Before we can talk about RSA, we need to equip some more necessary math tools.

In Core Module 3: Math Tools (https://canvas.duke.edu/courses/24695/modules/14410) and Exam 1 we have seen plenty of use of modulo reduction rules such as 
\[(a \times b) \mod k = ((a \mod k) \times (b \mod k)) \mod k.\] However, that does not help us when we wish to compute the exponentiation of a number modulo another. For a concrete example, how do we compute \(5^{230} \mod 7\)? Do we just invoke the multiplication rule above for a total of 229 times?

There is a better approach than that. Recall the following result from the CM5 Recitation:

**Theorem.** Every positive integer \(n\), can be written as a sum of distinct nonnegative integer powers of 2.

This is equivalent to finding the binary representation of \(n\). For \(n = 230\), its binary representation is \(230 = 128 + 64 + 32 + 4 + 2 = 2^7 + 2^6 + 2^5 + 2^2 + 2^1\). We can also write it as 
\((230)_{10} = (11100110)_{2}\), where the subscripts represent the former is base 10 and the latter is base 2.

**How does this help?** Now we can write \(5^{230}\) as \(5^{128} \times 5^{64} \times 5^{32} \times 5^4 \times 5^2\) and carry out our calculations in a lot fewer steps:

\[
\begin{align*}
5^2 &= 25 \equiv 4 \pmod{7} \\
5^4 &= 5^2 \times 5^2 \equiv 4 \times 4 \pmod{7} = 16 \equiv 2 \pmod{7} \\
5^8 &= 5^4 \times 5^4 \equiv 2 \times 2 \pmod{7} = 4 \pmod{7} \\
5^{16} &= 5^8 \times 5^8 \equiv 4 \times 4 \pmod{7} = 16 \equiv 2 \pmod{7} \\
5^{32} &= 5^{16} \times 5^{16} \equiv 2 \times 2 \pmod{7} = 4 \pmod{7}
\end{align*}
\]

Does the pattern feel familiar? Well, the Exam 1 question was there for a reason. Looking at this pattern, surely we have \(5^{64} \equiv 2 \pmod{7}\) and \(5^{128} \equiv 4 \pmod{7}\). Putting this altogether, we have:

\[
\begin{align*}
5^{230} &= 5^{128} \times 5^{64} \times 5^{32} \times 5^4 \times 5^2 \\
&\equiv 4 \times 2 \times 4 \times 2 \times 4 \pmod{7} \\
&= 8 \times 8 \times 4 \pmod{7} \\
&\equiv 1 \times 1 \times 4 \pmod{7} \\
&= 4 \pmod{7}
\end{align*}
\]

So \(5^{230} \equiv 4 \pmod{7}\).
Remark. Had the task been calculating $19^{230} \mod 7$, we would have first taken $19 \equiv 5 \pmod{7}$ and calculate $5^{230} \mod 7$ instead.

Practice this trick in the next practice question.