WHAT IS NUMBER THEORY AND WHAT ARE SOME OF IT'S MORE IMPORTANT RESULTS?

Number theory is one of the oldest and best known branches of mathematics. It deals strictly with only the positive integers n=1,2,3,4,5,… and their relation to each other. Many great mathematicians going back to those of ancient Babylon and Greece have contributed to this field. The interest has continued to the present day with mathematicians such as Mersenne, Fermat, Euler, Gauss, and Riemann having made major contributions along the way. Because of its pure nature, with almost no practical applications until the advent of electronic computers and digital cryptography in recent years, it is often referred to as the"Queen of Mathematics". We want here to briefly discuss some of its more important findings.

Our starting point is the collection of integers-

1 2 3 4 5 6 7 8 9 10 11 …..

These have the properties that –

n+m=m+n and n·m=m·n

One of the first things one can ask is what is the value of the sum of the first N positive integers? The answer has been known for at least 2000 years and goes as follows-

$$S[N] = 1+2+3+4+5+....(N-1)+N = (1+N)+(2+N-1)+... = \frac{N(N+1)}{2}$$

Likewise more complicated formulas exist for the sum of the kth power of the first N integers. The sum of the inverses of the powers of the first N integers reads-

$$F[N,k] = 1+\frac{1}{2^k}+\frac{1}{3^k}+\frac{1}{4^k}+\quad +\frac{1}{N^k} = \sum_{k=1}^{N}\frac{1}{n^k}$$

When N goes to infinity this sum is known as the Riemann Zeta Function ζ(k). Note that it diverges for k=1 but will have a finite value for k different from one. Euler for example showed that $\zeta(2)=\pi^2/6$.

The product of the first N integers is simply the factoral N! which may also be written as the gamma function Γ(N+1) . We have-

$$1\cdot 2\cdot 3\cdot 4\cdot 5\cdot ....\cdot N = N! = \Gamma(N+1) = \int_{t=0}^{\infty} t^N \exp(-t)dt$$

We also have that –

$$1 \cdot 4 \cdot 9 \cdot 16 \cdot ....N^2 = (N!)^2$$

and-

$$1 \cdot 3 \cdot 5 \cdot 7 \cdot ... \cdot (2N-1) = \frac{(2N)!}{2^N N!}$$

The sequence of integers-

1 2 3 5 8 13 21 34 55 89 144 …

is known as the Fibonacci Sequence and follows the generation rule that the nth term equals the sum of the two previous terms in the sequence. If one looks at the ratio of the k+1 term compared to the kth term in the Fibonacci Sequence the ratio approaches the Golden Ratio φ=[1+sqrt(5)]/2=1.6180339… .

There are two types of positive integers. They are the composite numbers and the prime numbers. The primes are divisible only by 1 and themselves while composites are divisible by one or more additional numbers. With the exception of 2, all prime numbers are odd although not all odd integers are prime. The first few odd primes are-

p_k=3,5,7,11,13,17,19,23,29,31,…

while the first few composites are-

c_k=4,6,8,9,10,12,14,15,16,18,….

Christian Goldbach first noticed back in 1742 that the sum of any two primes equals an even number. That is-

$$p_a + p_b = 2N$$

which produces, for example, the identity 1249+3559=2(2404)=4808. So far no one has succeeded in given a definitive proof of this conjecture although many, including Leonard Euler, have tried. It is known that the distance between primes in a given integer interval increases with the value of the integer. This fact is expressed by the prime number theorem which states that the number π(n,m) of primes existing between the nth and mth integer is approximately-

$$\pi(n,m) \approx [\frac{m}{\ln(m)} - \frac{n}{\ln(n)}] \quad for \quad m > n >> 1$$

Thus if we take n=ithprime(58)=271 and m=ithprime(72)=359, we get the estimate –

$$\pi(271,359) = \frac{359}{\ln(359)} - \frac{271}{\ln(271)} = 12.645...$$

for the number of primes in the range. The actual number is 72-58=14 and thus the estimate is close.

