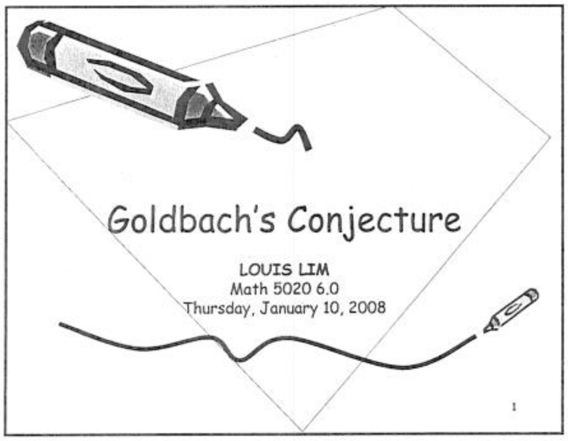
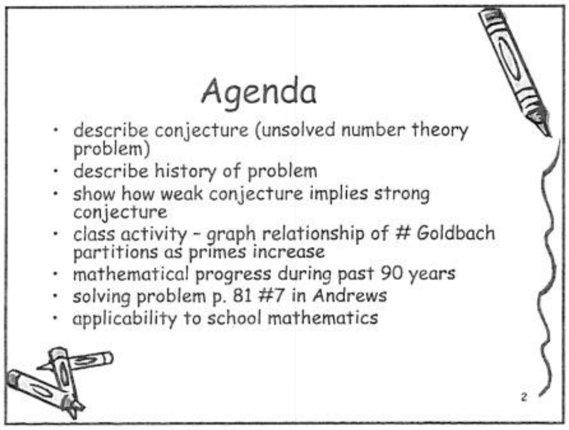


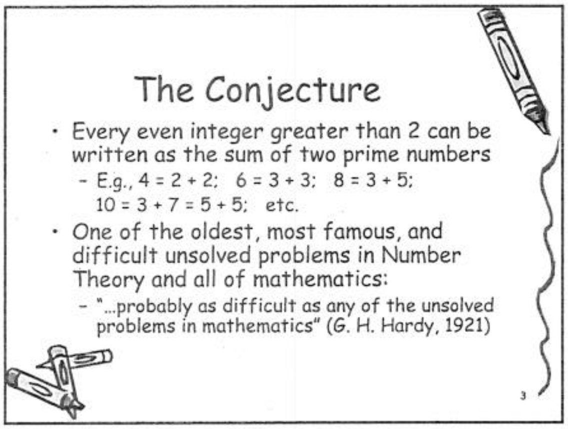
Goldbach's Conjecture

LOUIS LIM
Math 5020 6.0
Thursday, January 10, 2008



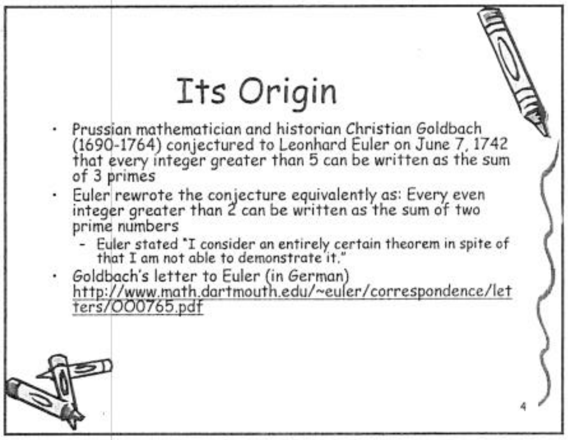
Agenda

- describe conjecture (unsolved number theory problem)
- describe history of problem
- show how weak conjecture implies strong conjecture
- class activity – graph relationship of # Goldbach partitions as primes increase
- mathematical progress during past 90 years
- solving problem p. 81 #7 in Andrews
- applicability to school mathematics



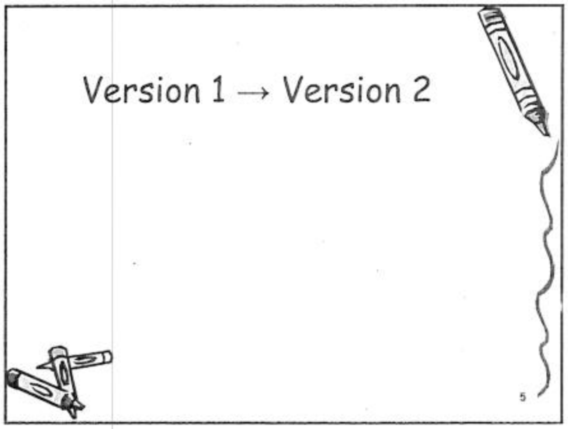
The Conjecture

- Every even integer greater than 2 can be written as the sum of two prime numbers
  - E.g., 4 = 2 + 2; 6 = 3 + 3; 8 = 3 + 5; 10 = 3 + 7 = 5 + 5; etc.
- One of the oldest, most famous, and difficult unsolved problems in Number Theory and all of mathematics:
  - "...probably as difficult as any of the unsolved problems in mathematics" (G. H. Hardy, 1921)

