

syringe of the "tuberculin" type, which contains one milliliter (formerly styled "cubic centimeter") and is calibrated at hundredths, 0.01, 0.02, ..., 0.99, 1.00 ml. The first five injections were administered one every seven days beginning later November through December. The first five amounts measured were 0.08, 0.13, 0.21, 0.34, and 0.55. The greatest and least increments between any of these doses were 62.5 percent and 61.5385... percent. Q.E.D.

For another patient, a sequence of dosages growing stronger at a rate of approximately 27 percent might be appropriate. Such a sequence could be given using two solutions, A and B, with B approximately 27 percent stronger than A and alternating the dosages between the solutions as follows:

0.08A, 0.08B, 0.13A, 0.13B, 0.21A, 0.21B,

We shall follow up the progress of these patients and shall review other patients' allergic problems in a later paper.

So far, we have considered the mathematical problems met in sensory biology and in allergy-immunology but not often solved by nonmathematicians. We have touched upon the special limitations imposed by our tools that measure out amounts of liquids, and have groped toward adapting these tools for best results. We shall aim to get results that can be safe, simple, and on the mark. Our quest will lead us through continued fractions, and sometimes through Fibonacci-ratio fractional approximations.

VALUES OF CIRCULANTS WITH INTEGER ENTRIES

H. TURNER LAQUER

Student, University of New Mexico, Albuquerque, NM 87131

It is well known that the differences of squares $m = x^2 - y^2$, with x and y integers, are the integers satisfying $2 \nmid m$ or $4 \mid m$. It is not difficult to show that the integers m of the form $x^3 + y^3 + z^3 - 3xyz$, with x, y , and z integers, are those integers satisfying $3 \nmid m$ or $9 \mid m$. This paper generalizes on those results.

Let $C_n(x_1, \dots, x_n)$ be the determinant of the circulant matrix (a_{ij}) in which $a_{ij} = x_k$ when $j - i + 1 \equiv k \pmod{n}$. Note that $C_2(x, y) = x^2 - y^2$ and $C_3(x, y, z) = x^3 + y^3 + z^3 - 3xyz$.

Let V_n be the set of values of C_n when the domain is the set of all ordered n -tuples (x_1, \dots, x_n) with integer entries x_k . We will show below that, for odd primes p , V_p consists of the integers m with either $p \nmid m$ or $p^2 \mid m$, and that V_{2p} consists of the integers m satisfying either $p \nmid m$ or $p^2 \mid m$ and also satisfying either $2 \nmid m$ or $4 \mid m$, i.e.,

$$V_{2p} = [\{m:p \nmid m\} \cup \{m:p^2 \mid m\}] \cap [\{m:2 \nmid m\} \cup \{m:4 \mid m\}].$$

1. GENERAL N

In this section, the x_k may be any complex numbers. It is well known (see [1]) that

$$(1.1) \quad C_n(x_1, \dots, x_n) = \prod_{h=0}^{n-1} \left(\sum_{k=1}^n x_k \exp[2\pi h(k-1)i/n] \right).$$

We use this to establish the following.

Theorem 1: $C_n(x_1 + a, x_2 + a, \dots, x_n + a) = R \cdot C_n(x_1, x_2, \dots, x_n)$ where $R = (na + x_1 + x_2 + \dots + x_n) / (x_1 + x_2 + \dots + x_n)$.

Proof:

$$\begin{aligned} C_n(x_1 + a, \dots, x_n + a) &= \prod_{h=0}^{n-1} \left(\sum_{k=1}^n (x_k + a) \exp[2\pi h(k-1)i/n] \right) \\ &= \prod_{h=0}^{n-1} \left(\sum_{k=1}^n x_k \exp[2\pi h(k-1)i/n] + a \sum_{k=1}^n \exp[2\pi h(k-1)i/n] \right). \end{aligned}$$

Now

$$\sum_{k=1}^n \exp[2\pi h(k-1)i/n] = \begin{cases} n & \text{for } h = 0 \\ \frac{1 - \exp(2\pi hni/n)}{1 - \exp(2\pi hi/n)} = 0 & \text{for } 1 \leq h \leq n-1. \end{cases}$$

Thus

$$\begin{aligned} C_n(x_1 + a, \dots, x_n + a) &= \left(na + \sum_{k=1}^n x_k \right) \cdot \prod_{h=0}^{n-1} \left(\sum_{k=1}^n x_k \exp[2\pi h(k-1)i/n] \right) \\ &= C_n(x_1, \dots, x_n) \left(na + \sum_{k=1}^n x_k \right) / \left(\sum_{k=1}^n x_k \right). \end{aligned}$$

Another result to be used later is the following.

