hence q divides $(u^p+v)a_{n,i}$ for all i. But q does not divide u^p+v, and so q divides $a_{n,i}$ for all i. Therefore q divides D_n, which contradicts our induction hypothesis. □

3. The Exact GCD for the Square Root Case

Theorem 3.1. *Let $(u+\sqrt{v})^n = a_n + b_n\sqrt{v}$ where u and v are relatively prime positive integers, v is not a square and a_n and b_n are integers. Let $D_n = \gcd(a_n, b_n)$.*
(a) If $u^2 - v$ is odd, $D_n = 1$ for all $n \ge 1$.
(b) If $u^2 - v \equiv 2 \pmod 4$, $D_{2n-1} = 2^{n-1}$ and $D_{2n} = 2^n$ for all $n \ge 1$.
(c) If $u^2 - v \equiv 4 \pmod 8$, $D_{3n-2} = 2^{3n-3}$, $D_{3n-1} = 2^{3n-2}$, and $D_{3n} = 2^{3n}$ for all $n \ge 1$.
(d) If $u^2 - v \equiv 0 \pmod 8$, $D_n = 2^{n-1}$ for all $n \ge 1$.

Proof. To prove (a) we suppose that $u^2 - v$ is odd. We have seen that $D_1 = 1$. Assume that $D_n = 1$ for some n, and that $D_{n+1} > 1$. By Theorem 2.1, we know that 2 divides D_{n+1}. In the proof of Lemma 2.3 we saw that

$$(u^2 - v)a_n = ua_{n+1} - vb_{n+1}$$
$$(u^2 - v)b_n = -a_{n+1} + ub_{n+1}.$$

Since 2 divides D_{n+1}, 2 divides a_{n+1} and b_{n+1}, and hence 2 must divide both $(u^2-v)a_n$ and $(u^2-v)b_n$. Since $u^2 - v$ is odd, 2 does not divide it, and thus 2 must divide a_n and b_n. Therefore 2 divides D_n, which contradicts the induction hypothesis.

For the proofs of (b), (c) and (d), we use the following notation: Let $a_n = D_n\alpha_n$ and $b_n = D_n\beta_n$. Note that α_n and β_n cannot both be even. Rewriting equation (2.1) in matrix form gives us

$$\begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix} = \begin{pmatrix} u & v \\ 1 & u \end{pmatrix} \begin{pmatrix} a_n \\ b_n \end{pmatrix} = D_n \begin{pmatrix} u & v \\ 1 & u \end{pmatrix} \begin{pmatrix} \alpha_n \\ \beta_n \end{pmatrix} \tag{3.1}$$

To prove (b), we suppose $u^2 - v \equiv 2 \pmod 4$. Then u and v are odd, and $u^2 \equiv 1 \pmod 4$. Hence $v \equiv 3 \pmod 4$.

We want to show that $D_{2n-1} = 2^{n-1}$ and $D_{2n} = 2^n$. We have seen that $D_1 = 1$. Since $(u + \sqrt{v})^2 = u^2 + v + 2u\sqrt{v}$ we have that $D_2 = \gcd(u^2 + v, 2u) = 2$. Hence the statement is true for $n = 1, 2$.

Suppose it is true for $1 \le i \le n$ for some $n \ge 2$. We will show that $D_{n+2} = 2D_n$, from which the statement of (b) follows by induction. By equation (3.1) we have that

$$\begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix} = A \begin{pmatrix} a_n \\ b_n \end{pmatrix} = D_n A \begin{pmatrix} \alpha_n \\ \beta_n \end{pmatrix}$$

where $A = \begin{pmatrix} u & v \\ 1 & u \end{pmatrix}$. It follows that

$$\begin{pmatrix} a_{n+2} \\ b_{n+2} \end{pmatrix} = D_n A^2 \begin{pmatrix} \alpha_n \\ \beta_n \end{pmatrix} = D_n \begin{pmatrix} u^2 + v & 2uv \\ 2u & u^2 + v \end{pmatrix} \begin{pmatrix} \alpha_n \\ \beta_n \end{pmatrix}$$

Then we have that

$$\begin{pmatrix} a_{n+2} \\ b_{n+2} \end{pmatrix} = 2D_n \frac{A^2}{2} \begin{pmatrix} \alpha_n \\ \beta_n \end{pmatrix} = 2D_n \begin{pmatrix} \dfrac{u^2 + v}{2} & uv \\ u & \dfrac{u^2 + v}{2} \end{pmatrix} \begin{pmatrix} \alpha_n \\ \beta_n \end{pmatrix}$$

Note that $u^2 + v \equiv 1 + 3 \equiv 0 \pmod 4$. Hence $\dfrac{u^2 + v}{2}$ is even, and u and uv are both odd.