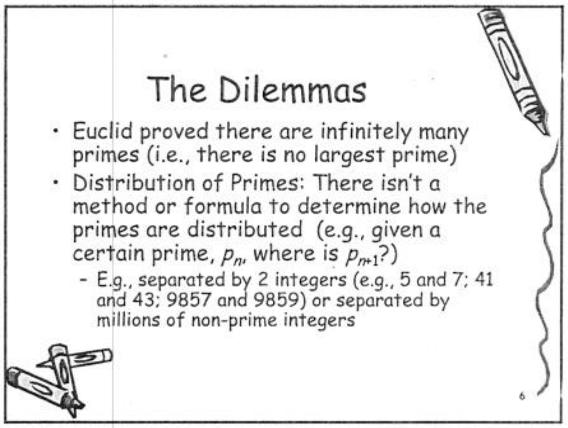


Its Origin

- Prussian mathematician and historian Christian Goldbach (1690-1764) conjectured to Leonhard Euler on June 7, 1742 that every integer greater than 5 can be written as the sum of 3 primes
- Euler rewrote the conjecture equivalently as: Every even integer greater than 2 can be written as the sum of two prime numbers
  - Euler stated "I consider an entirely certain theorem in spite of that I am not able to demonstrate it."
- Goldbach's letter to Euler (in German) http://www.math.dartmouth.edu/~euler/correspondence/letters/OO0765.pdf



Version 1 → Version 2



The Dilemmas

- Euclid proved there are infinitely many primes (i.e., there is no largest prime)
- Distribution of Primes: There isn't a method or formula to determine how the primes are distributed (e.g., given a certain prime, p_n, where is p_{n+1}?)
  - E.g., separated by 2 integers (e.g., 5 and 7; 41 and 43; 9857 and 9859) or separated by millions of non-prime integers

Activity 1

- For each even number, write all possible sums of 2 prime numbers.

4	6	8
10 = 3+7 = 5+5	12	14
16	18	20
22	24	26
28	30	32
34	36	38
40	42	44
	48	50

7

Defining $r(n)$

- Goldbach partition of n: Two primes (p, q) such that $p + q = n$, n is a positive even integer greater than 2
  - E.g., 11 and 13 is a Goldbach partition of 24
- Let $r(n)$ be the number of Goldbach partitions of n
- Goldbach's Conjecture is equivalent to the number of Goldbach partitions is > 0

8

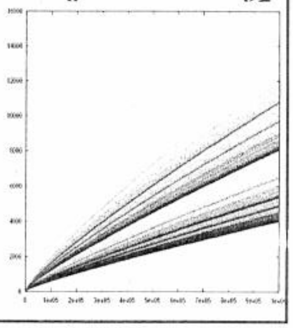
Activity 2

- Graph the relationship between:
  - the prime number (x-axis) and
  - number of Goldbach partitions of n, $r(n)$ (y-axis)

9

Progress: Using Computers to Support the Conjecture

- Graph shows number of ways to write an even number, n, as the sum of 2 primes ($4 \leq n \leq 1\,000\,000$)
- The likelihood of an even number being written as a sum of 2 primes increases as the even number becomes larger
- Graph known as "Goldbach's Comet"



... Progress

- "Such computations may also deepen insight into the problem and *could* possibly give a hint toward the proof or disproof of the Goldbach conjecture for the *infinite* set of all the even numbers." (Herman te Riele of the National Research Institute for Mathematics)

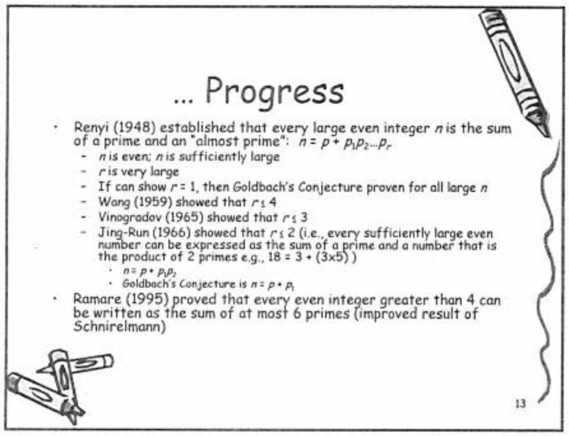
Verified to	
1×10^4	Desboves 1885
1×10^5	Pipping 1938
1×10^8	Stein & Stein 1965
2×10^{10}	Graville et al. 1989
4×10^{11}	Sinisalo 1993
1×10^{14}	Deshouillers et al. 1998
4×10^{14}	Richstein 1999
2×10^{16}	Oliveira e Silva 2003
6×10^{16}	Oliveira e Silva 2003
2×10^{17}	Oliveira e Silva 2005
3×10^{17}	Oliveira e Silva 2005
1×10^{18}	Oliveira e Silva 2007