Theorem 2: Let $n = rs$ where r and s are relatively prime. Then

$$C_n(x_1, \dots, x_n) = \prod_{g=0}^{s-1} C_r(y_{g1}, y_{g2}, \dots, y_{gr})$$

where

$$y_{gj} = \sum_{k=0}^{s-1} x_{kr+j} \exp[2\pi g(kr+j-1)i/s].$$

Proof:

$$\begin{aligned} \prod_{g=0}^{s-1} C_r(y_{g1}, \dots, y_{gr}) &= \prod_{g=0}^{s-1} \prod_{h=0}^{r-1} \left(\sum_{j=1}^r y_{gj} \exp[2\pi h(j-1)i/r] \right) \\ &= \prod_{g=0}^{s-1} \prod_{h=0}^{r-1} \left(\sum_{j=1}^r \sum_{k=0}^{s-1} x_{kr+j} \exp\{2\pi i[g(kr+j-1)/s + h(j-1)/r]\} \right) \\ &= \prod_{g=0}^{s-1} \prod_{h=0}^{r-1} \left(\sum_{k=0}^{s-1} \sum_{j=1}^r x_{kr+j} \exp\left\{ \frac{2\pi i}{n} [(rg+sh)(j-1) + r^2 gk] \right\} \right) \\ &= \prod_{g=0}^{s-1} \prod_{h=0}^{r-1} D(g, h). \end{aligned}$$

In $D(g, h)$ each variable x_t appears once and only once. Let d_t be the coefficient of x_t . Then

$$\frac{d_{t+1}}{d_t} = \frac{\exp\{2\pi i[(rg+sh)j + r^2 gk]/n\}}{\exp\{2\pi i[(rg+sh)(j-1) + r^2 gk]/n\}} = \exp\{2\pi i(rg+sh)/n\}$$

or

$$\begin{aligned} \frac{d_{t+1}}{d_t} &= \frac{\exp\{2\pi i[(rg+sh)(1-1) + r^2 g(k+1)]/n\}}{\exp\{2\pi i[(rg+sh)(r-1) + r^2 gk]/n\}} \\ &= \exp[2\pi i(rg+sh-rsh)/n] \\ &= \exp[2\pi i(rg+sh)/n] \cdot \exp(-2\pi ih) \\ &= \exp[2\pi i(rg+sh)/n]. \end{aligned}$$

Also, d_1 occurs when $k=0$ and $j=1$. So $d_1 = \exp 0 = 1$. Thus

$$D(g, h) = \sum_{t=1}^n x_t \exp[2\pi i(rg+sh)(t-1)/n].$$

Now as g goes from 0 to $s-1$ and h goes from 0 to $r-1$, $(rg+sh) \pmod n$ takes on n values. To see that these n values are distinct, one has that if $rg_1 + sh_1 \equiv rg_2 + sh_2 \pmod n$ then $r(g_1 - g_2) \equiv s(h_2 - h_1) \pmod n$. As $\gcd(r, s) = 1$, one then has $r \mid (h_2 - h_1)$ and $s \mid (g_1 - g_2)$. But $0 \leq g \leq s-1$ and $0 \leq h \leq r-1$, so $h_2 - h_1 = g_1 - g_2 = 0$. Thus $h_1 = h_2$ and $g_1 = g_2$. Hence $(rg+sh) \pmod n$ achieves every value from 0 to $n-1$. Thus

$$\prod_{g=0}^{s-1} C_r(y_{g1}, \dots, y_{gr}) = \prod_{k=0}^{n-1} \left(\sum_{t=1}^n x_t \exp[2\pi ikt/n] \right) = C_n(x_1, \dots, x_n).$$

Corollary: Let $n = 2r$ where r is an odd integer. Then $C_n(x_1, \dots, x_n)$

$$= C_r(x_1 + x_{r+1}, x_2 + x_{r+2}, \dots, x_r + x_{2r}) \cdot C_r(x_1 - x_{r+1}, x_2 - x_{r+2}, \dots, x_r - x_{2r}).$$

Proof: $C_n(x_1, \dots, x_n) = C_r(y_{01}, \dots, y_{0r})C(y_{11}, \dots, y_{1r})$ where

$$y_{0j} = x_j e^0 + x_{r+j} e^0 = x_j + x_{r+j}$$

and

$$y_{1j} = x_j (-1)^{j-1} + x_{r+j} (-1)^{(r+j-1)} = (-1)^{j-1} (x_j - x_{r+j})$$

since r is an odd integer.

