12 JANUARY 2012

MODULAR ARITHMETIC + PRIME NUMBERS

A note on history: ~~Ma~~ when Math makes headline on the NYT.

→ Andrew Wiles and Richard Taylor solves Fermat's Last Theorem.

- Fermat's Last Theorem:

$$a^n + b^n = c^n \qquad a, b, c \in \mathbb{N}$$

only valid if $a, b, c = 0$ or $n = 1, 2$.

- Proof of the above "theorem" is long and can only be understood by few ppl.
- Last "Theorem"?
  - ⇒ Fermat never provided the proof himself but only mentioned that he had produced a marvelous theorem that was too long to fit on the margin of his book.
  - ⇒ ~~whe~~. The case when $n=3$ and $n=4$ was proven by Pascal + Euler, respectively.
  - ⇒ ~~other~~ Subsquent mathematician thinks that Fermat probably did not prove the theorem ... only an incorrect version assuming unique factorization.

The Story of Primes

Set up: Looking at $\mathbb{Z}$, more pricesly the structure and behavior of prime numbers

Def Ring is a collection of numbers which allow addition and multiplication w/ the "usual rules" (associativity, communitivity, distributivity)

e.g. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$, Gaussian Integers $a + bi$ $\mathbb{Z}$

non-e.g. $\mathbb{N}$ (subtraction is not closed ... although we ~~do~~ need not insist on division ?)

Def a numper p is prime if whenever p divides a product $p \mid ab$, then $p \mid a$ or $p \mid b$.

Def a number p is irreducible if ~~#/##~~ when $p = ab$, then at least a or b is a unit (i.e. has an inverse)

FACT: Within the integers, primes and irreduciblity are the same.
(I think it may be because integers only has two inverse, -1 and 1)

Consequence: If $n \in \mathbb{Z}$, then there is a factorization
$n = c_1 \circ p_1 \circ p_2 \circ \cdots \circ p_k$ where c is a unit and $p_1 \cdots p$ are primes

e.g.
$$6 = 1 \cdot 2 \cdot 3 = (-1) \cdot 2 \cdot -3$$

Moreover, if
$$d \circ q_1 \circ \cdots \circ q_\ell = n = c \cdot p_i \cdots p_k$$
where c and d are units. and p_i and q_i are primes
then, $k = \ell$ and, with suitable reordering, $q_i = \pm p_i$
= unique factorization property

ex, when $n \notin \mathbb{Z}$:
$\mathbb{Z} + \mathbb{Z}\sqrt{-5} \in a + b\sqrt{-5}$ ϵ
$\Rightarrow$ closed under addition
$\Rightarrow$ multiplication:
$$(a+b\sqrt{-5})(a_1+b_1\sqrt{-5}) = (aa_1 - 5bb_1) + (ab_1 + ba')\sqrt{-5}$$
= closed under multiplication.

In this ring, unique factorization property DOES NOT HOLD
if $n = 6$
$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$
and $2 \neq 1+\sqrt{-5}, 1-\sqrt{-5}$ and $3 \neq 1+\sqrt{-5}, 1-\sqrt{-5}$

INTERESTING FACTS ABOUT PRIMES

Harmonic Series goes as follows
$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \cdots$$
We note that harmonic series diverges by following argument:
$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \cdots$$
$$\boxed{\tfrac{1}{1}} + \boxed{\tfrac{1}{2}} + \boxed{\tfrac{1}{4} + \tfrac{1}{4}} + \boxed{\tfrac{1}{8} + \tfrac{1}{8} + \tfrac{1}{8} + \tfrac{1}{8}} \cdots$$
$$1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \cdots = \infty$$
$\Rightarrow$ we will have infinite $\frac{1}{2}$s in above series
$\Rightarrow$ since the ~~above~~ harmonic series is at least as great as the ~~harmonic~~ above series, the harmonic series must also diverge.

Thm There are infinite numbers of prime

Proof by Euclid

Suppose we had a finite list of primes, $p_1, \cdots, p_k$. If we consider $N = p_1 \circ p_2 \circ \cdots \circ p_k + 1$, N will not be divisible by any of those finite number of primes. (e.g. consider a number not divisible by 2 and 3. Simplest method of finding such number is $2 \cdot 3 + 1 = 7$)

So $p_i \nmid p_i \circ \cdots \circ p_k + 1$

By unique factorization, $N = p_i \circ \cdots \circ p_k + 1$ is a product of primes and a unit.