It is always possible to break any integer N into products of primes taken to specified powers. That is-

$$N = \prod_{k=1}^{m} {p_k}^{a_k} = {p_1}^{a_1} \cdot {p_2}^{a_2} \cdot {p_3}^{a_3} \cdot .... \cdot {p_m}^{a_m}$$

From this fact we have-

$1346423=(13)^2(31)(257)$ and $5678=(2)(17)(167)$

To determine the greatest common divisor between two integers one needs to only look as the product terms which are common between the two integers. Thus we see that-

gcd(136,368)=8 since $136=2^3 \cdot 17$ and $368=2^4 \cdot 23$

The French cleric Mersenne(1588-1648) noticed (after studying Euclid) that numbers of the type-

$$M[p] = 2^p - 1$$

are likely to be primes. This works fine for p=3, 5, 7 but breaks down at p=11 and for most higher prime numbers p. To this date only 48 Mersenne Primes have been found although one suspects there are an infinite number of them.

The sum of all the divisors of a number N are designated by the sigma function σ(N). A variation on this number, which we introduced recently, is the <u>number fraction</u>-

$$f(N) = \frac{[\sigma(N) - N - 1]}{N}$$

This function has the interesting property that it increases only very slowly with increasing N and that it yields f[N]=0 only when N is a prime. Since the sigma function is built into most advanced computer mathematics programs, we can distinguish at once between a prime and composite number by looking the value of f(N). The f(N)s are unique for each number with number fractions above f(N)=1 considered super-composites. A number such as N=421123 has f(N)= 0 and so is a prime while N=202574105542278 yields f=1.340812267.. and is thus a super-

composite. The average value of f(N) in the range 3<N<100 is about 0.65. The number 24=2+4+6+8+12 has f[24]=1.333.. and is therefore a super-composite.

Another interesting property of integers is that some combinations constitute Pythagorean Triplets in the sense that-

$$a^2 + b^2 = c^2$$

An example is a=3, b=4, and c=5 yield 9+16=25. There are of course an infinite number of other triplets as already known to the ancient Babylonians. One can generate some of these triplets by use of the identity-

$$(x^2 - \Delta^2)^2 + (2\Delta x)^2 = (x^2 + \Delta^2)^2$$

for any integer x and Δ. Taking x=12345 and Δ=6000 , we find a=116399025, b=148140000, and c=188399025.

Equations of the type-

$$F(x)+G(y)=C$$

are referred to as Diophantine Equations. One seeks solutions satisfied by integer pairs [x,y]. As an example, consider the simple equation-