It is now useful to obtain some n -tuples that produce various values in V_n .

Lemma 1: $C_n(2, 0, 1, 1, 1, \dots, 1) = n^2$.

Proof: By adding every row to the first row and every column to the first column in the determinant form of $C_n(2, 0, 1, 1, 1, \dots, 1)$ one has

$$C_n(2, 0, 1, 1, 1, \dots, 1) = \begin{vmatrix} n^2 & n & n & n & \dots & n \\ n & 2 & 0 & 1 & \dots & 1 \\ n & 1 & 2 & 0 & \dots & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ n & 1 & 1 & 1 & \dots & 2 \end{vmatrix}$$

One can then factor n from both the first column and the first row. One then adds the negative of the first row to each of the succeeding rows to obtain an upper triangular determinant all of whose diagonal elements are 1. Thus, $C_n(2, 0, 1, 1, 1, \dots, 1) = n^2$.

By Theorem 1, with $a = j - 1$, one has the following.

Theorem 3: $C_n(j + 1, j - 1, j, j, j, \dots, j) = jn^2$.

Lemma 2: Let $A(n, r) = C_n(1, 1, \dots, 1, 0, \dots, 0)$ where the first r elements of the C_n are one and the rest are zero. One has, if $\gcd(n, r) > 1$, then $A(n, r) = 0$, and if $\gcd(n, r) = 1$, then $A(n, r) = r$.

Proof: From (1.1) one has

$$A(n, r) = \prod_{h=0}^{n-1} \left(\sum_{k=1}^r \exp[2\pi h(k-1)i/n] \right) = r \prod_{h=1}^{n-1} \left(\frac{1 - \exp(2\pi h r i/n)}{1 - \exp(2\pi h i/n)} \right)$$

If $\gcd(n, r) = j > 1$, then when $h = n/j$ (which is $\leq n - 1$) one has $1 - \exp(2\pi h r i/n) = 0$ and $A(n, r) = 0$. If $\gcd(n, r) = 1$, then letting $\theta = \exp(2\pi i/n)$ one has

$$A(n, r) = r \prod_{h=1}^{n-1} [(1 - \theta^{hr}) / (1 - \theta^h)].$$

Suppose $\theta^{hr} = 1$. Then $hr \equiv 0 \pmod{n}$ and as $\gcd(n, r) = 1$, one has $h \equiv 0 \pmod{n}$ which has no solutions when $1 \leq h \leq n - 1$. Suppose $\theta^{jr} = \theta^{kr}$. Then $jr \equiv kr \pmod{n}$ and as $\gcd(n, r) = 1$, one has $j \equiv k \pmod{n}$. The only solution to this when $1 \leq j \leq n - 1$ and $1 \leq k \leq n - 1$ is $j = k$. Thus the $n - 1$ terms $(1 - \theta^{hr})$, $1 \leq h \leq n - 1$, are all different and nonzero. As there are only $n - 1$ different nonzero terms of the form $(1 - \theta^k)$, one has that these $n - 1$ terms are the same as the $n - 1$ terms $(1 - \theta^k)$ with $1 \leq k \leq n - 1$. Thus, if $\gcd(n, r) = 1$, then $A(n, r) = r$.

By Theorem 1, one has the following.

Theorem 4: Let $A(n, r, j) = C_n(x_1, \dots, x_n)$ where x_1 through x_r equal $j + 1$ and x_{r+1} through x_n equal j . One has, if $\gcd(n, r) > 1$, then $A(n, r, j) = 0$ and if $\gcd(n, r) = 1$, then $A(n, r, j) = nj + r$.

2. THE CASE $N = P$, AN ODD PRIME

Consider $C_p(x_1, x_2, \dots, x_p)$ where p is an odd prime. Also let the x_k be integers from now on. Let the corresponding matrix be (a_{ij}) where $a_{ij} = x_k$ when $j - i + 1 \equiv k \pmod{p}$.