Let $\bar{B} = \dfrac{A^2}{2} \pmod 2$. Then $\bar{B} = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix}$. This implies that

$$\begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix} \begin{pmatrix} \alpha_n \\ \beta_n \end{pmatrix} = \begin{pmatrix} \beta_n \\ \alpha_n \end{pmatrix} \neq \begin{pmatrix} \bar{0} \\ \bar{0} \end{pmatrix} \pmod 2,$$

since α_n and β_n cannot both be even. It follows that the entries of $\dfrac{A^2}{2} \begin{pmatrix} \alpha_n \\ \beta_n \end{pmatrix}$ are not both even, and hence their greatest common divisor is not even. Therefore $D_{n+2} = 2D_n$ thus proving (b).

To prove (c) we suppose that $u^2 - v \equiv 4 \pmod 8$. Both u and v are odd, thus $u^2 \equiv 1 \pmod 8$ and $v \equiv 5 \pmod 8$.

Observe that $D_1 = \gcd(u, 1) = 1$ and $D_2 = \gcd(u^2 + v, 2u)$. Since $u^2 + v \equiv 1 + 5 \equiv 6 \pmod 8$ and u is odd, we have that $D_2 = 2$.

Since $(u + \sqrt{v})^3 = u^3 + 3uv + (3u^2 + v)\sqrt{v}$ it is the case that $D_3 = \gcd(u^3 + 3uv, 3u^2 + v)$. We will show that $D_3 = 8$.

Since $u^2 \equiv 1 \pmod 8$ and $v \equiv 5 \pmod 8$, we see that

$$u^3 + 3uv = u(u^2 + 3v) \equiv u(1 + 15) \equiv 0 \pmod 8,$$

and

$$3u^2 + v \equiv 3 + 5 \equiv 0 \pmod 8.$$

Hence both $u^3 + 3uv$ and $3u^2 + v$ are divisible by 8. If they are both divisible by 16, then $3(u^3 + 3uv) - u(3u^2 + v) = 8uv$ is divisible by 16. But this is false since u and v are both odd. Hence $D_3 = 8$. (Recall that for all n, D_n is a nonnegative power of 2.)

We assume that $D_{3i-2} = 2^{3i-3}$, $D_{3i-1} = 2^{3i-2}$ and $D_{3i} = 2^{3i}$ for $1 \le i \le n$, and show that $D_{n+3} = 2^3 D_n$. Then the statement of (c) will follow by induction.

$$\begin{pmatrix} a_{n+3} \\ b_{n+3} \end{pmatrix} = D_n A^3 \begin{pmatrix} \alpha_n \\ \beta_n \end{pmatrix} = 2^3 D_n \frac{1}{8} \begin{pmatrix} u^3 + 3uv & 3u^2 v + v^2 \\ 3u^2 + v & u^3 + 3uv \end{pmatrix} \begin{pmatrix} \alpha_n \\ \beta_n \end{pmatrix}$$

Define $\bar{C} = \frac{1}{8}A^3 \pmod 8$. Since $\gcd(u^3+3uv, 3u^2+v) = 8$, $\dfrac{u^3+3uv}{8}$ and $\dfrac{3u^2+v}{8}$ are not both even. Since also $3(u^3+3uv) - u(3u^2+v) = 8uv$ is not divisible by 16, one of $\dfrac{u^3+3uv}{8}$ and $\dfrac{3u^2+v}{8}$ is even and the other is odd. Thus either $\bar{C} = \begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}$ or $\bar{C} = \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix}$. Hence $\bar{C}\begin{pmatrix} \alpha_n \\ \beta_n \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod 2$, which implies that the entries of $\dfrac{A^3}{8}\begin{pmatrix} \alpha_n \\ \beta_n \end{pmatrix}$ are not both even. Therefore $D_{n+3} = 2^3 D_n$.

For (d), we have that $u^2 - v \equiv 0 \pmod 8$, which implies that $u^2 \equiv 1 \pmod 8$ and $v \equiv 1 \pmod 8$.

We can show that $D_1 = 1$ and $D_2 = 2$. Assume that $D_i = 2^{i-1}$ for $1 \leq i \leq n$ for some $n > 1$. By equation (3.1) we see that

$$\begin{pmatrix} a_n \\ b_n \end{pmatrix} = \begin{pmatrix} u & v \\ 1 & u \end{pmatrix}\begin{pmatrix} a_{n-1} \\ b_{n-1} \end{pmatrix} = D_{n-1}\begin{pmatrix} u & v \\ 1 & u \end{pmatrix}\begin{pmatrix} \alpha_{n-1} \\ \beta_{n-1} \end{pmatrix} = D_{n-1}\begin{pmatrix} u\alpha_{n-1} + v\beta_{n-1} \\ \alpha_{n-1} + u\beta_{n-1} \end{pmatrix}.$$

Since $D_n = 2D_{n-1}$, $\gcd(u\alpha_{n-1} + v\beta_{n-1}, \alpha_{n-1} + u\beta_{n-1}) = 2$. Since $u^2 - v \equiv 0 \pmod 4$ and $u^2 \equiv 1 \pmod 4$, we see that $v \equiv 1 \pmod 4$ It follows that

$$u\alpha_{n-1} + v\beta_{n-1} \equiv u\alpha_{n-1} + \beta_{n-1} \pmod 4$$

and

$$u\alpha_{n-1} + \beta_{n-1} \equiv u(\alpha_{n-1} + u\beta_{n-1}) \pmod 4.$$

Therefore

$$u\alpha_{n-1} + v\beta_{n-1} \equiv u(\alpha_{n-1} + u\beta_{n-1}) \pmod 4.$$

Since u is odd and $\gcd(u\alpha_{n-1} + v\beta_{n-1}, \alpha_{n-1} + u\beta_{n-1}) = 2$, it must be the case that

$$u\alpha_{n-1} + v\beta_{n-1} \equiv \alpha_{n-1} + u\beta_{n-1} \equiv 2 \pmod 4.$$

