Using Matrix In Solving Problems

Masum Billal

In this note, I have presented some examples of solving problems using matrix representation. This comes to the rescue often as a handy in olympiad problems frequently(specially in *Diophantine* equation), and contributes a much better and elegant solution. I have assumed that, matrix multiplication and other basic operations in matrix needed in this paper are known. We shall use the following known facts:

Theorem 1. *The product of the determinant of two matrix is the determinant of their product i.e.*

$$\det(\mathcal{AB}) = \det(\mathcal{A})\det(\mathcal{B})$$

Theorem 2. *If $\mathcal{A}$ is a square matrix, then*

$$\mathcal{A}^{m+n} = \mathcal{A}^m\mathcal{A}^n$$

Also, we assume

- *s.t.* stands for *such that.*
- $\det(A)$ is the determinant of a square matrix A.

1. Problems

Problem 1 (Fibonacci-Brahmagupta Identity)**.** The sum of two squares is $bi-square$. Prove that, the product of two bi-squares is a bi-square.

Solution. The following problem is rather a general one. So we prove the latter.

Problem 2. Prove that the product of two number of the form $x^2 + dy^2$ is of the same form for certain d.

Solution. Consider the matrix

$$\mathcal{M} = \begin{pmatrix} x & yd \\ -y & x \end{pmatrix}$$

and

$$\mathcal{N} = \begin{pmatrix} u & vd \\ -v & u \end{pmatrix}$$

s.t. $\det(\mathcal{M}) = x^2 + yd^2, \det(\mathcal{N}) = u^2 + dv^2$. Now, we multiply them.

$$\mathcal{M} \cdot \mathcal{N} = \begin{pmatrix} xu - dvy & dvx + duy \\ -(vx + uy) & xu - dvy \end{pmatrix}$$

Thus, $\det(\mathcal{M}\mathcal{N}) = (xu - dvy)^2 + d(vx + uy)^2$. Therefore,

$$(x^2 + dy^2)(u^2 + dv^2) = (xu - dvy)^2 + d(vx + uy)^2$$

which is of the same form.

Problem 3. Prove that the product of two numbers of the form $x^2 - dy^2$ is again of the same form.

Solution. This is same as before, only the matrix would be

$$\mathcal{M} = \begin{pmatrix} x & yd \\ y & x \end{pmatrix}$$

Problem 4. Prove that the following equation has infinite solution:

$$(a^2 + ab + b^2)(c^2 + cd + d^2) = (e^2 + ef + f^2)$$

for integers a, b, c, d, e, f.

Solution. The following identity gives an infinite family of solutions:

$$(x^2 + x + 1)(x^2 - x + 1) = x^4 + x^2 + 1$$

But we present a different solution using matrix. In fact, we can prove that, for any quartet (a, b, c, d) there are integers e, f s.t.

$$(a^2 + ab + b^2)(c^2 + cd + d^2) = (e^2 + ef + f^2)$$

Again, we need to choose a suitable matrix. We choose

$$\mathcal{A} = \begin{pmatrix} a & b \\ -b & a + b \end{pmatrix}$$

$$\mathcal{B} = \begin{pmatrix} c & d \\ -d & c + d \end{pmatrix}$$

Remark. We could do this factorizing $a^2 + ab + b^2$ as $(a + \zeta b)(a + \zeta^2 b)$ too with $\zeta^3 = 1$, third root of unity.

2. Proving Fibonacci Number Identities

We define general Fibonacci numbers by: $G_0 = a, G_1 = b$ and $G_n = pG_{n-1} + qG_{n-2}$ for $n > 1$. Then using matrix,

$$\begin{pmatrix} p & q \\ 1 & 0 \end{pmatrix} \begin{pmatrix} G_n & G_{n-1} \\ G_{n-1} & G_{n-2} \end{pmatrix} = \begin{pmatrix} G_{n+1} & G_n \\ G_n & G_{n-1} \end{pmatrix}$$

Special cases are:

1. Fibonacci numbers: $a = 0, b = p = q = 1$, n^{th} number denoted by F_n.
2. Lucas numbers: $a = 2, b = p = q = 1$, n^{th} number denoted by L_n.

THEOREM 3.

$$\begin{pmatrix} p & q \\ 1 & 0 \end{pmatrix}^{n-1} \begin{pmatrix} G_2 & G_1 \\ G_1 & G_0 \end{pmatrix} = \begin{pmatrix} G_{n+1} & G_n \\ G_n & G_{n-1} \end{pmatrix} \tag{2.1}$$

Corollary 2.1.1.

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n} = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$

Proof. We can use induction. It's rather straight-forward. □

THEOREM 4.

$$G_{n+1}G_{n-1} - G_n^2 = (-1)^{n-1}q^{n-1}\left(a^2p + abq - b^2\right)$$

Proof. Take determinant in equation 2.1. □

Corollary 2.1.2.

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n$$

Corollary 2.1.3.

$$L_{n+1}L_{n-1} - L_n^2 = 5 \cdot (-1)^{n-1}$$

Problem 5. Prove that,

$$F_{m+n+1} = F_{m+1}F_{n+1} + F_mF_n \tag{2.2}$$

Solution. Consider $I = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Then, $I^{m+n} = I^mI^n$.

$$\begin{aligned} I^m &= \begin{pmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{pmatrix} \\ I^n &= \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} \\ I^{m+n} &= \begin{pmatrix} F_{m+n+1} & F_{m+n} \\ F_{m+n} & F_{m+n-1} \end{pmatrix} \end{aligned}$$

$$\begin{pmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{pmatrix} \cdot \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} = \begin{pmatrix} F_{m+1}F_{n+1} + F_mF_n & F_{m+1}F_n + F_mF_{n-1} \\ F_mF_{n+1} + F_{m-1}F_n & F_mF_n + F_{m-1}F_{n-1} \end{pmatrix}$$

Therefore,

$$\begin{pmatrix} F_{m+1}F_{n+1} + F_mF_n & F_{m+1}F_n + F_mF_{n-1} \\ F_mF_{n+1} + F_{m-1}F_n & F_mF_n + F_{m-1}F_{n-1} \end{pmatrix} = \begin{pmatrix} F_{m+n+1} & F_{m+n} \\ F_{m+n} & F_{m+n-1} \end{pmatrix}$$

Equating the cell-values of them, we get

$$F_{m+n+1} = F_{m+1}F_{n+1} + F_mF_n$$

Corollary 2.2.1.

$$F_{mk+n} = F_{mk+1}F_n + F_{mk}F_{n-1}$$

Corollary 2.2.2. Setting $m = n$,

$$F_{2n+1} = F_n^2 + F_{n+1}^2$$

We end here. But it's obvious that we can derive so many more similar identities using the same approach.