Equational Sudoku: Solution

First, we want to figure out which of $0, 1, \star, ☾$ that $\star \times ☾$ is. We will set it equal to elements and multiply by $\star^{-1}$ or $☾^{-1}$ to get contradictions:

- $\star \times ☾ = 0 \quad \Rightarrow \quad \star, ☾ = 0$
- $\star \times ☾ = \star \quad \Rightarrow \quad ☾ = 1$
- $\star \times ☾ = ☾ \quad \Rightarrow \quad \star = 1$

These are all contradictions because $0, 1, \star, ☾$ are all distinct. This leaves the only possibility $\star \times ☾ = 1$, which also means $☾ \times \star = 1$. In other words, $\star$ and $☾$ are each other's multiplicative inverses, $\star^{-1} = ☾$ and $☾^{-1} = \star$.

Second, we do the same for $\star \times \star$, multiplying by $\star^{-1} = ☾$:

- $\star \times \star = 0 \quad \Rightarrow \quad \star = 0$
- $\star \times \star = 1 \quad \Rightarrow \quad \star = ☾$
- $\star \times \star = \star \quad \Rightarrow \quad \star = 1$

This leaves only $\star \times \star = ☾$. Symmetrically, we must also have $☾ \times ☾ = \star$.

Third, we may do the same for $1 + \star$:

- $1 + \star = 1 \quad \Rightarrow \quad \star = 0 \quad$ (add -1)
- $1 + \star = \star \quad \Rightarrow \quad 1 = 0 \quad$ (add $-\star$)
- $1 + \star = 0 \quad \Rightarrow \quad \star = ☾$

From $1+\star = 0$ we may multiply by $☾$ to get $☾ + 1 = 0$. Setting $1+\star = ☾ + 1$, we may add -1 to get $\star = ☾$, a contradiction. This leaves only $1 + \star = ☾$, and symmetrically $1 + ☾ = \star$. Not much left to go!

Multiplying $1 + \star = ☾$ by $\star$ (or $1 + ☾ = \star$ by $☾$) gives $\star + ☾ = 1$.

Lastly, multiplying the element $\bigcirc := 1 + \star + \leftmoon$ by either of $\star$ or $\leftmoon$ leaves it unchanged - thus, we have $(1-\star)\bigcirc = (1-\leftmoon)\bigcirc = 0$, and multiplying by $(1-\star)^{-1}$ or $(1-\leftmoon)^{-1}$ (which is possible because $\star, \leftmoon, 1$ are distinct) yields $\bigcirc = 0$. Replacing $\star + \leftmoon$ in $\bigcirc = 0$ with 1, this equation is now $1 + 1 = 0$.

Our completed table now reads

$+$	0	1	$\star$	$\leftmoon$
0	0	1	$\star$	$\leftmoon$
1	1	0	$\leftmoon$	$\star$
$\star$	$\star$	$\leftmoon$	0	1
$\leftmoon$	$\leftmoon$	$\star$	1	0

$\times$	0	1	$\star$	$\leftmoon$
0	0	0	0	0
1	0	1	$\star$	$\leftmoon$
$\star$	0	$\star$	$\leftmoon$	1
$\leftmoon$	0	$\leftmoon$	1	$\star$

What this problem called a "number system" in math is known as a *field*, and when it has a finite number of elements it is a **finite field**.

For comparison, consider the **integers mod** n, denoted $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$. This effectively consists of $\{0, 1 \cdots, n-1\}$ with "clock arithmetic," where the addition and multiplication operations "wrap around," for instance $11+2 = 1$ in $\mathbb{Z}_{12}$ just as 2 hours after 11:00 is 1:00. If n is composite, then $\mathbb{Z}_n$ has nonzero elements without multiplicative inverses (anything not relatively prime to n), but if p is prime then $\mathbb{Z}_p$ is a finite field.

There is essentially only one finite field of size q for prime powers q, and none for other cardinalities, denoted $\mathbb{F}_q$ in math or $GF(q)$ in computer science ("Galois field"). For primes p, the finite field $\mathbb{F}_p$ is just $\mathbb{Z}_p$. But for higher prime powers q, we construct $\mathbb{F}_q$ by adding "imaginary" elements to $\mathbb{F}_p$ just as how we construct $\mathbb{C}$ from $\mathbb{R}$. For instance, we may construct $\mathbb{F}_4$ from the problem by adjoining a cube root of unity $\leftmoon$ to $\mathbb{F}_2 = \{0, 1\}$.

Finite fields are indispensable to modern cryptography and error correction.