Since $\begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix} = \begin{pmatrix} u & v \\ 1 & u \end{pmatrix}^2 \begin{pmatrix} a_n \\ b_n \end{pmatrix}$, we see that

$$\begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix} = D_{n-1}\begin{pmatrix} u^2+v & 2uv \\ 2u & u^2+v \end{pmatrix}\begin{pmatrix} \alpha_{n-1} \\ \beta_{n-1} \end{pmatrix} = 2D_{n-1}\begin{pmatrix} \frac{u^2+v}{2} & uv \\ u & \frac{u^2+v}{2} \end{pmatrix}\begin{pmatrix} \alpha_{n-1} \\ \beta_{n-1} \end{pmatrix}.$$

Since $u^2 + v \equiv 2 \pmod 8$ and $v \equiv 1 \pmod 4$, we have that

$$\frac{u^2+v}{2} \equiv 1 \pmod 4,$$

and

$$\left(\frac{u^2+v}{2}\right)\alpha_{n-1} + uv\beta_{n-1} \equiv \alpha_{n-1} + u\beta_{n-1} \pmod 4.$$

Also

$$u\alpha_{n-1} + \left(\frac{u^2+v}{2}\right)\beta_{n-1} \equiv u\alpha_{n-1} + \beta_{n-1} \pmod 4.$$

Hence each entry in

$$\begin{pmatrix} \frac{u^2+v}{2} & uv \\ u & \frac{u^2+v}{2} \end{pmatrix}\begin{pmatrix} \alpha_{n-1} \\ \beta_{n-1} \end{pmatrix} = \begin{pmatrix} \left(\frac{u^2+v}{2}\right)\alpha_{n-1} + uv\beta_{n-1} \\ u\alpha_{n-1} + \left(\frac{u^2+v}{2}\right)\beta_{n-1} \end{pmatrix}$$

is congruent to 2 (mod 4). Therefore $D_{n+1} = 2^2 D_{n-1} = 2^n$. The result of (d) follows by induction.

□

4. The Exact GCD for an Odd Prime p

Theorem 4.1. *Let* $\left(u+v^{1/p}\right)^n = a_{n,0}+a_{n,1}v^{1/p}+a_{n,2}v^{2/p}+\cdots+a_{n,p-1}v^{(p-1)/p}$ *for some integers* $a_{n,0}, a_{n,1}, \ldots, a_{n,p-1}$, *where* p *is a an odd prime,* u *and* v *are relatively prime positive integers, and* $v^{1/p}$ *is not an integer. 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, $D_{np+i} = p^n$ *for all* $n \geq 0$ *and* $0 \leq i \leq p-i$.
(c) If u^p+v *is divisible by* p^2, *then* $D_{n(p-1)+i} = p^n$ *where* $n \geq 0$ *and* $1 \leq i \leq p-1$.

Proof. We begin by proving (a). Suppose that u^p+v is not divisible by p. From the binomial expansion of $\left(u+v^{1/p}\right)^n$ for $1 \leq n \leq p-1$ we see that $D_n = 1$ for $1 \leq n \leq p-1$. Suppose that $D_n = 1$ for some $n \geq p-1$ and $D_{n+1} > 1$. By Theorem 2.7 D_{n+1} is equal to a positive power of p. We saw in Section 2 that

$$\begin{pmatrix} a_{n,0} \\ a_{n,1} \\ a_{n,2} \\ \vdots \\ \vdots \\ a_{n,p-2} \\ a_{n,p-1} \end{pmatrix} = \begin{pmatrix} u & 0 & 0 & \cdots & 0 & 0 & v \\ 1 & u & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & \vdots & \vdots & \cdots & 1 & u & 0 \\ 0 & \vdots & \vdots & \cdots & 0 & 1 & u \end{pmatrix}^{-1} \begin{pmatrix} a_{n+1,0} \\ a_{n+1,1} \\ a_{n+1,2} \\ \vdots \\ \vdots \\ a_{n+1,p-2} \\ a_{n+1,p-1} \end{pmatrix} = \frac{1}{(u^p+v)} A \begin{pmatrix} a_{n+1,0} \\ a_{n+1,1} \\ a_{n+1,2} \\ \vdots \\ \vdots \\ a_{n+1,p-2} \\ a_{n+1,p-1} \end{pmatrix}$$

where A is a $p \times p$ matrix with integer values. Hence each of $(u^p+v)a_{n,0}$, $(u^p+v)a_{n,1}, \ldots, (u^p+v)a_{n,p-1}$ is a linear combination of $a_{n+1,0}, a_{n+1,1}, \ldots a_{n+1,p-1}$ with integer coefficients. Since p divides D_{n+1} and p does not divide u^p+v, p divides $a_{n,0}$, $a_{n,1}, \ldots, a_{n,p-1}$ and hence divides D_n contrary to the induction hypothesis. □

In order to prove part (b) of Theorem 4.1 we will use the following lemma and corollary.

