

PROPERTIES OF THE INTEGER SPIRAL

Several years ago while lecturing on complex variables to our undergraduate engineering analysis class we encountered the function-

$$(1+i)^n = 2^{n/2} \exp(i\pi n/4)$$

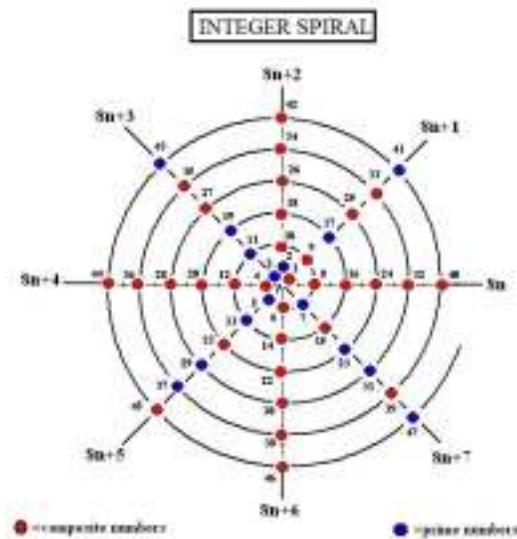
This function represents essentially an exponential spiral when plotted as an Argand diagram. On looking a bit more at this function it became clear that there should also be a related function-

$$F(n) = n \exp(i\pi n/4)$$

which in polar coordinates reads $r=n$ and $\theta=\pi n/4$. Eliminating the n between r and θ leads to an Archimedes Spiral-

$$r = (4/\pi)\theta$$

If we now think of n as being any positive integer $n=1, 2, 3, 4, 5, 6, \dots$ then it falls at a point along the Archimedes Spiral at angle $\theta=n\pi/4$. A plot of this function out to $n=47$ looks like this-



We term this figure the INTEGER SPIRAL with all positive integers located at the intersection of the spiral and four straight lines passing through the plot origin at angles $0, \pi/4, \pi/2,$ and $3\pi/4$. Note that all even numbers fall along the x or y axis while all odd numbers fall along the diagonals $y=\pm x$. The jump between integers lying along the same straight line is always equal to an integer multiple of eight. The integers which are prime are indicated in blue while those in red are composite numbers. Note that, except for $n=2$, all primes lie on the diagonals. As we have already shown in an earlier note, the well known Ulam Spiral shows a prime number structure to which some individuals have ascribed deeper

meaning . What has not been realized by these individuals is that the pattern represents no more than a statement that all primes, except $n=2$, are odd numbers as can easily be shown by a simple transformation (see our 2008 article at <http://www2.mae.edu/~uhk/MORPHING-ULAM.pdf>).

Note that this graphical method of representing numbers allows us to break the integers into a total of eight subgroups. The even integers are given by $8n$, $8n+2$, $8n+4$, and $8n+6$ while the odd integers have the form $8n+1$, $8n+3$, $8n+5$, and $8n+7$. To determine into which of these subgroups an integer N belongs one needs to simply divide by 8 and look at the remainder. Thus $N=379237$ produces 4742.125. This means this number is found at the intersection of the 4742nd turn of the Archimedes Spiral along the diagonal in the first quadrant. Another way to get this same result is to apply a mod 8 operation to the number N . For this number my PC states that-

$$379237 \text{ mod } 8 = [1]$$

Likewise the number 48210937523 produces a mod of [3] and so lies along the diagonal in the second quadrant. The numbers $N=2^{2n+1}-1$, which represent the Mersenne Numbers, contains as a sub-class the well known Mersenne Primes for certain integer values of n . When these numbers are subjected to a mod 8 operation they always yield [7]. Thus all Mersenne Numbers lie along the diagonal in the 4th quadrant. The numbers defined as $N=2^{2^n} + 1$, represent the Fermat Numbers. They all yield [1] on a mod operation and hence will be found along the diagonal in the first quadrant.

One can carry out mathematical manipulations including sum and product of n s along the Integer Spiral. Take first the case of addition-

$$(8n_1+1)+(8n_2+4)=8(n_1+n_2)+5 =N$$

Using the mod 8 operation, it tells us that the sum of the number $8n_1+1= [1]$ and $8n_2+4= [4]$ produces $[1]+[4]=[5]$ and implies a number lying along the diagonal in the 3rd quadrant. If we next take the product-

$$(8n_1+3)(8n_2+5)=64n_1n_2+(40n_1+24n_2)+15$$

, we see that it produces a number lying along the 4th quadrant since $15 \text{ mod } 8 = [7]$. As a special case consider $n_1=423$ and $n_2=615$ so that one is multiplying the numbers $N_1= 3387$ and $N_2=4925$ together. Without needing the value of their product N_3 we know that N_3 lies along the diagonal in the 4th quadrant. The actual product equals-

