12 JANUARY 2012

MODULAR ARITHMETIC + PRIME NUMBERS

1993: Mathematics Story Makes NYT Headline

→ Fermat's Last Theorem:

$$a^n + b^n + c^n$$

$a, b, c \in \mathbb{N}$ only happens if $a=0$ or $b=0$ or $c=0$

$n=1, 2$ but no other.

Proved by Richard Taylor & Andrew Wiles

Fermat: prolific writer of math.

"This (theorem) is true: I have produced a marvelous proof, but the margin of the page is too narrow."

↳ Later, someone reproduce his proof, (or what they thought was what he thought), but it was wrong. (It assumed true something not)

→ Euler proved $n \neq 3$ or 4 (Pascal)

Thinking is fun (Chris Dunham has a really good bk about math)

STORY OF PRIMES

setup: Looking at $\mathbb{Z}$, more precisely structure & behavior of prime numbers

Def Ring (same as field?) is a collection of numbers which allow addition and multiplication with the usual rules.

($a+b = b+a$ ... associativity, commutativity, distributivity)

e.g. $\mathbb{R}, \mathbb{R}, \mathbb{C}, \mathbb{Q}$, Gaussian Integers $a+bi$ ($i = \sqrt{-1}$), others (are these equiv; $\mathbb{Z}$; don't we need why? $\exists a, b$ s.t. $ab=1$)

Nonex: $\mathbb{N}$ (subtraction is required, although we do not insist on division)

Def a number p is a prime if whenever p divides a product $plab$, then pla or plb.

? Not entirely sure what unit is. Is p = prime

Def: a number p is irreducible if $p = ab$ then, at least one of a or b is a unit; i.e. has an inverse)

applies to all rings

= Note, we are in $\mathbb{Z}$.

Fact: Within the integers, primness and irreducibility are the same. (because then is only one inverse, -1 & 1 ?)

Consequence: If $n \in \mathbb{Z}$, then there is a factorization

$n = c \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_k$ where c is a unit and $p_1, \ldots, p_k$ are primes

e.g.

$$6 = 1 \cdot 2 \cdot 3 = (-1) \cdot 2 \cdot (-3)$$

Moreover, ~~the number~~ if

$$d \cdot q_1 \cdot q_2 = n = c \cdot p_1 \cdot p \ldots p_k$$

where c, d units and p_i, q_i primes

then, $k = \ell$ and, after a suitable reordering, $q_i = \pm p_i$

= "unique factorization property"

Ex: $\mathbb{Z} + \mathbb{Z}\sqrt{-5} \in a + b\sqrt{-5}$ (closed under addition)

$(a+b\sqrt{-5})(c+d\sqrt{-5}) = (ac - 5bd) + (ad+bc)\sqrt{-5}$ (closed under mult)

In this particular ring, unique factorization does not work

Note: $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

then all irreducible but obviously $2 = 1 \pm \sqrt{-5}$ or $3 = 1 \pm \sqrt{-5}$

↳ This assumption that unique factorization property works for all rings is false, thus Fermat may have thought wrong..

INTERESTING THINGS ABOUT MATH

FACT: harmonic series

"at least as much"

$$\underbrace{1}_{\|} + \underbrace{\frac{1}{2}}_{\|} + \underbrace{\frac{1}{3} + \frac{1}{4}}_{\text{VI}\ \text{VI}} + \underbrace{\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}}_{\text{VI}\ \text{VI}\ \text{VI}\ \|} + \ldots = \infty$$

$$\underbrace{\frac{1}{2^1}}_{|} + \underbrace{\frac{1}{2}}_{\frac{1}{2}} + \underbrace{\frac{1}{4} + \frac{1}{4}}_{\frac{1}{2}} + \underbrace{\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}}_{\frac{1}{2}} + \ldots = \infty$$

∴ will have $\frac{1}{2}$ for infinity and the bottom is is at least great as above so above most ∞

Thm There are infinite #s of prime

pf (Euclid)

Suppose we had a finite list of primes, $p_1, \ldots, p_k$. and assume no other primes exist

suppose we are looking for # not divisible by 2, 3. Then, $2 \cdot 3 + 1 = 7$ is not divisible by 2 & 3

Note: $p_1 \cdot p_1 \cdot \ldots \cdot p_k + 1$

$N = p_1 \cdots p_k + 1$

By unique factorization, is a product of primes with a unit. ?