Lemma 4.1.

$$\begin{pmatrix} u & 0 & 0 & \cdots & 0 & 0 & v \\ 1 & u & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & \vdots & \vdots & \cdots & 1 & u & 0 \\ 0 & \vdots & \vdots & \cdots & 0 & 1 & u \end{pmatrix}^n = \begin{pmatrix} a_{n,0} & va_{n,p-1} & va_{n,p-2} & \cdots & va_{n,2} & va_{n,1} \\ a_{n,1} & a_{n,0} & va_{n,p-1} & \cdots & va_{n,3} & va_{n,2} \\ a_{n,2} & a_{n,1} & a_{n,0} & \cdots & \vdots & va_{n,3} \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ a_{n,p-2} & \vdots & \vdots & \cdots & a_{n,0} & va_{n,p-1} \\ a_{n,p-1} & \vdots & \vdots & \cdots & a_{n,1} & a_{n,0} \end{pmatrix}$$

for all $n \geq 1$.

Proof. The result is proved by a straightforward induction argument. □

Corollary 4.2. *For all* $n \geq 1$, $(u^p+v)^n$ *is divisble by* $(D_n)^p$.

Proof. Equate the determinants in the statement of Lemma 4.1. Recall that

$$\det\left(\begin{pmatrix} u & 0 & 0 & \cdots & 0 & 0 & v \\ 1 & u & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & u & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots & \vdots \\ 0 & \vdots & \vdots & \cdots & 1 & u & 0 \\ 0 & \vdots & \vdots & \cdots & 0 & 1 & u \end{pmatrix}^n\right) = \left(\det\begin{pmatrix} u & 0 & 0 & \cdots & 0 & 0 & v \\ 1 & u & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & u & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots & \vdots \\ 0 & \vdots & \vdots & \cdots & 1 & u & 0 \\ 0 & \vdots & \vdots & \cdots & 0 & 1 & u \end{pmatrix}\right)^n = (u^p+v)^n.$$

This implies that $(u^p+v)^n$ is equal to a homogeneous polynomial of degree p in $a_{n,0}, a_{n,1}, \ldots, a_{n,p-1}$. Since D_n divides each of $a_{n,0}, a_{n,1}, \ldots, a_{n,p-1}$, $(D_n)^p$ divides $(u^p+v)^n$.

□

Now we continue the proof of Theorem 4.1 proving part (b).

Proof. Suppose $u^p+v=pm$ for some m not divisible by p. We want to show that $D_n=1$ for $1\le n\le p-1$ and $D_{pn+i}=p$ for all $n\ge 1$ and $0\le i\le p-1$. We saw in the proof of (a) that $D_n=1$ for $1\le i\le p-1$. From the binomial expansion for $\left(u+v^{1/p}\right)^p$ we see that

$$D_p=\gcd\left(u^p+v,\binom{p}{1}u^{p-1},\binom{p}{2}u^{p-2},\ldots,\binom{p}{p-1}u\right)=p.$$

Suppose the result is true for some $n\ge p$ and some i where $0\le i\le p-1$. Then $D_{pn+i}=p^n$. We will show that $D_{p(n+1)+i}=p^{n+1}$, from which the result follows by induction.

$$\begin{pmatrix} a_{p(n+1)+i,0}\\ a_{p(n+1)+i,1}\\ \vdots\\ \vdots\\ \vdots\\ a_{p(n+1)+i,p-1}\end{pmatrix}=\begin{pmatrix} u & 0 & 0 & \cdots & 0 & 0 & v\\ 1 & u & 0 & \cdots & 0 & 0 & 0\\ 0 & 1 & u & \cdots & 0 & 0 & 0\\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots\\ 0 & \vdots & \vdots & \cdots & 1 & u & 0\\ 0 & \vdots & \vdots & \cdots & 0 & 1 & u\end{pmatrix}^p\begin{pmatrix} a_{pn+i,0}\\ a_{pn+i,1}\\ \vdots\\ \vdots\\ \vdots\\ a_{pn+i,p-1}\end{pmatrix}$$

$$=\begin{pmatrix} (u^p+v) & \binom{p}{p-1}uv & \cdots & \binom{p}{p-2}u^2v & \binom{p}{1}u^{p-1}v\\ \binom{p}{1}u^{p-1} & (u^p+v) & \cdots & \binom{p}{p-3}u^3v & \binom{p}{p-2}u^2v\\ \vdots & \vdots & \cdots & \vdots & \vdots\\ \binom{p}{p-2}u^2 & \binom{p}{p-3}u^3 & \cdots & (u^p+v) & \binom{p}{p-1}uv\\ \binom{p}{p-1}u & \binom{p}{p-2}u^2 & \cdots & \binom{p}{1}u^{p-1} & (u^p+v)\end{pmatrix}\begin{pmatrix} a_{pn+i,0}\\ a_{pn+i,1}\\ \vdots\\ \vdots\\ \vdots\\ a_{pn+i,p-1}\end{pmatrix}$$

Since p divides u^p+v, every entry in the $p\times p$ matrix is divisible by p. It follows that pD_{pn+i} divides each of $a_{p(n+1)+i,0}, a_{p(n+1)+i,1},\ldots a_{p(n+1)+i,p-1}$, and hence $pD_{pn+i}=p^{n+1}$ divides $D_{p(n+1)+i}$. Let $D_{p(n+1)+i}=p^r$. Then $r\ge n+1$.

