Modular Arithmetic

Recall: when working with our doomsday algorithm, we wrote things like $4+22=5$ (because 22 days after a Thursday is a Friday) and $4-10=1$ (because 10 days before a Thursday is a Monday). As written, these equations look a little silly, because they're literally false. So we invent notation to express the above sentiment: we'll write

$$4+22\equiv 5 \pmod 7 \qquad \text{and} \qquad 4-10\equiv 1 \pmod 7.$$

Formally we can define this as follows: we say

$$a\equiv b \pmod 7$$

(read "a is congruent to b modulo 7") if and only if $7 \mid b-a$. More generally, we say $a\equiv b \pmod n$ if and only if $n \mid b-a$. Using this, we can do addition, subtraction, and multiplication modulo n. For example:

$$3\cdot 5\equiv 1 (\text{mod } 7) \qquad \text{and} \qquad \tfrac{1}{3}\equiv 5 \pmod 7.$$

There are a couple different ways to think about the latter example. One approach: note that $1\equiv 15 \pmod 7$, whence

$$\frac{1}{3}\equiv\frac{15}{3}\equiv 5 \pmod 7.$$

We can also change the denominator, e.g.

$$\frac{1}{3}\equiv\frac{8}{-4}\equiv -2\equiv 5 \pmod 7.$$

Yet another way to think of this is that $1/3$ is the number with the property that when multiplied by 3 yields 1; in other words, it's the solution to $3x\equiv 1 \pmod 7$. Since $3\cdot 5\equiv 1 \pmod 7$, we see that $x\equiv 5 \pmod 7$ is a solution.

Notice that we can't divide by any number. For instance, $\frac{1}{7}$ is undefined (mod 7), since $7x\equiv 0 \pmod 7$ for every x.

To build our intuition, we construct a (mod 7) multiplication table; see below. From the table we make a few observations:
1) Rows n and $7-n$ are reversed order
2) All diagonals are symmetric
3) No number appears twice in any row or column (a.k.a. the Sudoku rule)

Also notice that

$$2\equiv 5\cdot 6 (\text{mod } 7) \implies \tfrac{2}{5}\equiv 6 (\text{mod } 7).$$

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Also, $\sqrt{2} \equiv 3$ or $4 \pmod 7$. We can make this look nicer by observing that $4 \equiv -3 \pmod 7$, so really $\sqrt{2} \equiv \pm 3 \pmod 7$. Similarly, $\sqrt{-3} \equiv \pm 2 \equiv 2, 5 \pmod 7$.

Next, for comparison, we construct a multiplication table modulo 6. Since the zero row and column are trivial, we omit them from the table.

×	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

From this we can make further observations:
1) The sudoku rule only holds in the 1st and 5th rows/columns.
2) Division breaks in some cases. For example,
- 2/3 is undefined: there's no multiple of 3 that produces $2 \pmod 6$;
- 3/3 is not well-defined: there are several possible answers to what 3/3 might be!

To make our 'Sudoku Rule' more rigorous, we prove the following proposition.

Proposition: If $an \equiv bn \pmod 7$ then $a \equiv b \pmod 7$ or $n \equiv 0 \pmod 7$.
Proof: Suppose that $an \equiv bn \pmod 7$. By definition, this means that $7 \mid (b-a)n$, and since 7 is prime we have either $7 \mid b-a$ or $7 \mid n$. By definition again, these are $a \equiv b \pmod 7$ and $n \equiv 0 \pmod 7$ respectively. □

Notice that the only property of 7 that we needed was that it was prime. Thus we can generalize:

Proposition 2.0: For any prime p, if $an \equiv bn \pmod p$, then $a \equiv b \pmod p$ or $n \equiv 0 \pmod p$.

Even more generally:

<u>Proposition 3.0:</u> For any $m \geq 2$, if $an \equiv bn \pmod{m}$ and $\gcd(n,m) = 1$ then $a \equiv b \pmod{m}$.
<u>Proof:</u> Suppose $an \equiv bn \pmod{m}$ and $\gcd(n,m) = 1$. Then $m \mid (a-b)n$, and since $\gcd(n,m) = 1$ we deduce $m \mid b-a$, or in other words, $a \equiv b \pmod{m}$. □

What does any of this have to do with the sudoku rule? Well, consider the contrapositive: if a and b are distinct $\pmod{m}$, then an and bn are also distinct $\pmod{m}$ so long as $(m,n) = 1$.

Let's return to the multiplication table modulo 7. Consider the 4th row of that table:

$$4, 1, 5, 2, 6, 3.$$

But of course, each of these is a multiple of 4 modulo 7:

$$4 \cdot 1, 4 \cdot 2, 4 \cdot 3, 4 \cdot 4, 4 \cdot 5, 4 \cdot 6.$$

Multiplying these all together, we deduce that

$$4 \cdot 1 \cdot 5 \cdot 2 \cdot 6 \cdot 3 \equiv (4 \cdot 1)(4 \cdot 2)(4 \cdot 3)(4 \cdot 4)(4 \cdot 5)(4 \cdot 6) \pmod{7}.$$

This simplifies to

$$6! \equiv 4^6 \cdot 6! \pmod{7}.$$

Since $\gcd(6!, 7) = 1$, our Proposition 3.0 yields $4^6 \equiv 1 \pmod{7}$. This is an example of Fermat's Little Theorem:

<u>Proposition:</u> For and $a \not\equiv 0 \pmod{7}$, $a^6 \equiv 1 \pmod{7}$.
<u>Proof:</u> Same as before: multiply all the elements in the ath row of the table and interpret in two different ways.

Once again, 7 isn't all that special – we could do this for any prime.

<u>Fermat's Little Theorem:</u> For any $a \not\equiv 0 \pmod{p}$ for a prime p, $a^{p-1} \equiv 1 \pmod{p}$.
<u>Proof:</u> By the sudoku rule, we know that the ath row of the multiplication table $\pmod{p}$ contains $p-1$ distinct numbers. However, since 0 definitely can't be in the row and there are precisely $p-1$ distinct numbers left $\pmod{p}$, we see that the ath row is simply a permutation of the numbers $1, 2, 3, \cdots, p-1$. Thus

$$(p-1)! = \prod_{n=1}^{p-1} n \equiv \prod_{n=1}^{p-1} (an) \equiv a^{p-1}(p-1)! \pmod{p}$$

whence $a^{p-1} \equiv 1 \pmod{p}$. □