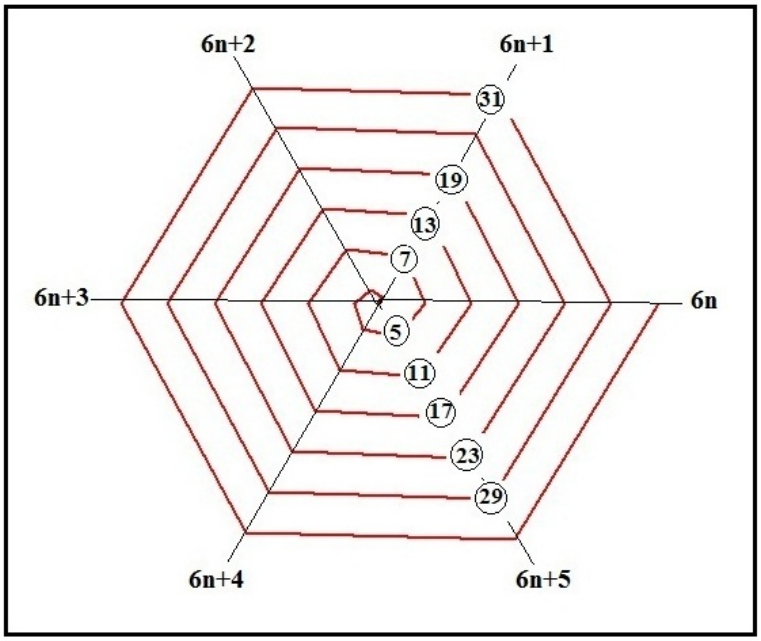
$$y^2 = x + 1$$

If we set x=k then y must equal sqrt(k+1) and both x and y must be integers. We see at once that this is possible for [x,y]=[0,1],[3,2], [8,3],[15,4] and so on. That is we have the general solution pairs [x,y]=[n^2-1, n] for any integer including negative n. A special modern version of a Diophantine equation is our own equation-

$$y^2 = [36x - (N+1)]^2 - 4N$$

which we have used recently to factor semi-primes N of the type 6n+1 into their prime components p and q. A trivial case corresponds to N=7 where the above equation yields just one integer pair [x,y]=[0, 6]. A much more difficult evaluation is encountered when N=21428053. There one finds a solution pair (besides the obvious one at [0, N-1]) equal to [x,y]=[595483, 1188].

We have been studying prime numbers in great detail in the last few years and have come to the conclusion that all prime numbers above 3 must be of the form p=6n±1. We call these numbers the Q Primes. A very interesting property of these primes is that they all fall along two diagonal lines when plotted as part of an integer spiral of hexagonal form as shown-



The few gaps noted along the two diagonals where the Q Primes are located, correspond to composite numbers of the type 6n±1 such as 25 and 35. We have found in searching over the integer range 3<n<5000, that the number of Q Primes in a given range match exactly the total number of primes for that range. This fact can be used to advantage when factoring large semi-primes as we have done in another note posted on our MATHFUNC page. The Mersenne Primes all are of the form 6n+1 and so will be found along the diagonal in the first quadrant of the graph.

Finally we conclude by looking at the use of modular arithmetic for integers N. This is a very important number theory concept first introduced by Gauss in 1801 . It says essentially that when an integer M is divided by another integer N the result will be-

M/N=integer +A/N with A the remainder

This fact may be expressed in modular arithmetic language as –

M mod(N)=A

One says M is congruent to N modulo A. Thus 123 mod(36)=15 and 38738 mod(124)=50 . This is the same as saying that 123 divided by 36 leaves a remainder of 15 and 38738 divided by 124 yields a remainder of 50. One can use such modular operations to advantage in recognizing where along the six radial lines in the above diagram a number N will be found. As an example we have that –

36561009825477 mod(6)=3

This number lies along the line 6n+3 and tells us at once that it cannot be a prime. As another example look at-

67093264351 mod(6)=1

This could possibly be a Q prime. A check on its number fraction yields f(67093264351)=0 and so it is indeed a prime number. Another advantage one has with mod operations is that one can use it to tell along which diagonals in the above diagram the primes p and q making up a semi-prime N=pq will be found. So the product 37 x 89 =3293 yields 37 mod(6)=1 and 89 mod(6)=5. From this we see that the number N=pq must have 3293 mod(6)=5. That is 37 lies along the diagonal 6n+1 while both 89 and 3293 lie along the diagonal 6n+5. One can also use the mod operation to treat certain algebraic expressions such as Fermat's Little Theorem which states that –

$$\frac{n^{p-1}-1}{p} = \text{integer when p is a prime and n equals any integer 2,3,4,..}$$

Converting this to modular form we have-

$(n^p-n) \bmod(p)=C_1$ **or the equivalent** $n^{p-1} \bmod(p)=C_2$

where C_1 and C_2 are integers. Thus if n=2 and p=13 we have 8190 mod(13)=630 which is an integer and hence p=13 is a prime, On the other hand when n=2 and p=27 we have134217726 mod(27)=4971026.889.. which means that p=27 is a composite.