By Corollary 4.2, $(D_{p(n+1)+i})^p$ divides $(u^p+v)^{p(n+1)+i}=p^{p(n+1)+i}m^{p(n+1)+i}$. Since $D_{p(n+1)+i}=p^r$, $rp\le p(n+1)+i$. But $rp\ge p(n+1)$, and therefore $n+1\le r\le n+1+\dfrac{i}{p}$.

Since $0\le i\le p-1$, $r=n+1$ and $D_{p(n+1)+i}=p^{n+1}$ proving (b).

To prove (c) we suppose that u^p+v is divisible by p^2.

Let $A=\begin{pmatrix} u & 0 & 0 & \cdots & v\\ 1 & u & 0 & \cdots & 0\\ \vdots & \vdots & \vdots & \cdots & \vdots\\ 0 & 0 & 0 & \cdots & u\end{pmatrix}$. The first column of A^p is

$$\left(u^p+v,\binom{p}{1}u^{p-1},\binom{p}{2}u^{p-2},\ldots,\binom{p}{p-1}u^p\right),$$

which comes from the expansion of $\left(u+v^{1/p}\right)^p$. Note that every term is divisible by p. It follows from Lemma 4.1 that every entry of A^p is divisible by p.

By Fermat's Little Theorem [4, p.24], $u^p \equiv u \pmod p$. Since $u^p + v$ is divisible by p^2, $u \equiv -v \pmod p$. Therefore

$$\bar{A} = \begin{pmatrix} u & 0 & 0 & \cdots & 0 & v \\ 1 & u & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & u \end{pmatrix} \equiv \begin{pmatrix} u & 0 & 0 & \cdots & 0 & -u \\ 1 & u & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & u \end{pmatrix} \pmod p.$$

Let $\bar{B} = \dfrac{1}{p}A^p \pmod p$, and let $e = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$. Then for any $p \times p$ matrix C, Ce is equal to the first column of C. □

Lemma 4.2. *The set $\{e, \bar{A}e, \bar{A}^2e, \ldots, \bar{A}^{p-1}e\}$ is linearly independent, and hence is a basis for $(\mathbb{Z}_p)^p$.*

Proof. For $0 \le r \le p-1$, the entries of $\bar{A}^r e$ are the coefficients of $v^0, v^{1/p}, v^{2/p}, \ldots, v^{(p-1)/p}$ in the expansion of $\left(u + v^{1/p}\right)^r$. Hence all the entries in column r below the r-th place are zero. Thus the matrix with columns $e, \bar{A}e, \bar{A}^2e, \ldots, \bar{A}^{p-1}e$ is upper triangular, and therefore its determinant is equal to the product of the diagonal elements [3, p.207].

The r-th diagonal element is the coefficient of $v^{r/p}$ in the expansion of $\left(u + v^{1/p}\right)^r$, which is 1. Hence every diagonal element is 1, and the determinant is nonzero. Therefore the matrix is invertible, and the column vectors $e, \bar{A}e, \bar{A}^2e, \ldots, \bar{A}^{p-1}e$ are linearly independent. [3, p.151] □

Lemma 4.3. *$\bar{B}e, \bar{B}\bar{A}e, \bar{B}\bar{A}^2e, \ldots, \bar{B}\bar{A}^{p-2}e$ are all nonzero and $\bar{B}\bar{A}^{p-1}e = 0$.*

Proof. Since $\bar{B} \equiv \frac{1}{p}A^p \pmod p$, the statements are equivalent to the following:

(1) At least one entry of $A^{p+r}e$ is not divisible by p^2 for $0 \le r \le p-2$.
(2) Every entry of $A^{2p-1}e$ is divisible by p^2.

We first show that (i) is true. The entries of $A^{p+r}e$ are the coefficients of $v^0, v^{1/p}, v^{2/p}, \ldots, v^{(p-1)/p}$ in the expansion of $\left(u + v^{1/p}\right)^{p+r}$ where $0 \le r \le p-2$. The coefficient of $v^{(r+1)/p}$ is $\binom{p+r}{r+1}u^{2p-1}$, and $\binom{p+r}{r+1} = \dfrac{(p+r)(p+r-1)\cdots p}{(r+1)!}$. The numerator is divisible by p but not by p^2.

