Counting Backwards (Modular Arithmetic, Take 3)

Although **PwP** only counts using positive numbers (for jumps, or points, for example), it is sometimes worthwhile to consider the negative counterpart of that positive counting process. In Files 1 and 2, for example, *a number of the most interesting images occur when one number is just under or just over a multiple of another number* (see, for example, Stars as rotating polygons in File 1 or Porcupine Polygons in File 2).

This material is discussed in a bit more abstract fashion than in the introductory MOD explainer so do not worry if some of this sounds more abstract as well. We also reexamine the notions of *congruence* and *residue class* introduced in the second MOD explainer in order to add additional detail to these concepts.

In this explainer, we use ***m*** as the modulus (or denominator), and we restrict ourselves to ***m*** > 0. We use ***m*** rather than ***n*** because sometimes we will want to have denominators other than ***n*** (like ***S***, ***n*·*S***, or something else).

Claim: There are ***m*** possible modular outcomes MOD ***m*** since the only possible remainders are 0, 1, …, ***m***-1.

This means that we can categorize ALL numbers according to their remainder. Suppose we want to describe all numbers with remainder ***r*** upon division by ***m***, $0 \le r < m$. This is easy to describe. Consider the set of numbers:

$$\ldots, r - 3\cdot m, r - 2\cdot m, r - 1\cdot m, r - 0\cdot m, r + 1\cdot m, r + 2\cdot m, r + 3\cdot m, \ldots .$$

This can be more compactly described as the set of numbers of the form: $r + x\cdot m$ where ***x*** is the set of integers. Each of these number has the same remainder upon division by ***m***. One can describe these numbers as being in the same *residue class* MOD ***m***. If two numbers ***a*** and ***b*** are in the same residue class, their difference is divisible by ***m***. As noted in the second MOD explainer, we say that ***a*** and ***b*** are *congruent modulo* ***m***, $a \equiv b \pmod{m}$ if ***a*** MOD ***m*** = ***b*** MOD ***m***.

Examples: **A)** …, -47, -30, -13, 4, 21, 38, 55, … **B)** …, -47, -27, -7, 13, 33, 53, 73, … **C**) …, -57, -38, -19, 0, 19, 38, 57, …

Answer *i.* and *ii.* for **A**, **B**, and **C**: *i. What is modulo for each set of numbers? ii. What is the remainder in each case?*

Answer two final questions: *iii. Describe what you would need to do to each set of numbers if you wanted to obtain the next higher remainder for that set of numbers? iv. How about the next lower remainder?*

Questions *iii.* and *iv.* were asked in order to make three points.

(1) Each set of numbers (residue class) is just one larger or one less than the original set of numbers. Note that we could ask question *iii.* ***m*** times. After that, we would return to the original residue class of numbers.

(2) One less than remainder 0 is remainder ***m***-1 (as noted in the move from **C** to **C_**). The other side of this coin is that one more than ***m***-1 is 0, MOD ***m*** (as noted in the move from **C_** to **C**).

(3) Although **PwP** only counts using positive numbers (for jumps, or points, etc.), it is sometimes worthwhile to consider the negative counterpart.

Positive and negative *a*. If ***r*** = ***a*** MOD ***m***, then -***r*** = -***a*** MOD ***m*** because of the *multiplication by a constant rule* (the constant here is -1). If ***r*** = 0, ***a*** and -***a*** are both divisible by ***m*** and if ***r*** > 0, 0 < ***r*** < ***m*** implies 0 > -***r*** > -***m*** (because multiplying by a negative number changes the direction of the inequality). Adding ***m*** to each term does not change the direction of each inequality so ***m***+0 > ***m***-***r*** > ***m***-***m*** = 0. Reorganizing yields: 0 < ***m***-***r*** < ***m*** so that if ***r*** = ***a*** MOD ***m***, then ***m***-***r*** = -***a*** MOD ***m***.

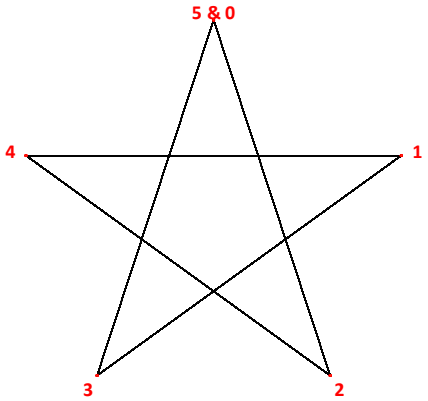
Answers. *i.* and *ii.* The modulus, ***m***, is the difference between successive numbers and the remainder is the first non-negative value in each set of numbers. This will necessarily be a number between 0 and ***m***-1. Given this:

A) Modulo m_A = 17, remainder is 4. **B)** Modulo m_B = 20, remainder is 13. **C)** Modulo m_C = 19, remainder is 0.

iii. Next higher: **A$^+$)** …, -46, -29, -12, **5**, 22, 39, 56, … **B$^+$)** …, -46, -26, -6, **14**, 34, 54, 74, … **C$^+$)** …, -56, -37, -18, **1**, 20, 39, 58, …

iv. Next lower: **A_)** …, -48, -31, -14, **3**, 20, 37, 54, … **B_)** …, -48, -28, -8, **12**, 32, 52, 72, … **C_)** …, -58, -39, -20, -1, **18**, 37, 56, …

These examples amplify the third point and show how images can be *conceptualized* as being *counterclockwise-drawn* by simply counting backwards. We start with a quick discussion of MOD 5.



