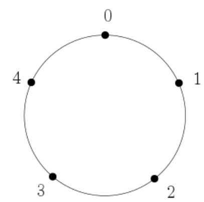
Modular Arithmetic

Think about how a clock works. Instead of the numbers going up forever, we "reset" every 12 (or 24) hours. This is essentially the idea in modular arithmetic. If we're counting "mod 5," we would say $0, 1, 2, 3, 4, 0, 1, 2, 3, 4, \ldots$ and "wrap around" every 5. Instead of a number line for this kind of counting, we have a circle, like a clock.



Doing arithmetic "mod 5" works like normal, except you have to figure out where you'd wrap around to with this special counting. For example, $2 \times 3 = 6 \equiv 1 \mod 5$. (We use the special $\equiv$ symbol to denote that we're doing this special modular arithmetic, not the usual arithmetic with integers.) As another example, $2 - 4 = -2 \equiv 3 \mod 5$.

P1. Make an addition and multiplication table for mod 3, mod 4, mod 5, mod 6, mod 7, and mod 10 arithmetic. What patterns do you notice? (By the way, can you explain how to figure out what a number is mod 10 very quickly? What is 4982017489352762 mod 10?)

P2. Can you find a number that you might consider $\frac{1}{2}$ mod 3, 4, 5, 6, 7, or 10? How about $\sqrt{-1}$? (What is -1 mod 3, 4, 5, 6, 7, and 10, anyway?)

P3. Look at the perfect squares $1, 4, 9, 16, \ldots$. What are these numbers mod 10? What about the perfect cubes, fourth powers, or fifth powers? What are these mod 10?

Powers

P4. Take powers of 3 mod 10 until you see a pattern. ($3^1 \equiv ? \mod 10,\ 3^2 \equiv ? \mod 10, \ldots$) What is the pattern? Can you predict what 3^{107} will be mod 10?

P5. Give a general statement: Can you predict what 3^n is mod 10?

P6. Repeat P4 and P5, but mod 100. What is $3^{107} \mod 100$? Can you state a general rule for what 3^n is mod 100?

P7. Repeat P4 and P5, but mod 20. What is $3^{107} \mod 20$? Can you state a general rule for what 3^n is mod 20?