The i-th entry of $A^{2p-1}e$ is the coefficient of $v^{i/p}$ in the expansion of $\left(u + v^{1/p}\right)^{2p-1}$, which is $\binom{2p-1}{i}u^{2p-1-i} + \binom{2p-1}{p+i}u^{p-1-i}v = u^{p-1-i}\left(\binom{2p-1}{i}u^p + \binom{2p-1}{p+i}v\right)$. Since $\binom{2p-1}{i}u^p + \binom{2p-1}{p+i}v = \binom{2p-1}{i}(u^p + v) + \left(\binom{2p-1}{p+i} - \binom{2p-1}{i}\right)v$ and p^2 divides $(u^p + v)$, it is sufficient to show that p^2 divides $\binom{2p-1}{p+i} - \binom{2p-1}{i}$ for $0 \le i \le p-1$.

We use induction on i. The result is true when $i = 0$ by a result of Charles Babbage [1]

Suppose it is true for some $i < p-1$. Observe that

$$\binom{2p-1}{p+i+1} = \frac{p-i-1}{p+i+1}\binom{2p-1}{p+i}$$

and

$$\binom{2p-1}{i+1} = \frac{2p-i-1}{i+1}\binom{2p-1}{i}.$$

Then

$$\binom{2p-1}{p+i+1} - \binom{2p-1}{i+1}$$
$$= \frac{p-i-1}{p+i-1}\left(\binom{2p-1}{p+i} - \binom{2p-1}{i}\right) + \left(\frac{p-i-1}{p+i+1} - \frac{2p-i-1}{i+1}\right)\binom{2p-1}{i}.$$

Observe that $\dfrac{p-i-1}{p+i+1} - \dfrac{2p-i-1}{i+1} = -\dfrac{2p^2}{(p+i+1)(i+1)}$. Since p^2 divides $\binom{2p-1}{p+i} - \binom{2p-1}{i}$ and neither $(p+i+1)$ nor $(i+1)$ is divisible by p, $\binom{2p-1}{p+i+1} - \binom{2p-1}{i+1}$ is divisible by p^2, and the result follows. □

Lemma 4.4. $\text{Null}(\bar{A}) = \left\langle \begin{pmatrix} 1 \\ -u^{p-2} \\ u^{p-3} \\ \vdots \\ -u \\ 1 \end{pmatrix} \right\rangle = \langle \bar{A}^{p-1}e \rangle$, *where* $\langle S \rangle$ *is the subspace spanned by the set* S *of vectors.*

Proof. Recall that $\bar{A} = \begin{pmatrix} u & 0 & 0 & \cdots & 0 & 0 & v \\ 1 & u & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & u & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 & u \end{pmatrix}$. The unique solution of $\bar{A}\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_p \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ is $t\begin{pmatrix} 1 \\ -u^{p-2} \\ u^{p-3} \\ \vdots \\ -u \\ 1 \end{pmatrix}$ for some t in $\mathbb{Z}_p$. Note that since p does not divide u, Fermat's Little Theorem implies that $u^{p-1} \equiv 1 \pmod{p}$. By expanding $(u + v^{1/p})^{p-1} \pmod{p}$, we can show that $\bar{A}^{p-1}e = \begin{pmatrix} 1 \\ -u^{p-2} \\ u^{p-3} \\ \vdots \\ -u \\ 1 \end{pmatrix}$. □

Lemma 4.5. $\text{Null}(\bar{B}) = \left\langle \begin{pmatrix} 1 \\ -u^{p-2} \\ u^{p-3} \\ \vdots \\ -u \\ 1 \end{pmatrix} \right\rangle = \langle \bar{A}^{p-1}e \rangle$.

Proof. By Lemma 4.2, the set $\{e, \bar{A}e, \bar{A}^2e, \ldots, \bar{A}^pe\}$ is a basis for $(\mathbb{Z}_p)^p$. Let $x \in \text{Null}(\bar{B})$. Then $x = c_0e + c_1\bar{A}e + c_2\bar{A}^2e + \cdots + c_{p-1}\bar{A}^{p-1}e$ for some $c_0, c_1, \ldots, c_{p-1}$ in $\mathbb{Z}_p$. Since by Lemma 4.3 $\bar{B}\bar{A}^{p-1}e = 0$, we have that $\bar{B}x = c_0\bar{B}e + c_1\bar{B}\bar{A}e + c_2\bar{B}\bar{A}^2e + \cdots + c_{p-2}\bar{B}\bar{A}^{p-2}e = 0$. This implies that $\bar{A}^{p-2}(c_0\bar{B}e + c_1\bar{B}\bar{A}e + c_2\bar{B}\bar{A}^2 + \cdots + c_{p-2}\bar{B}\bar{A}^{p-2}e = 0$. Since $\bar{A}\bar{B} \equiv$

$\bar{B}\bar{A} \equiv \frac{1}{p}A^{p+1} \pmod{p}$, and $\bar{B}\bar{A}^r e = 0$ for all $r \geq p-1$, $c_0\bar{B}\bar{A}^{p-2}e = 0$, and hence $c_0 = 0$. Similarly we see that $\bar{A}^{p-3}(c_1\bar{B}\bar{A}e + c_2\bar{B}\bar{A}^2e + \cdots + c_{p-2}\bar{B}\bar{A}^{p-2}e) = 0$ implies that $c_1 = 0$. By similar reasoning, $c_r = 0$ for $0 \leq r \leq p-2$. So $x = c_{p-1}\bar{A}^{p-1}e$, and hence x is in $\langle \bar{A}^{p-1}e \rangle$. □