→ N is a fairly large number, and is not a unit

→ No prime on our list can divide N. So all the factors are off the list.

⇒ if you had finite list of primes, you have had to have another primes.

⇒ No finite list contains all primes

Euler Product

Recall $\frac{1}{1-x} = 1 + x + x^2 + \ldots$ — why doesn't pw series work if $x > 1$

then, $(1-x)(1+x+x^2+\ldots) = 1$

$$= \begin{array}{l} 1 + x + x^2 + \ldots \\ -x - x^2 - x^3 + \ldots \end{array} = 1$$

(proof ☐)

$$\prod_{\text{primes } p} \frac{1}{1-\frac{1}{p}} = \frac{1}{1-\frac{1}{2}} \cdot \frac{1}{1-\frac{1}{3}} \cdot \frac{1}{1-\frac{1}{5}} \cdot \frac{1}{1-\frac{1}{7}} \cdots$$

invoking Power Series

$$= \left(1+\tfrac{1}{2}+\tfrac{1}{4}+\ldots\right)\left(1+\tfrac{1}{3}+\tfrac{1}{9}+\ldots\right)\left(1+\tfrac{1}{5}+\tfrac{1}{25}+\ldots\right)\cdots$$

$$= 1+\tfrac{1}{2}+\tfrac{1}{3}+\tfrac{1}{4}+\tfrac{1}{5}+\tfrac{1}{6}+\ldots = \sum \frac{1}{n}.$$

($\frac{1}{2}$(1 in all others) ($\frac{1}{2}$, $\frac{1}{3}$ and $\frac{1}{5}$ in all others)

How can I know for certain that a particular $\frac{1}{n_k}$ appears only once... because they are primes? ~~Then, I should~~ Unique factorization?

Consequence

$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\ldots$ is still infinite.

Proof ?! BELIEVE!

DENSITY OF PRIMES

Q: How large, roughly, is the k-th prime number?

Thm Let π_k be the k^{th} prime number.

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

Nonetheless, it is entirely unknown how the gaps between prime numbers behave.

For example, a prime twin is a prime like 11 and 13 or 101 and 103. primes with difference of 2.

Q: Are there infinitely many twin primes?

(It is known that if you were to add that $\sum_{p=\text{twin}} \frac{1}{p} < \infty$

⇒ equivalent statement that $\frac{1}{p}$ isn't large since converge but twin primes does not.

?? So are the infinite twin primes?

prime triplets?

p, p+2, p+4 prime

apart from $p=3$, 3 cannot divide p.

after some thought, triplets don't exist unless $p=3$.

→ if I divide any p by 3, we have 2 cases

(1) Remainder of ~~3|p~~ $\frac{p}{3}$ is one. That means $p+2$ is divisible by 3. thus not a prime

(2) Remainder of $\frac{p}{3}$ is two. Than $p+4$ (remainder $2+4=6$) is divisible by 3 and this cannot be prime.

→ How about triples of ~~equiet~~ equidistance other than 2?

Thm If you look at an arthmetic pro? :

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

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

Then / triplets, quadruplets, ... exist if you make distance large

ex. 3, 7, 11 11, 17, 23

↳ equidistance of 4. ↳ equidistant of 6.

Larger the distance, longer ~~distance~~ sequence can be created.

=e.g. 10 sequence of primes of equidist. would need dist of ~10 billion

Open questions (Solve & be famous)

→ Is it possible to write each even integer >2 as a sum of two primes.

$4=2+2$, $6=3+3$ $8=3+5$ $20=3+17$ ... (Goldbach conjecture)

→ every integer ≥ 2 is a sum of at most 3 primes

→ $\frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{3^s}+\ldots$ (harmonic, modified) $= \xi(s)$

Riemann Zeta function

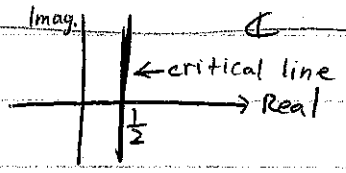
$s=1$ ⇒ zeta function has a pole? (diverge?)

$s=2,4$ (more generally, integer) the value of zeta shows up in physics

Q: Describe All poles of the zeta function (∞)

Generally belief about ζ:

if you allow s to be complex, then all (interesting) poles lie on the line $Re(s) = \frac{1}{2}$.



= Riemann Hypothesis (Clay Problem)

I like stories