$$N_3=16649280+(31680)+15=16680975$$

A simple mod operation shows that $N_3 \text{ mod } 8 = [7]$ confirming the location of this odd number N_3 . The mod 8 operation will always apply to the present Integer Spiral. Thus the operation-

$$678 \times 9123 \times 982+(645-712) \times 23=N=6074055367$$

tells us that $678 \text{ mod } 8 = [6]$, $9123 \text{ mod } 8 = [3]$, $982 \text{ mod } 8 = [6]$, $(645-712) \text{ mod } 8 = [5]$, and $23 \text{ mod } 8 = [7]$. So

$$[6 \times 3] \times [6] + [5] \times [7] = ([108] + [35]) \bmod 8 = [7]$$

According to this result the ten digit number $N = 6074055367$ is odd and lies along the diagonal in the 4th quadrant. One way to convert this last number to an even number lying along the negative x axis is to replace 23 by 16 because $108 \bmod 8 = [4]$.

We have shown above that all Mersenne Numbers must be divisible by $8n+7$. In addition, we can restrict things further by using only those divisors for which $8n+7$ is prime. This leaves us with the divisor set-

$$\{7, 23, 31, 47, 71, 79, 103, 127, 151, 167, 191, 199, 223, 239, 263, 271, 311, 359, 367, 383, \dots\}$$

We need to take this divisor up to a value close to \sqrt{N} to check the Mersenne Number for primeness. Look first at $2^{11}-1=2047$. Dividing it by numbers in the above set up to near 45.2437.. (hence 47), we find $(2^{11}-1)/23=89$. So the number 2047 is composite and factors into 23×89 . Note we accomplished this factoring with only two divisions. Next examine $N=2^{13}-1=8191$. Its root is 90.504.. So we try division by $\{7, 23, 31, 47, 71, 79\}$ and find none of the numbers divide evenly into N . Hence this number is one of the Mersenne Primes. As another possibility try $N=2^{37}-1=137438953471$. This time the divisor might have to go as high as 370726. However starting again with a divisor of 7 we find 223 divides things evenly. Hence it took just 13 divisions to factor this composite Mersenne Number as-

$$2^{37}-1=137438953471=223 \times 616318177$$

One can use a similar approach for producing factors of the Fermat Numbers $N=2^{2^n} + 1$. The first few of these numbers are 5, 17, 257, 65537, 4294967297, and, 18446744073709551617. They all lie along the diagonal in the first quadrant and hence should be divisible by those prime numbers which have the form $8n+1$. This divisor set is found to be-

$$\{17, 41, 73, 89, 97, 113, 137, 193, 233, 241, 257, 281, 313, 337, 353, 401, \dots\}$$

From the numbers in this set it is at once apparent that the Fermat Numbers 5, 17 and 257 are prime since they appear in the $8n+1$ set. Looking next at 65537 we find that its square root is approximately 256 so we need to divide by $\{17, 41, \dots \text{up through } 241\}$. If this is done we find no even division results and hence 65537 is prime. This result was established with just ten divisions. The next Fermat Number $2^{32}+1$ turns out to be composite as first shown by Euler. If we tried to establish this fact by the present approach it could possibly involve values in the set up to approximately 20724, a formidable task. However as we will show below the factoring can be simplified considerably by redefining the Integer Spiral. We also want to point out that the present approach for factoring Mersenne and Fermat Numbers, is about four times faster than the standard brute force approach. It works because the smaller factor of N has the same mod value as the original number. This procedure will not work in general for other large odd numbers. Take the case of –

$$N= 110357851=863 \times 127877$$

In mod notation it reads $[3]=[7] \times [5]$ and so neither factor matches the mod of N . For numbers such as this last one no short cut exists and one must divide N by all prime numbers increasing the work by about a factor of four.

Finally let us look at the problem of accelerating the factoring process for large Fermat Numbers. We know from our Integer Spiral that these numbers fall along the diagonal in the 1st quadrant. It would seem that one can speed up the factoring process for these numbers by using a divisor set constructed from the numbers $(2^{3+m} + 1)$. Choosing $m=4$, we get the divisor set based in prime numbers satisfying $(128 \times n+1)$. The set reads -

$$\{257, 641, 769, 1153, 1409, \dots\}$$

If we now look at the Fermat Number $2^{32} + 1$ and divide by the numbers in this divisor set, an even division first occurs for 641 and one has the factor-

$$2^{32} + 1 = 4294967297 = 641 \times 6700417$$

The factoring was achieved with just two divisions. Note that if we had gone to $m=5$ then $256 \times n+1$ would have its divisor set go as $\{257, 769, 329, \dots\}$ and no factoring would be observed. Thus one must conclude that m cannot become too large. The introduction of the integer m into the evaluation is essentially the same as taking the original Integer Spiral above and placing integers upon it at smaller angle intervals of $\Delta\theta = 2\pi/2^{3+m}$. Each turn of this new Integer Spiral will contain 2^{3+m} successive integers and the jump between integers lying on the same diagonal will be $n2^{3+m}$.

August 2012