↳ N is a large number and is not a unit

→ No list on the finite list of primes divides N. There must exist a prime not captured by the list of primes above.

→ In this manner, we can produce infinite # of primes.

Euler Product

Recall $\frac{1}{1-x} = 1 + x + x^2 + \cdots$

consider $\frac{1}{1-\frac{1}{p}}$ where p is prime. Then, we consider

$$\frac{1}{1-\frac{1}{2}} \circ \frac{1}{1-\frac{1}{3}} \circ \frac{1}{1-\frac{1}{5}} \circ \frac{1}{1-\frac{1}{7}} \circ \cdots$$

$$= \left(1 + \frac{1}{2} + \frac{1}{4} + \cdots\right) \cdot \left(1 + \frac{1}{3} \cdot \frac{1}{9} + \cdots\right) \circ \left(1 + \frac{1}{5} \cdot \frac{1}{25} \circ \cdots\right) \circ \cdots$$

Consider "foil" method, we see that $1 \cdot 1 \cdot 1 \cdots = 1$, $1 \circ \frac{1}{2} \circ 1 \circ 1 \circ = \frac{1}{2}$, $\frac{1}{3} \circ 1 \circ 1 \circ 1 \circ \cdots$

and, eventually

$$= 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} \cdot \frac{1}{5} \cdot \frac{1}{6} \cdots = \Sigma \frac{1}{n}$$

?

<u>Consequence</u>

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{15} + \cdots \text{ diverges}$$

Density of Primes

Q: How large is the k^{th} prime number?

<u>Thm</u> Let π_k be the k^{th} prime number. We can make a statistic statement;

$$\lim_{k\to\infty} \frac{\pi_k}{k \cdot \ln(k)} = 1$$

This is bizarre and remarkable fact about primes, but it tells us ~~be~~ nothing on the spaces between primes. It can be that primes are separated by 2 integers or million integers.

We consider twin primes, pair of primes with difference of 2 (e.g. 11, 13).

Q: Are there infinitely many primes?

$\Rightarrow$ It is known that $\sum_{p=\text{twin}} \frac{1}{p} < \infty$.

$\Rightarrow$ equivalent statement is that above summation is not very large since it converges?

Consider prime triplets:

$$p \qquad p+2 \qquad p+4$$

We assert that apart from 3, 5, 7 such form of prime cannot exist.

$\Rightarrow$ if we divide p by 3, we have ~~3~~ 2 cases

(1) p is prime and thus 3 cannot divide p without producing a remainder. Suppose the remainder is 1. Then, since we consider a number $p+2$, this number must be divisible by 3. So triplet cannot exist.

(2) If the remainder was 2, then $p+4$ must be divisible by 3. Therefore, triplet cannot exist.

What if we consider ~~primes~~ prime triplets with distance other than 2?

<u>Thm</u>

$A = (a, a+n, a+2n, a+3n, \dots)$ $\quad a n \in \mathbb{N}$

then, unless $a|n$ there are infinitely many primes in A

So triplet, quadruplets, ... exists if you consider a large n

ex. 11, 17, 23

equidistance/$n=6$

Larger the distance, longer the sequence of primes of equidistance

= e.g. 10 sequence of primes may ~~be~~ have $n=$ 10 billion.

OPEN QUESTIONS OF MATH

$\Rightarrow$ Solve and be on the cover of NYT.

Q: Is it possible to write each even integer >2 as a sum of two primes?

eg. $4=2+2$ $\quad 6=3+3$ $\quad 8=3+5$ $\quad 20=13+7$

Goldbach Conjecture claims "yes you can".

Q: $\frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{3^s}+\ldots$ (harmonic series, modified) $=\zeta(s)$ Riemann zeta Function

$s=1 \Rightarrow$ zeta function diverges (or has a pole)

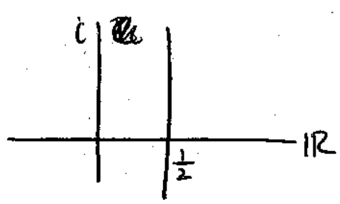
$S=2,4$, or any other integer: the value of zeta function shows up in physics

~~Q:~~ Describe all poles of the zeta function:

Generally believed answer.

If you allow s to be complex, then all (interesting i.e $s\neq 1$)

lies on the line $\mathrm{Re}(s)=\frac{1}{2}$



$\|$

Riemann Hypothesis, one of Clay Problems