PROPERTIES OF THE INTEGERS 6n±1

We have shown in several notes over the last few years that all primes above three have the form 6n±1 but, at the same time, that not all 6n±1 integers are prime. We wish in this note to investigate further the properties of all integers having the form 6n±1.

Let us begin by writing out the first few of these odd integers. They are-

N[n]= 6n+1={7, 13, 19, 25, 31, 37, 43, 49, 55, 61, 67 , 73, 79, 85, 91, 97,..}

and

M[n]=6n-1={5, 11, 17, 23, 29, 35, 41, 47, 53, 59, 65, 71, 77, 83, 89,95,.. }

If we look at all 26 prime numbers from 5 through 97, they read-

P={5, 7, 11,13, 17, 19, 23, 29, 31, 37. 41, 43, 47, 49, 53, 55, 61, 67, 71, 73,
77, 79, 83, 89, 91, 97}

That is, with the exception of 25, 35, 49, 55, 65, 77, 85, 91, and 95 , all numbers of the form N[n] and M[n] are primes. The exceptions are semi-primes of the form-

25=5x5 35=5x7 49=7x7 55=5x11 65=5x13 77=7x11
85=5x17 91=7x13 95=5x19 etc.

or possibly multiple prime products such as 834=7x7x17=6(139)-1. Since semi-primes are the product of two primes 6n±1 and 6m±1, it is clear that all semi-primes also will have the form 6k±1. In terms of modular arithmetic we have that-

(6n+1) mod(6)=1 and (6n-1) mod(6)=5

So that a mod(6) operation on any prime above 3 or semi-prime above 9 will yield 1 or 5. Take, for example, the semi-prime –

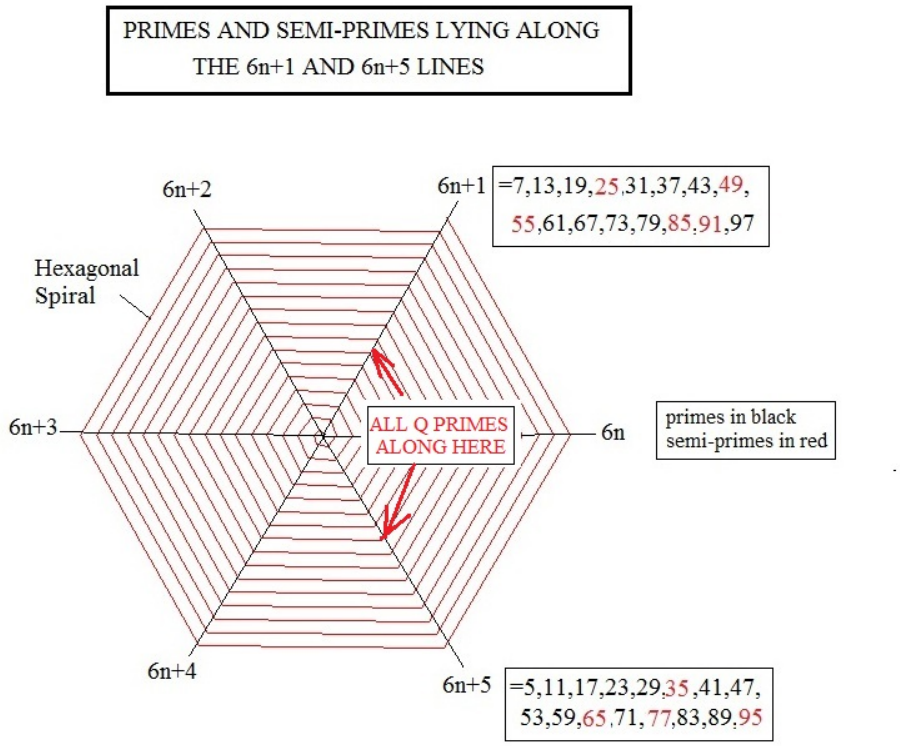
6497 = 73x89 which yields 6497 mod(6)=5

Its prime components yield 73 mod (6)=1 and 89 mod (6)=5

Because of the cyclical nature of a mod (6) operation it should be clear that a mod(6) operation yielding 5 is the same as saying it lies along the line 6n-1. These facts allow us to plot all primes and semi-primes within the polar r-θ plane at the intersection of two diagonal lines and a hexagonal spiral defined by –

r=integer , θ= integer π/3

The diagonal are 6n+1 and 6n-1 (or the equivalent 6n+5). Here is the resultant picture-



What is most interesting about this result is that all primes above 3 lie just along the lines 6n+1 and 6n-1 with no exception found for numbers as high as six digits We call this collective group of primes the Q Primes. It is amazing that no one has realized this fact previously considering all the work mathematicians have put into obtaining the location of primes along an Ulam Spiral. The rather scattered location of primes found there really shows no more than the fact that prime numbers above 3 must be of the form 6n±1. From our observations, we can state at once that the huge number-

741888142827763156497323

is a composite since it is of the form 6(n)+3. However the number-

6(34783750937)+1=208702505623

could be either prime or possibly a composite. A prime test shows it to be prime.