MOD 5 is even easier than MOD 12. Because we have five fingers and our number system is base 10, it is easy to see the remainder for any number, positive or negative, MOD 5.

Positive values: Consider the number 27. Because 10 is a multiple of 5 we can ignore all but the ones digit (7) of any number MOD 5. But 7 = 5 + 2 (five fingers on one hand and the last two on the other), so 2 = 27 MOD 5.

Negative values: Consider the number -27. As above we can ignore all but the ones digit, but what does -7 signify? The first thing to note is that -7 is the same as -2 MOD 5 because of the -2 = -7 + 5. Applying this a second time (3 = -2 + 5) shows that 3 = -27 MOD 5. This can also be seen by noting that -27 = 3 - 6·5, or to put it in the terms used above, -27 is part of the residue class …, -12, -7, -2, **3**, 8, 13, 18, … so that in fact, 3 = -27 MOD 5.

It is worth explicitly pointing out that this example reminds us that the mod of a negative number is NOT the same as the MOD of its absolute value counterpart. Indeed, as noted above: if ***a*** > 0 and ***r*** = ***a*** MOD ***m***, then ***m-r*** = -***a*** MOD ***m***.

How Pentagons and Pentagrams are Drawn. The table below shows the possible outcomes from File 1 given ***n*** = 5. For a given value of ***J***, one of five things must happen because there are 5 possible remainders. These outcomes are listed in the Resulting Image column. There is no image (or more accurately, there is a single point) if ***J*** is a multiple of ***n*** = 5 (which is the remainder = 0 row). Two remainders produce a pentagon, and two produce a pentagram.

Remainder	Possible Jump Values*	Vertex Jump Pattern	Resulting Image (and how it is actually drawn)	Appears as if drawn as
0	… -5 0 5 10 15 …	0, 0, …	A single point, the top vertex alone	-
1	… -4 1 6 11 16 …	0, 1, 2, 3, 4, 0, …	Pentagon drawn clockwise each vertex connected to next	clockwise, J = 1
2	… -3 2 7 12 17 …	0, 2, 4, 1, 3, 0, …	Pentagram drawn clockwise every 2nd vertex connected	clockwise, J = 2
3	… -2 3 8 13 18 …	0, 3, 1, 4, 2, 0, …	Pentagram drawn clockwise every 3rd vertex connected	counterclockwise, J = -2
4	… -1 4 9 14 19 …	0, 4, 3, 2, 1, 0, …	Pentagon drawn clockwise every 4th vertex connected	counterclockwise, J = -1

*Jump values are positive in PwP.

Consider first the remainder 1 pentagon. It is drawn as 5 segments in a 1-time-around fashion if ***J*** = 1. But exactly the same clockwise-drawn pentagon is created in a 6-times-around fashion if ***J*** = 6. (The first line is drawn after going around once and ending 1 vertex past the top, 6 = 1 + 1·5, the second goes around a second time and ends at vertex 2, 12 = 2 + 2·5, and so on until the fifth line ends at vertex 0, 30 = 0 + 6·5.) Had ***J*** = 11, then the image is still a clockwise-drawn pentagon created by counting 11-times-around (since 11·5 = 55 which represents 11 clockwise counts around the 5 vertices).

Consider next the remainder 4 pentagon. It is drawn as 5 segments in a 4-times-around fashion if ***J*** = 4. Exactly the same clockwise-drawn pentagon is created as a 9 times around fashion if ***J*** = 9. However, notice that it could be *conceptualized* as counting backwards (***J*** = -1, counterclockwise) 1 vertex at a time as a 1-time around *counterclockwise-drawn* image.

*The **J** = 2 and **J** = 3 pentagrams follow the same patterns.* The ***J*** = 2 pentagram is drawn as a 2-times-around clockwise-drawn image. The ***J*** = 3 pentagram is drawn as a 3-times-around clockwise-drawn image, but you could conceptualize this image as a 2-times-around *counterclockwise-drawn* image (***J*** = -2).

Note: We can conceptualize a *just-under-a-multiple* as a -1 and a *just-over-a-multiple* as a +1 in modular terms.

A more general rule. If all you care about is the final image, it makes sense to count in whichever direction creates the least total counting. This is why we restrict ***J*** to ***J*** < ***n***. However, note that many **PwP** files exhibit vertical symmetry. In this instance, the same image will result for ***J*** and ***n-J*** so one can simply ask which is smaller, ***J*** and ***n-J***? Put another way, in this instance, we can restrict ourselves to ***J*** < ***n***/2 and count vertices in a clockwise fashion around the polygon.