Lemma 3: $C_p(x_1, \dots, x_p) \equiv x_1 + x_2 + \dots + x_p \pmod{p}$.

Proof: Consider any term $\prod_{k=1}^p a_{k, i_k}$ in the expansion of the determinant. Consider all terms $\prod_{k=1}^p a_{k-j, i_k-j}$ for all integers $j \geq 0$ where subscripts are taken mod p . This method divides all

terms in the expansion of the determinant into equivalence classes. If the initial term

equals x_i^p , then the class consists of just one member. In any other case, the class consists of p members of equal values in terms of the x_k 's. In addition, the sign of the permutation corresponding to the product is the same for each member of a class. This follows by induction, since

$$\begin{aligned} & [(i_3 - i_2)(i_4 - i_2) \dots (i_p - i_2)(i_1 - i_2)] \cdot [(i_4 - i_3) \dots (i_p - i_3)(i_1 - i_3)] \\ & \quad \dots [(i_p - i_{p-1})(i_1 - i_{p-1})] \cdot [(i_1 - i_p)] \\ = & (-1)^{p-1} [(i_2 - i_1)(i_3 - i_1) \dots (i_p - i_1)] \cdot [(i_3 - i_2) \dots (i_p - i_2)] \dots [(i_p - i_{p-1})] \\ = & [(i_2 - i_1)(i_3 - i_1) \dots (i_p - i_1)] \dots [(i_p - i_{p-1})] \end{aligned}$$

since p is odd. Thus in the expansion of the determinant, all of the p terms have the same sign and the same value. This implies that

$$(2.1) \quad C_p(x_1, \dots, x_p) \equiv x_1^p + x_2^p + \dots + x_p^p \pmod{p}.$$

Using Fermat's Theorem, (2.1) implies

$$(2.2) \quad C_p(x_1, \dots, x_p) \equiv x_1 + x_2 + \dots + x_p \pmod{p}.$$

One now has the following result.

Theorem 5: If $C_p(x_1, \dots, x_p)$ is divisible by p , it is divisible by p^2 .

Proof: If $C_p(x_1, \dots, x_p)$ is divisible by p , then (2.2) tells us that $\sum_{j=1}^p x_j$ is divisible by p . Also

$$\begin{aligned} C_p(x_1, \dots, x_p) &= \left(\sum_{j=1}^p x_j \right) \begin{vmatrix} 1 & x_2 & x_3 & \dots & x_p \\ 1 & x_1 & x_2 & \dots & x_{p-1} \\ 1 & x_p & x_1 & \dots & x_{p-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_3 & x_4 & \dots & x_1 \end{vmatrix} \\ &= \left(\sum_{j=1}^p x_j \right) \begin{vmatrix} p & \sum_{j=1}^p x_j & \sum_{j=1}^p x_j & \dots & \sum_{j=1}^p x_j \\ 1 & x_1 & x_2 & \dots & x_{p-1} \\ 1 & x_p & x_1 & \dots & x_{p-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_3 & x_4 & \dots & x_1 \end{vmatrix} \end{aligned}$$

Thus, if $\sum_{j=1}^p x_j$ is divisible by p , one can factor an additional p from each entry of the

first row of the last determinant and $C_p(x_1, \dots, x_p)$ is divisible by p^2 . This proves the theorem.

Now by using Theorems 3 and 4, one sees that V_p consists of the integers m satisfying either $p \nmid m$ or $p^2 \mid m$.

3. THE CASE $N = 2P$

Consider $C_{2p}(x_1, \dots, x_{2p})$ where p is an odd prime. By the Corollary to Theorem 2, one has

$$(3.1) \quad C_{2p}(x_1, \dots, x_{2p}) = C_p(y_1, \dots, y_p) \cdot C_p(z_1, \dots, z_p)$$

where $y_j = x_j + x_{p+j}$ and $z_j = (-1)^{j-1}(x_j - x_{p+j})$. One now has the following.

Theorem 6: If $C_{2p}(x_1, \dots, x_{2p})$ is divisible by p , it is divisible by p^2 .

Proof: If $p \mid C_{2p}(x_1, \dots, x_{2p})$, then $p \mid C_p(y_1, \dots, y_p)$ or $p \mid C_p(z_1, \dots, z_p)$. But then $p^2 \mid C_p(y_1, \dots, y_p)$ or $p^2 \mid C_p(z_1, \dots, z_p)$ and $p^2 \mid C_{2p}(x_1, \dots, x_{2p})$.