Lemma 4.6. *$D_{n+p} \geq pD_n$.*

Proof. First note that $\begin{pmatrix} a_{n,0} \\ a_{n,1} \\ \vdots \\ a_{n,p-1} \end{pmatrix} = D_n \begin{pmatrix} \alpha_{n,0} \\ \alpha_{n,1} \\ \vdots \\ \alpha_{n,p-1} \end{pmatrix}$, where $\gcd(\alpha_{n,0}, \alpha_{n,1}, \ldots, \alpha_{n,p-1})$ is not divisible by p. Then

$$\begin{pmatrix} a_{n+p,0} \\ a_{n+p,1} \\ \vdots \\ a_{n+p,p-1} \end{pmatrix} = A^p \begin{pmatrix} a_{n,0} \\ a_{n,1} \\ \vdots \\ a_{n,p-1} \end{pmatrix} = A^p D_n \begin{pmatrix} \alpha_{n,0} \\ \alpha_{n,1} \\ \vdots \\ \alpha_{n,p-1} \end{pmatrix}.$$

Since every entry in the matrix A^p is divisible by p, every entry in $A^p \begin{pmatrix} \alpha_{n,0} \\ \alpha_{n,1} \\ \vdots \\ \alpha_{n,p-1} \end{pmatrix}$ is a multiple of p. Therefore $D_{n+p} \geq pD_n$.

□

Lemma 4.7. *$D_{n+p} \geq p^2 D_n$ if and only if $D_{n+1} \geq pD_n$.*

Proof. Suppose that $D_{n+p} \geq p^2 D_n$. Then

$$\begin{pmatrix} a_{n+p,0} \\ a_{n+p,1} \\ \vdots \\ a_{n+p,p-1} \end{pmatrix} = A^p \begin{pmatrix} a_{n,0} \\ a_{n,1} \\ \vdots \\ a_{n,p-1} \end{pmatrix} = A^p D_n \begin{pmatrix} \alpha_{n,0} \\ \alpha_{n,1} \\ \vdots \\ \alpha_{n,p-1} \end{pmatrix} = pD_n \frac{1}{p} A^p \begin{pmatrix} \alpha_{n,0} \\ \alpha_{n,1} \\ \vdots \\ \alpha_{n,p-1} \end{pmatrix}.$$

Since $D_{n+p} \geq p^2 D_n$, then every entry in $\frac{1}{p}A^p \begin{pmatrix} \alpha_{n,0} \\ \alpha_{n,1} \\ \vdots \\ \alpha_{n,p-1} \end{pmatrix}$ must be divisible by p. Therefore $\bar{B} \begin{pmatrix} \alpha_{n,0} \\ \alpha_{n,1} \\ \vdots \\ \alpha_{n,p-1} \end{pmatrix} \equiv 0 \pmod{p}$. By Lemma 4.5, $\begin{pmatrix} \alpha_{n,0} \\ \alpha_{n,1} \\ \vdots \\ \alpha_{n,p-1} \end{pmatrix} = t \begin{pmatrix} 1 \\ -u^{p-2} \\ u^{p-3} \\ \vdots \\ -u \\ 1 \end{pmatrix}$ for some t in $\mathbb{Z}_p$.

By Lemma 4.4 $\bar{A}\begin{pmatrix}\alpha_{n,0}\\ \alpha_{n,1}\\ \vdots\\ \alpha_{n,p-1}\end{pmatrix} \equiv 0 \pmod{p}$. This implies that each entry in $A\begin{pmatrix}\alpha_{n,0}\\ \alpha_{n,1}\\ \vdots\\ \alpha_{n,p-1}\end{pmatrix}$ is divisible by p. Since

$$\begin{pmatrix}a_{n+1,0}\\ a_{n+1,1}\\ \vdots\\ a_{n+1,p-1}\end{pmatrix} = A\begin{pmatrix}a_{n,0}\\ a_{n,1}\\ \vdots\\ a_{n,p-1}\end{pmatrix} = D_nA\begin{pmatrix}\alpha_{n,0}\\ \alpha_{n,1}\\ \vdots\\ \alpha_{n,p-1}\end{pmatrix},$$

it follows that $D_{n+1} \geq pD_n$.

Now suppose that $D_{n+1} \geq pD_n$. Since

$$\begin{pmatrix}a_{n+1,0}\\ a_{n+1,1}\\ \vdots\\ a_{n+1,p-1}\end{pmatrix} = \begin{pmatrix}a_{n,0}\\ a_{n,1}\\ \vdots\\ a_{n,p-1}\end{pmatrix} = D_nA\begin{pmatrix}\alpha_{n,0}\\ \alpha_{n,1}\\ \vdots\\ \alpha_{n,p-1}\end{pmatrix},$$

the entries of $A\begin{pmatrix}\alpha_{n,0}\\ \alpha_{n,1}\\ \vdots\\ \alpha_{n,p-1}\end{pmatrix}$ are divisible by p. Hence $\bar{A}\begin{pmatrix}\alpha_{n,0}\\ \alpha_{n,1}\\ \vdots\\ \alpha_{n,p-1}\end{pmatrix} \equiv 0 \pmod{p}$.

