MMI and Negative MMI (nMMI)

Background. In arithmetic, the multiplicative inverse of a number $x \neq 0$ is a number that, when multiplied by x is equal to 1. The multiplicative inverse of x is $1/x$ or x^{-1}. For example, the multiplicative inverse of 3 is 1/3 because $3 \cdot (1/3) = 1$. Note in particular that if the number is an integer (other than 1 or -1) the multiplicative inverse is NOT an integer but is instead a fraction. In modular arithmetic, the product of two integers can be 1 larger than a multiple of a third. This is the essence of modular multiplicative inverse.

Definition. When numbers a, b, and m have the property that $a \cdot b = b \cdot a$ is one larger than a multiple of m we say that a *and* b *are modular multiplicative inverses modulo* m (a and b are MMI MOD m if $1 = a \cdot b$ MOD m).

Facts about MMI.

Existence.	If b and m are coprime, then there exists a number a such that a and b are MMI MOD m.
Special values.	The MMI of 1 is 1 MOD m for all m. The MMI of m-1 is m-1 MOD m for all m.
Excluded values.	If b is not coprime to m, then it is not possible to find an a such that $1 = a \cdot b$ MOD m. In particular, there is no MMI for 0 MOD m.
Examples. $m = 5$	Since 5 is prime, b and m are coprime for b = 1, 2, 3, 4, it is possible to find the MMI for each value of b. Since order does not matter, the three (a, b) MMI pairs are: (1, 1), (2, 3), and (4, 4).
$m = 12$	b = 1, 5, 7, 11 are coprime to m. Here the (a, b) MMI pairs are: (1, 1), (5, 5), (7, 7) and (11, 11).

We have only discussed MMI for a and b smaller than m. But a and b are only the smallest positive number examples of two numbers which are in an MMI MOD m. Note that *the residue class of* a, defined as the set of numbers $x_a = a + k \cdot m$ for integer values of k once multiplied by b is also 1 more than a multiple of m. This is easy to see:

Assume $1 = a \cdot b$ MOD m. Consider $x_a \cdot b = (a + k \cdot m) \cdot b = a \cdot b + k \cdot m \cdot b$. This has the same product, MOD m, as $a \cdot b$.
The same argument can be made for the residue class b, $x_b = b + j \cdot m$ for integer values of j.

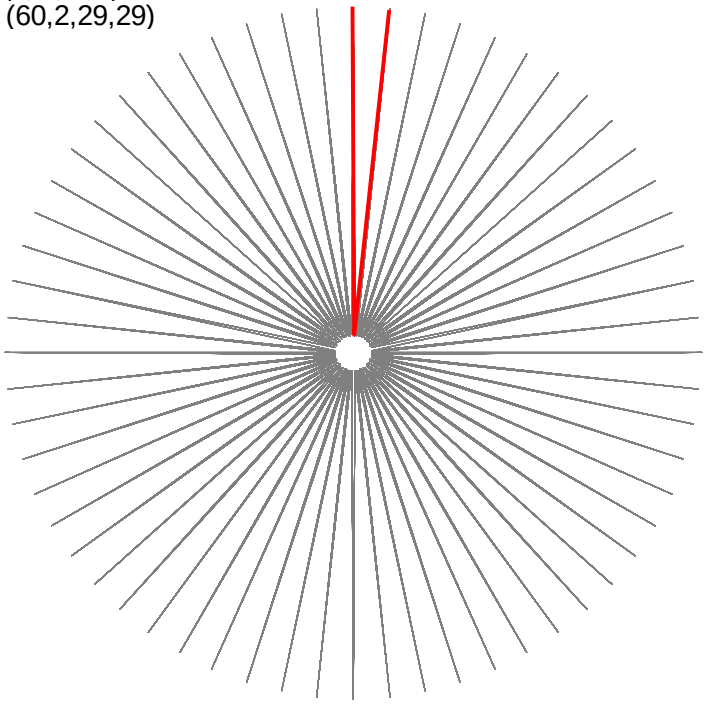
Extended values. If $1 = a \cdot b$ MOD m, then $1 = x_a \cdot x_b$ MOD m for $x_a = a + k \cdot m$ and $x_b = b + j \cdot m$ for all integers k and j.

Examples. Since 2 is MMI of 3 MOD 5, we know that $1 = 17 \cdot 48$ MOD 5 because $17 = 2 + 3 \cdot 5$ and $48 = 3 + 9 \cdot 5$.