Theorem 7: If $C_{2p}(x_1, \dots, x_{2p})$ is divisible by 2, it is divisible by 4.

Proof: One has that $x_j + x_{p+j}$ is of the same parity as $\pm(x_j - x_{p+j})$. Since the calculation of a determinant involves only addition, subtraction, and multiplication, this implies that $C_p(y_1, \dots, y_p)$ and $C_p(z_1, \dots, z_p)$ are both odd or are both even. Hence, their product $C_{2p}(x_1, \dots, x_{2p})$ is either odd or a multiple of 4.

We next turn to some particular results. Let

$$(3.2) \quad B(2p, r) = C_{2p}(x_1, \dots, x_{2p}) = C_p(y_1, \dots, y_p) \cdot C_p(z_1, \dots, z_p)$$

where $y_1 = 1 = y_{r+1}$, $y_2 = y_3 = \dots = y_r = 2$, $y_{r+2} = \dots = y_p = 0$, $z_1 = 1 = z_{r+1}$, $z_2 = \dots = z_r = z_{r+2} = \dots = z_p = 0$, and $x_{2j+1} = (y_{2j+1} + z_{2j+1})/2$, $x_{2j} = (y_{2j} - z_{2j})/2$

where the subscripts on the y 's and z 's are taken mod p . Note that since p is odd, $y_j = x_j + x_{p+j}$ and $z_j = (-1)^{(j-1)}(x_j - x_{p+j})$. Also, the x 's are integers since $y_j \equiv z_j \pmod{2}$. One has the following result.

Lemma 4: $B(2p, r) = 4r$ for $1 \leq r \leq p-1$.

$$\begin{aligned} \text{Proof: } C_p(y_1, \dots, y_p) &= \prod_{h=0}^{p-1} \left(1 + 2 \sum_{k=2}^r \exp[2\pi h(k-1)i/p] + \exp[2\pi hri/p] \right) \\ &= 2r \prod_{h=1}^{p-1} \left\{ \frac{(1 + 3\exp[2\pi hi/p])(1 - \exp[2\pi hri/p])}{(1 - \exp[2\pi hi/p])} \right\}. \end{aligned}$$

Now

$$(3.3) \quad C_p(1, 1, 0, 0, \dots, 0) = 2 = 2 \prod_{h=1}^{p-1} (1 + \exp[2\pi hi/p]).$$

Hence,

$$(3.4) \quad C_p(y_1, \dots, y_p) = 2r \prod_{h=1}^{p-1} \frac{1 - \exp[2\pi hri/p]}{1 - \exp[2\pi hi/p]} = 2A(p, r).$$

As $1 \leq r \leq p-1$, $\gcd(p, r) = 1$ so $A(p, r) = r$ and $C(y_1, \dots, y_p) = 2r$. Now

$$C_p(z_1, \dots, z_p) = \prod_{h=0}^{p-1} (1 + \exp[2\pi hri/p]).$$

But the p terms $1 + \exp[2\pi hri/p]$ are all different, as p and r are relatively prime. Hence, they equal the p terms $1 + \exp[2\pi hi/p]$ in the expansion of $C_p(1, 1, 0, 0, \dots, 0)$ and one has

$$(3.5) \quad C_p(z_1, \dots, z_p) = \prod_{h=0}^{p-1} (1 + \exp[2\pi hi/p]) = C_p(1, 1, 0, 0, \dots, 0) = 2.$$

Thus, $B(2p, r) = 2r \cdot 2 = 4r$.

By letting $B(2p, r, j)$ be the C_{2p} obtained from $B(2p, r)$ by increasing each x_k by j , one has the following.

Theorem 8: $B(2p, r, j) = 4r + 4pj$ for $1 \leq r \leq p-1$.

Proof: $B(2p, r, j) = 4r(2pj + 2r)/(2r) = 4r + 4pj$ by Theorem 1.