By Lemma 4.4 $\begin{pmatrix}\alpha_{n,0}\\ \alpha_{n,1}\\ \vdots\\ \alpha_{n,p-1}\end{pmatrix} = t\begin{pmatrix}1\\ -u^{p-2}\\ u^{p-3}\\ \vdots\\ -u\\ 1\end{pmatrix}$ for some t in $\mathbb{Z}_p$. By Lemma 4.5, $\bar{B}\begin{pmatrix}\alpha_{n,0}\\ \alpha_{n,1}\\ \vdots\\ \alpha_{n,p-2}\end{pmatrix} \equiv 0 \pmod{p}$.

Therefore every entry in $\frac{1}{p}A^p\begin{pmatrix}\alpha_{n,0}\\ \alpha_{n,1}\\ \vdots\\ \alpha_{n,p-1}\end{pmatrix}$ is a multiple of p.

Since

$$\begin{pmatrix}a_{n+p,0}\\ a_{n+p,1}\\ \vdots\\ a_{n+p,p-1}\end{pmatrix} = A^p\begin{pmatrix}a_{n,0}\\ a_{n,1}\\ \vdots\\ a_{n,p-1}\end{pmatrix} = A^pD_n\begin{pmatrix}\alpha_{n,0}\\ \alpha_{n,1}\\ \vdots\\ \alpha_{n,p-1}\end{pmatrix} = pD_n\frac{1}{p}A^p\begin{pmatrix}\alpha_{n,0}\\ \alpha_{n,1}\\ \vdots\\ \alpha_{n,p-1}\end{pmatrix},$$

we have that $D_{n+p} \geq p^2D_n$.

□

Corollary 4.3. *$D_{n+1} = D_n$ if and only if $D_{n+p} = pD_n$.*

Proof. Suppose $D_{n+1} = D_n$. By Lemma 4.7, $D_{n+p} < p^2D_n$. But Lemma 4.6 says that $D_{n+p} \geq pD_n$. Therefore $D_{n+p} = pD_n$.

Now suppose that $D_{n+p} = pD_n$. By Lemma 4.7 we have that $D_{n+1} < pD_n$. But $D_{n+1} \geq D_n$ and both D_n and D_{n+1} are equal to a power of p. Therefore $D_{n+1} = D_n$. □

Finally we are ready to prove (c).

Proof. We want to show that $D_{n(p-1)}+i = p^n$ for $n \geq 0$ and $1 \leq i \leq p-1$. We first prove that it is true for $n = 0$ and $n = 1$. By using the binomial expansion of $\left(u + v^{1/p}\right)^i$ we can show that $D_i = 1$ for $1 \leq i \leq p-1$ and $D_p = p$. In the proof of Lemma 4.3 we saw that at least one entry of $A^{p+r}e$ is not divisible by p^2 for $0 \leq r \leq p-2$. This, together with the result of Lemma 2.4 that D_i divides D_{i+1} for all i, implies that $D_i = p$ for $p \leq i \leq 2p-2$. Hence the result is true for $n = 0$ and for $n = 1$.

Now suppose that it is true for $1 \leq i \leq n(p-1)+p-1$ for some $n \geq 1$. Then $D_{n(p-1)+1} = p^n$ and $D_{n(p-1)} = D_{(n-1)(p-1)+p-1} = p^{n-1}$. Hence $D_{n(p-1)+1} = pD_{n(p-1)}$. By Lemma 4.7 $D_{(n+1)(p-1)+1} = D_{n(p-1)+p} \geq p^2 D_{n(p-1)} = p^{n+1}$.

It is also true that $D_{n(p-1)+p-1} = D_{n(p-1)+p-2} = p^n$. By Corollary 4.3, $D_{n(p-1)+p-2+p} = pD_{n(p-1)+p-2} = p^{n+1}$. That is $D_{(n+1)(p-1)+p-1} = p^{n+1}$. Since D_i is nondecreasing as i increases (by Lemma 2.4), $D_{(n+1)(p-1)+i} = p^n$ for $1 \leq i \leq p-1$. The result follows by induction. □

References

[1] Babbage, C. Demonstration of a theorem relating to prime numbers. *The Edinburgh Philosophical Journal 1* (1819), 46–49.

[2] Columbus State University Problem Solving Group Proposal 2137. Problems and solutions. *Mathematics Magazine 95*, 1 (2022), 73–82.

[3] S.H. Friedberg, A.J. Insel, and L.E. Spence. *Linear Algebra*, 3 ed. Prentice Hall, 1997.

[4] Shifrin, T. *Abstract Algebra - A Geometric Approach*, 1 ed. Prentice Hall, 1996.