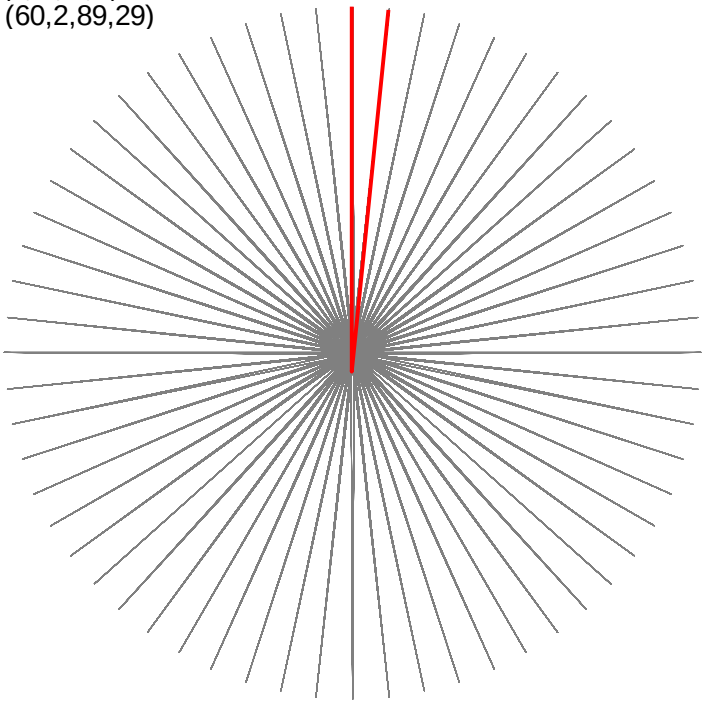
Since 5 is MMI of 5 MOD 12, we know that $1 = 17 \cdot 65$ MOD 12 because $17 = 5 + 1 \cdot 12$ and $65 = 5 + 5 \cdot 12$.

Left Image Both are *60-second images* (click *Toggle Drawing*) because $1 = 29 \cdot 29 = 89 \cdot 29 = P \cdot J$ (MOD 60). Right Image

(n, S, P, J)
(60,2,29,29)
120 lines



(n, S, P, J)
(60,2,89,29)
120 lines

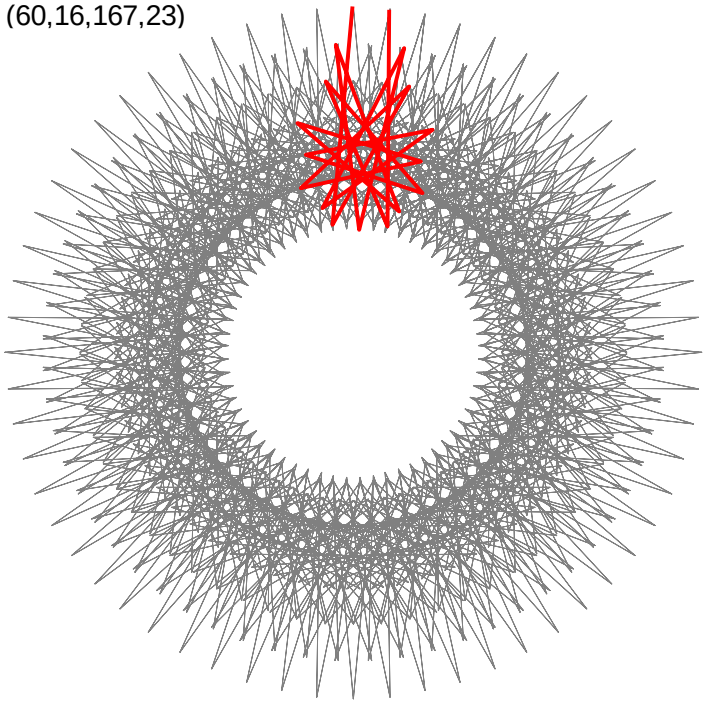


The **first cycle is shown in red** in both images on the previous page and each ends one vertex past the top of the hour; subsequent cycles click off seconds one at a time, just like the second hand of a clock (in this instance a very quick clock). The difference is that the first image excludes the center and the second crosses over the center. If you change ***S*** to values other than 2, you maintain the same 60-second attribute as long as ***P*** and ***J*** are MMI MOD 60 (with the additional requirement that the GCD(***S***, ***P***) = 1), but the images can become much more intricate.

