USE OF MODULAR ARITHMETIC FOR DETERMINING THE ADDTION AND MUTIPLICATION OF INTEGERS

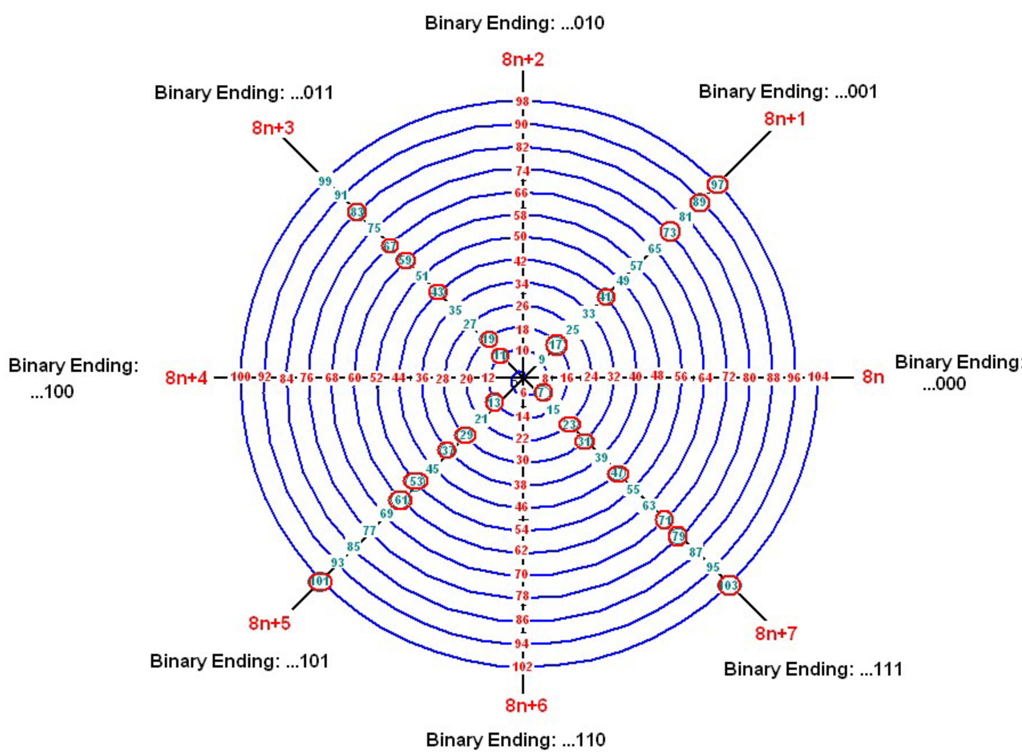
In the last year or so we have been studying the properties of large prime numbers and how to generate them. During this process we have come up with a way to represent all integers in a cyclic fashion by designating them as the points of intersection of eight radial lines with an Archimedes spiral. The spiral has the polar form-

$$r = sqrt[x^2 + y^2] = \frac{4}{\pi}\theta$$

and superimposed on this spiral one draws eight equally spaced radial lines given by-

$$\theta = \frac{n\pi}{4}, n = 0, 1, 2, 3, 4, 5, 6, 7$$

The intersections they produce with the spiral represents all integers grouped into 4 even and 4 odd groups as indicated in the following graph-



The eight groups are-

$8n= 0, 8, 16, 24, 32, 40, 48, 56, 64,\ldots\equiv 0(mod(8)$

$8n+1= 1, 9, 17, 25, 33, 41, 49, 57, 65,\ldots\equiv 1(mod8)$

$8n+2= 2, 10, 18, 26, 34, 42, 50, 58, 66,\ldots\equiv 2(mod8)$

$8n+3= 3, 11, 19, 27, 35, 43, 51, 59, 67,..\equiv 3(mod8)$

$8n+4= 4, 12, 20, 28, 36, 44, 52, 60, 68,\ldots\equiv 4(mod8)$

$8n+5= 5, 13, 21, 29, 37, 45, 53, 61, 69,\ldots\equiv 5(mod8)$

$8n+6= 6, 14, 22, 30, 38, 46, 54, 62, 70,\ldots\equiv 6(mod8)$

$8n+7= 7, 15, 23, 31, 39, 47, 55, 63, 71,\ldots\equiv 7(mod(8)$

It is clear that all odd integers lie along the four diagonal lines given by $(2n+1)(mod8)$ and the remaining even integers lie along either the x or y axis as given by $(2n)(mod8)$. The radial distance from the origin to a particular number N is just its value. The three digit binary endings along the eight radial lines are as indicated. Thus, for example, the number-