Lemma 5: When $x_1 = 1$, $x_2 = 0$, $x_3 = x_4 = \dots = x_{p+1} = 1$, $x_{p+2} = \dots = x_{2p} = 0$, one has $C_{2p}(x_1, \dots, x_{2p}) = p^2$.

$$\begin{aligned} \text{Proof: } C_{2p}(x_1, \dots, x_{2p}) &= C_p(2, 0, 1, 1, \dots, 1) \cdot C_p(0, 0, 1, -1, 1, \dots, -1, 1) \\ &= p^2 C_p(0, 0, 1, -1, 1, \dots, -1, 1) \end{aligned}$$

by Lemma 1. Letting $\theta = \exp(2\pi i/p)$ one has

$$\begin{aligned} (3.6) \quad C_p(0, 0, 1, -1, 1, \dots, -1, 1) &= 1 \cdot \prod_{h=1}^{p-1} (\theta^{2h} - \theta^{3h} + \theta^{4h} - \dots - \theta^{(p-2)h} + \theta^{(p-1)h}) \\ &= \prod_{h=1}^{p-1} \frac{(\theta^{2h} + \theta^{ph})}{(1 + \theta^h)} = \prod_{h=1}^{p-1} \frac{(1 + \theta^{2h})}{(1 + \theta^h)} \end{aligned}$$

$$= \frac{C_p(1, 0, 1, 0, 0, \dots, 0)/2}{C_p(1, 1, 0, 0, 0, \dots, 0)/2} = \frac{2/2}{2/2} = 1.$$

Thus, $C_{2p}(x_1, \dots, x_{2p}) = p^2$.

Theorem 9: When $x_1 = j + 1$, $x_2 = j$, $x_3 = x_4 = \dots = x_{p+1} = j + 1$, $x_{p+2} = \dots = x_{2p} = j$, one has $C_{2p}(x_1, \dots, x_{2p}) = (2j + 1)p^2$.

Proof: $C_{2p}(x_1, \dots, x_{2p}) = p^2(2pj + p)/p = (2j + 1)p^2$, by using Lemma 5 and Theorem 1.

Theorem 10: $V_{2p} = [\{m:p \nmid m\} \cup \{m:p^2 \mid m\}] \cap [\{m:2 \nmid m\} \cup \{m:4 \mid m\}]$.

Proof: By Theorems 6 and 7, no other values are possible. The only possible values are the integers not divisible by 2 or p [by using $A(2p, r, j)$ with $\gcd(2p, r) = 1$], the multiples of 4 that are not divisible by p (by using Theorem 8), the multiples of p^2 that are not divisible by 2 (by using Theorem 9), and the multiples of $4p^2$ (by using Theorem 3). Thus, V_{2p} consists of the integers m satisfying either $p \nmid m$ or $p^2 \mid m$ and also satisfying either $2 \nmid m$ or $4 \mid m$.

ACKNOWLEDGMENT

The author would like to thank Professor A. P. Hillman for suggesting the problem and for his continued interest.

REFERENCE

1. Roger Chalkley. "Circulant Matrices and Algebraic Equations." *Math. Magazine* 48, No. 2 (1975):73-80.

POWERS OF MATRICES AND RECURRENCE RELATIONS

WILLIAM H. CORNISH

Flinders University, Bedford Park, South Australia 5042

0. INTRODUCTION

This article arose out of the desire to demonstrate an interesting and perhaps initially surprising application of the theory of matrices to final year high school students. Thus, we consider a matrix-theoretic approach to firstly the solution of two simultaneous first-order recurrence relations and secondly to the solution of a single second-order recurrence relation, together with the proofs of a few identities.

It is well known that the solution of an m th order linear homogeneous recurrence relation can be found by means of the theory of matrices. Indeed, Rosenbaum [4] gave an approach which is based on the Jordan normal form; the reader should also see the recent article [5] of Ryavec. The technique used in Section 1 of this paper is based upon the Cayley-Hamilton theorem for 2×2 matrices and is particularly elementary. A novel feature of Section 2 is the use of 2×2 matrices to obtain generalizations of a few well-known identities which interrelate the Fibonacci and Lucas numbers.

1. POWERS OF 2×2 MATRICES

Let $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ be a 2×2 matrix whose entries are real, or even complex, numbers.

The characteristic polynomial of A is

$$\det(\lambda I - A) = \begin{vmatrix} \lambda - a_{11} & -a_{12} \\ -a_{21} & \lambda - a_{22} \end{vmatrix} = \lambda^2 - (a_{11} + a_{22})\lambda + (a_{11}a_{22} - a_{12}a_{21}).$$

It can be verified by direct computation that

$$A^2 - (a_{11} + a_{22})A + (a_{11}a_{22} - a_{12}a_{21})I = 0.$$

This is a special case of the famous Cayley-Hamilton theorem which says that if