For example the 16 point spinning star on the left or the stacked circles image on the right. The only difference is ***P*** = 167 on the left and 47 on the right. Like above, the **first cycle** ends at vertex 1 because 1 = 167·23 = 47·23 MOD 60. In the terms used above, 167 is in residue class 47 MOD 60, and because 47 is MMI of 23 MOD 60, so is 167 (and other values).

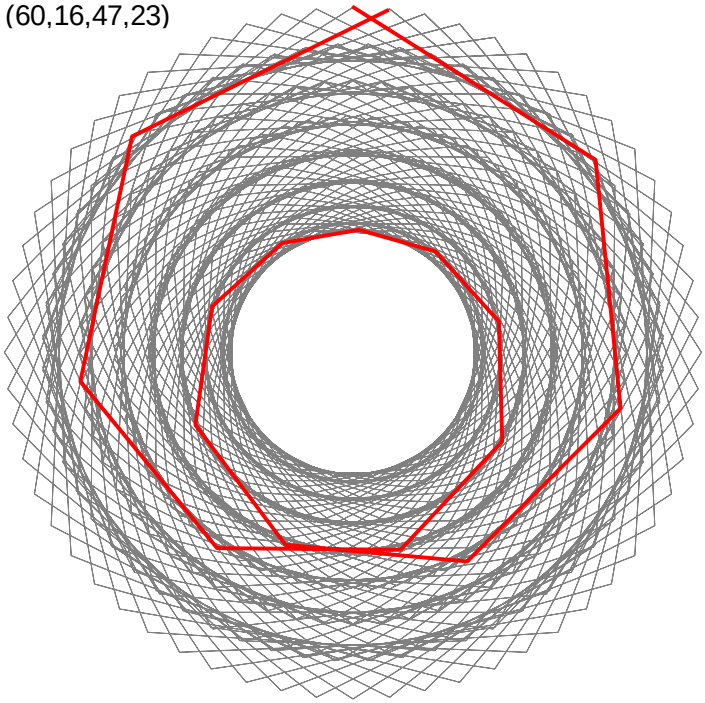
(n, S, P, J)
(60,16,167,23)

960 lines



(n, S, P, J)
(60,16,47,23)

960 lines



If you want to learn more about 60-second images, there is a 6 page paper, *The Ticking Clock*, at the end of **File 2** dealing with this topic. Unfortunately, it is a bit too complex to be covered in a 1-2 page *explainer*.

Negative MMI. One point discussed in that paper is that one can readily conceptualize an extension to the notion of MMI, by asking: can we describe two numbers ***a*** and ***b*** whose product is that 1 **less than** a multiple of ***m***? If so, we call this a negative MMI. Such values would allow us to model a fanciful world in which clocks run backwards.

Definition. When numbers ***a***, ***b***, and ***m*** have the property that ***a***·***b*** is one smaller than a multiple of ***m*** we say that ***a*** *and* ***b*** *are* ***negative*** *modular multiplicative inverses modulo* ***m*** (***a*** and ***b*** are nMMI MOD ***m*** if ***m***-1 = ***a***·***b*** MOD ***m***).

This does indeed happen, and in fact it happens just as often as MMI because if 1 = ***a***·***b*** MOD ***m*** then -1 = -1·***a***·***b*** MOD ***m***. Note that ***m*** – ***a*** = -1·***a*** MOD ***m*** and ***m*** – ***b*** = -1·***b*** MOD ***m*** since it does not matter whether you apply the -1 to ***a*** or ***b***.

Examples. Suppose you want to replicate the images above, but you want them drawn counterclockwise. All you need to do is replace ***J*** by ***n*** – ***J*** above. Here are links to the backward left image, and to the backward right image.

A second way to obtain the same image drawn counterclockwise is to replace ***P*** by ***n***·***S*** – ***P***.

(1, 4), (2, 2), (3, 3) are all nMMI pairs MOD 5. Additionally, (1, 11) and (5, 7) are nMMI pairs MOD 12.

A final note. Many of the images of interest in **Part I** and **Part II** that appear to be the most interesting are ones where one or more of the parameters are a bit more or less than a multiple of another parameter (or product of parameters). The formal mathematical issue in this instance boils down to MMI and nMMI.