N= 63459813 reads 11110010000101000111100101 in binary

Hence it lies along the diagonal in the third quadrant at the $n=[63459813-5]/8=7932476^{th}$ turn of the Archimedes spiral. Since all prime numbers(with the exception of 2) are odd numbers, they all will necessarily fall along the straight diagonal lines $y=x$ and $y=-x$. The much discussed Ulam spiral for primes does not really contain any hidden information as thought by some investigators since (as we have already shown in one of our earlier notes above) the Ulam spiral patterns can easily be transformed into the much simpler straight line patterns shown here and hence say no more than that primes are odd numbers. One can use modular arithmetic to work out the basic operation of addition (+) and multiplication (x) for the above described integers. We note that $n(mod8)+m(mod(8)=(m+n)(mod8)$ and $[n(mod8)] \times [m(mod8)=(n\cdot m)(mod8)$, so that one has the following addition and multiplication tables-

(+)	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

and

(x)	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Notice the cyclic pattern of period 8. As a special example, consider multiplying any odd number along the diagonal in the second quadrant by any even number along the negative y axis. Here one has-

$$3(\bmod 8)\cdot 6(\bmod 8)=2(\bmod 8)\ \textit{from the table}$$

So that one knows the product will lie along the positive y axis. This is confirmed by 59· 38=2242=8(280)+2. Also, by looking at the tables, we have the following generalizations-

(1)-Multiplication of an even number by an odd number results in an even number

(2)-Multiplication of two even numbers will yield an even number

(3)-Multiplication of two odd numbers will be odd. The product of two primes(other than 2) will also be odd

(4)-Addition of an even number and an odd number will be odd

(5)-Addition of two even numbers is even

(6)-Addition of two odd numbers will be even. Thus the addition of two prime numbers(with the exception of 2) must also be even.

The length along the Archimedes spiral from the number N to N+1 is given by-

$$\Delta L(N) = \int_{r=N}^{N+1} \sqrt{(1+(r\pi/4)^2}\,dr$$

which leads to a rather complicated monotonic expression with increasing values N. A very good approximation to this integral for larger N is

$$\Delta L(N) \approx \frac{(2N+1)\pi}{8}$$

so that the distance along the spiral between neighboring integers is proportional to N for large N. There is not much additional information recoverable from this result.

To determine whether or not a particular odd number lying along one of the four diagonal lines is prime or composite, one generally requires division of all the odd integers less than about sqrt(N). Take the number N=457 reading 111001001 in binary and hence being part of the group 1(mod8). We first write the one line program-

```
for n from 1 to 3 do{n,457/(8*n+1)}od;
```

and find no integer answers. This is followed by redoing the calculation with the remaining three devisors 8n+3, 8n+5 and 8n+7 in turn. None of these quotients produce an integer solution and hence N=457 is a prime number. Next consider N=357867 whose binary form ends in 011 and hence the number lies along the diagonal in the third quadrant. This time the maximum value of n to be tested will be about 75 so one begins with the program-

```
for n from 1 to 75 do{n,357867/(8*n+3)}od;
```

It yields an integer solution of 7017 at n=6 and, hence, the number N=357857 is composite and equal to (8*6+3)(7017=51*7017. No further calculations for this number are thus required.

What is clear in these calculations is that n becomes large as N gets large and will require some 4*sqrt(N)/8 quotient evaluations to determine primality. If the number is composite the number of evaluations will be considerably less. To test a sixty digit number for primality by the present brute force approach would require some

0.5*10^30 separate quotient calculations. Fortunately, the primality of some special numbers such as those of Mersenne can be determined with fewer calculations. Also my canned MAPLE program uses a probabilistic primality testing routine which works very well and is fast. It can tell in a fraction of a second that the number-

[2^(701)+1]/3=35067572676989156714939932552534191103668932018821159063321
872687124881028647205480757776908517256341513219792374521451420129548334
558692420852098471012538999701491140856297321277758385895484781808621678
23854251

which in binary has the interesting periodic form-

101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010
1010101010101010101010101010101010101010101010101011

is prime and lies along the diagonal in the second quadrant. A more difficult problem is the actual factoring of large composite numbers such as the neighboring composite [(2^701+1)/3] +2. I ran my MAPLE program for a total of eight minutes to try to factor these without success. However I am able to show that it is composite by noting this number will lie along the diagonal in the third quadrant and hence may be divisible by 8n+5= 5, 13, 21,..Indeed after just two trials we find the integer quotient-

((2^701+1)/3 +2)/13 =
26975055905376274396107640425026300848976101552939353125632209759 3\
268315604978503698136745450132741088563229172111703472462534 98\
718891301862193921900778876153616531646812536400982891066073 44\
98321604782140296481

so that the number [(2^701+1)/3] +2 is clearly composite!

May 2009