To factor a large semi-prime N=pq we can use the fact that-

$$(6n\pm1)(6m\pm1)=36nm\pm6(n+m)+1=N$$

and then solve this equation as the algebraic equation m=f(n). Let us demonstrate this by looking at the semi-prime-

$$4717=6(786)+1$$

We get –

$$6\ nm+(n+m)=4716/6=786$$

or

$$m=\frac{786-n}{6n+1}$$

To solve this for integer values we can restrict ourselves to |n|<sqrt(N)/6≈11. Carrying out the search we find m= -15 at n=-9. That is-

$$[6(9)-1][6(15)-1]=53 \times 89=4717$$

The reason for the minus signs on n and m stems from the fact that we initially assumed p=6n+1 and q=6m+1. This usually will not cause a problem in the solution method. However, when N becomes considerably larger the search will need to extend over a much larger range -sqrt(N)/6<n<sqrt(N)/6 making the search quite time consuming. This is the reason large semi-primes can be used securely in cryptography. It is extremely time consuming to factor a 100 digit long semi-prime into its two prime components.

Two of the more famous prime number groups can be generated by the simple formulas-

$$M[p]=2\text{^}p-1 \quad \text{and } F[n]=2\text{^}2\text{^}n$$

Here ^ indicated a power. When these numbers are prime they are known, respectively, as Mersenne Primes and Fermat Primes. The first few Mersenne Primes read-

$$M[p]=\{3, 7, 31, 127, 8191, 131071, 524287, \ldots\}$$

The numbers increase in size very rapidly. To this day less than 50 of these primes have been found although it is believed there are an infinite number of them. Note that each of thee Mersenne Primes above 3 have the form 6n+1. They always end in 1 or 7. They are found along the 6n+1 curve in the above diagram. The Mersenne Primes are much rarer than the Q primes.

The Fermat Primes read-

$$F[n]=\{5, 17, 257, 65537\}$$

Euler was the first to show that $2^{32}+1$ is not a prime. Mathematicians later showed, within limits of their computers to handle large numbers, that no Fermat numbers above 2^4+1 is prime. It is still an open question whether this continuous to hold for all n in n^2^n. Notice that the Fermat numbers and primes all have the form 6n-1 and hence they will be found along the 6n+5 branch in the above graph. Again they are quite sparse compared to all Q Primes of the form 6n-1 , of which we expect an infinite number.

Consider next multiplying together two numbers 6n+1 and 6m+1 to see how they relate to a semi-prime 6k+1. Here n, m, and k are all taken as integers. We get-

$$k=nm+(n+m)/6$$

So if n=30 and m=66, we get 6(30)+1=181 and 6(66)+1=397. Also –

$$k=6nm+(n+m)=11976$$

This means we have the factored number-

$$71857=181 \times 397$$

Also we could take the primes 6n+1 and 6m-1 to generate a semi-prime 6k-1. This produces-

$$k=6nm+(m-n)$$

If we take n=121 and m=287, we get k=208528. This says that we have the factored number-

$$1251167=727 \times 1721$$

Thus we can always start with two integers n and m, which produce the primes primes p=6n±1 and q=6m±1, to generate a k and hence N=pq. This is the easy part consisting of simply multiplying two prime numbers together. The hard part of the problem is trying to reverse things by starting with a known value of k for a semi-prime and then trying to find n and m. This involves a search over integers n and m simultaneously and represents essentially the approach used above. Again, if k=37 so that N=221=6(37)-1, we have 37=6nm+m-n with n<3. So trying n=2 we get 37=12m+m-2 or 39=13m. Thus n=2 and m=3. We can write-

$$221=[6(2)+1][6(3)-1]=13 \times 17$$

Any integer power ‘a’ of 6n±1, can be expanded in its binomial form-

$$(6n+1)^a = (6n)^a + a(6n)^{a-1}/1! + (6n)^{a-2}/2! + \ldots + 1$$

From it one sees at once that –

$$(6n+1)^a \bmod(6)=1$$

Likewise one has –

$$(6n-1)^a \bmod(6)=5$$

This means any integer power of 6n±1 stays on the same diagonal. Take the prime 6(3)+1=19. Its 17th power equals –

N=5480386857784802185939 with N mod(6)=1

It, of course , must be a composite number since the positive integer power of any prime must be a composite. From this type of result it becomes clear that the density of Q primes will become progressively smaller relative to the composites as N gets larger and larger. This makes sense in terms of the fundamental theorem for prime numbers which states that the number of primes lying between N_1 and N_2 for larger numbers approximately equals-

$$\frac{N_2}{\ln(N_2)} - \frac{N_1}{\ln(N_1)} \quad where \quad N_2 > N_1 >> 1$$

To further verify the fact that all primes above p=3 are of the form 6n±1 let us look in the range between the 100th prime of 541 and the 110th prime of 601. All eleven primes in this range may be written in the form 6n±1 as shown-

541=6(90)+1	577=6(96)+1
547=6(91)+1	587=6(98)-1
557=6(93)-1	593=6(99)-1
563=6(94)-1	599=6(100)-1
569=6(95)-1	601=6(100)+1
571=6(95)+1	

In this case the fundamental theorem would predict-

601/ln(601)-541/ln(541)=7.96

primes. This number is a little low compared to the actual 11 do to the fact that the fundamental theorem only strictly applies when N heads to infinity. The actual

number of primes in the larger range $1 \leq N \leq 10{,}000$ is 1229. That is, there are 8771 composites in this range. The fundamental theorem predicts-

$$10{,}000/\ln(10{,}000)=1085$$

primes , so still a little low, but closer than the previous estimate. We can write the 1229^{th} prime as –

$$9973=6(1662)+1$$

The $10{,}000^{th}$ prime reads-

$$104729=6(17455)-1$$

May 25, 2015