Counting on Clocks
–A Math Circle by Michael Griffin

Number theory is the study of the whole numbers. Numbers like \(-2, -1, 0, 1, 2, \ldots\). The whole numbers have some beautiful properties, deep structure, and, sometimes, really bizarre behavior. The first door into number theory is modular arithmetic. You probably learned ordinary arithmetic a long time ago—addition, subtraction, multiplication, long division and fractions... a little later maybe you learned exponents and algebra. That’s the boring kind of arithmetic, stuck on a number line. Don’t get me wrong, it’s very important and beautiful in its own right, but it can also be the jumping-off point into some much more interesting mathematics.

Let me give you some examples of problems that are easy to state with ordinary arithmetic, but not easy to solve:

1. You have a machine working on a job that takes 10,000 hours to finish. You started the job at Midnight, and what to know what time of day it will be when the job finally finishes.

2. What is the digit in the ones place of the number 3157914328178324987?

3. The number $2^{29}$ has nine digits, none of which repeat. Without a calculator, find which digit is missing.

Like I said before, the arithmetic you are used to doing is on a number line. These kinds of problems are better suited to a kind of arithmetic on a circle, like a clock. The clock doesn’t care what day it is. It doesn’t know the difference between times twelve hours apart. 10 o’clock + 5 hours = 3 o’clock. Which is really the same as 15 o’clock or 27 o’clock. All that matters is the remainder after you divided by 12. That first problem? If we do a bit of long division, we get $10,000 = 12 \cdot 833 + 4$. The clock goes around 833 times, but we don’t care about that. All we care about is the 4. It will be 4 o’clock when the machine finishes. We write this like

$$10,000 \equiv 4 \pmod{12}.$$  

The “(mod 12)” means we are looking at a clock with 12 numbers on it. The 12 here is called the modulus. If we wanted to see whether this was 4 A.M. or 4 P.M., we would have to use a clock with 24 hours on it (i.e. (mod 24)). For other problems we might want a clock with 7 numbers on it, or 67 numbers.

If $a$ and $b$ are integers, then the statement $a \equiv b \pmod{12}$ means $a - b$ is divisible by 12, or in other words $a = b + 12 \cdot n$ for some integer $n$. It also means that $a + 12 \cdot m \equiv b \pmod{12}$ for any integer $m$. 

1
Exercise 1. Fill in the following addition table (mod 7).

<table>
<thead>
<tr>
<th>+</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Subtraction is the same idea. Something to think about—negative numbers make sense in modular arithmetic, same as positive numbers. Can you ever have \(-x \equiv x \pmod{M}\)?

Addition on clocks is not too strange. But what about multiplication? Can you multiply on clocks? What would this mean? What I want to be able to say is that if \(a' \equiv a \pmod{M}\) and \(b' \equiv b \pmod{M}\), then \(a' \cdot b' \equiv a \cdot b \pmod{M}\). But \(a' = a + M \cdot n\) for some \(n\), and \(b' = b + M \cdot m\) for some \(m\), so \(a' \cdot b' = (M \cdot n \cdot m + m + n) \cdot M + a \cdot b\). So the answer is yes! \(a' \cdot b' \equiv a \cdot b \pmod{M}\), so modular multiplication makes sense!

Exercise 2. Fill in the following multiplication tables (mod 7) and (mod 12).

\[
\begin{array}{cccccccc}
\times & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\
1 & 1 & & & & & & & & & & \\
2 & & & & & & & & & & & \\
3 & & & & & & & & & & & \\
4 & & & & & & & & & & & \\
5 & & & & & & & & & & & \\
6 & & & & & & & & & & & \\
\end{array}
\]
We can also do algebra with modular arithmetic.

**Exercise 3.** Find all the solutions for the following expressions (mod 7) and (mod 12)

1. \(5x + 3 \equiv 2\)
2. \(4x - 2 \equiv 6\)
3. \(3x + 2 \equiv 1\)
4. \(x^2 - 4 \equiv 0\)

Solving equations like these are why we like division. Division in modular arithmetic is a little different than in usual arithmetic. Instead of fractions \(1/x\), we write \(x^{-1}\) to mean the number so that \(x \cdot x^{-1} \equiv 1 \pmod{M}\). But notice \(x^{-1}\) doesn’t always exist. For instance \(3^{-1}\) and \(4^{-1}\) (mod 12) do not exist, which makes one of those equations in the exercise above impossible, and another has more answers than you might expect. This is because 3 and 4 each share a factor with 12. In fact, \(3 \cdot 4 \equiv 12 \equiv 0 \pmod{12}\), which is the source of the problem. Weird things happen when you can multiply two non-zero numbers together and get zero. We can avoid this problem by staying away from numbers that share a factor with the modulus. If our modulus is prime, that makes things easy.