11

... Progress

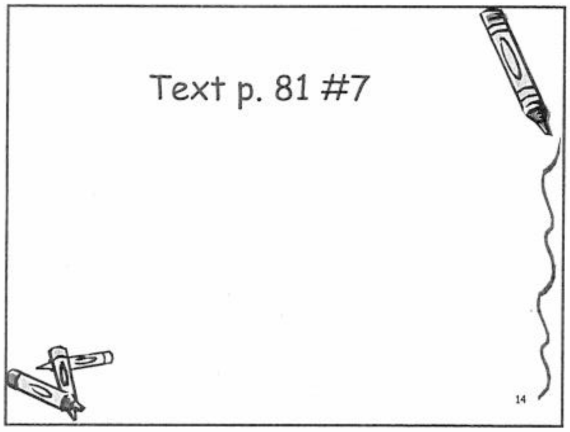
- Brun (1920) proved every sufficiently large even number can be written as the sum of 2 terms, where each has at most 9 prime factors
  - Brun developed an extension of the Sieve method of Eratosthenes
  - Buchstab (1940) improved Brun's result to 4 prime factors
- Lev Schnirelmann (1930) proved every even integer greater than 4 can be written as the sum of at most 300 000 primes
- Vinogradov (1937): Every sufficiently large (although not sure how large) odd number is a sum of 3 primes
- Borozdkin (1956) proved the sufficiently large odd number is less than 3^(3^15)
  - Chen & Wang (1989) reduced that to 10^43 000
  - Liu & Wang (2002) reduced further to e^3100

12

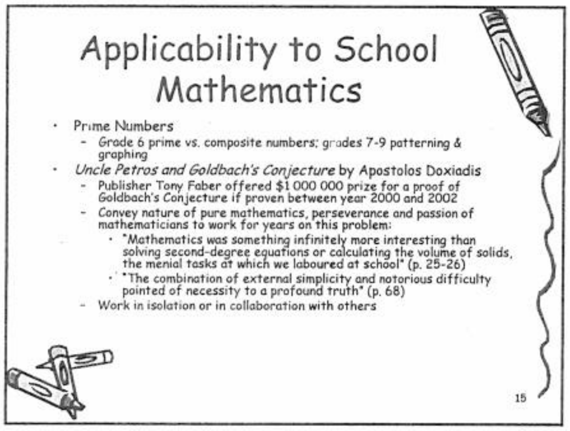


… Progress

- Renyi (1948) established that every large even integer n is the sum of a prime and an "almost prime": $n = p + p_1p_2...p_r$
  - n is even; n is sufficiently large
  - r is very large
  - If can show $r = 1$, then Goldbach's Conjecture proven for all large n
  - Wang (1959) showed that $r \leq 4$
  - Vinogradov (1965) showed that $r \leq 3$
  - Jing-Run (1966) showed that $r \leq 2$ (i.e., every sufficiently large even number can be expressed as the sum of a prime and a number that is the product of 2 primes e.g., 18 = 3 + (3x5))
    - $n = p + p_1p_2$
    - Goldbach's Conjecture is $n = p + p_1$
- Ramare (1995) proved that every even integer greater than 4 can be written as the sum of at most 6 primes (improved result of Schnirelmann)

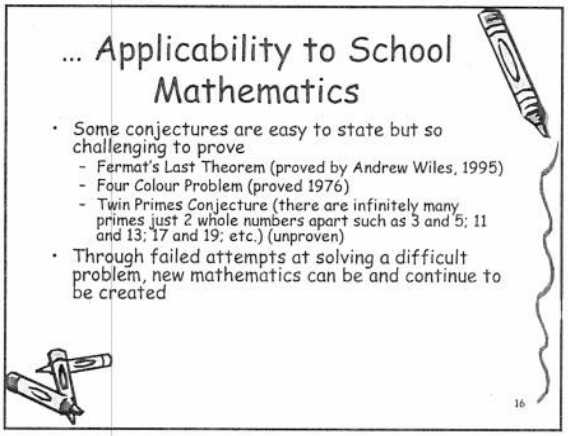


Text p. 81 #7



Applicability to School Mathematics

- Prime Numbers
  - Grade 6 prime vs. composite numbers; grades 7-9 patterning & graphing
- *Uncle Petros and Goldbach's Conjecture* by Apostolos Doxiadis
  - Publisher Tony Faber offered $1 000 000 prize for a proof of Goldbach's Conjecture if proven between year 2000 and 2002
  - Convey nature of pure mathematics, perseverance and passion of mathematicians to work for years on this problem:
    - "Mathematics was something infinitely more interesting than solving second-degree equations or calculating the volume of solids, the menial tasks at which we laboured at school" (p. 25-26)
    - "The combination of external simplicity and notorious difficulty pointed of necessity to a profound truth" (p. 68)
  - Work in isolation or in collaboration with others



… Applicability to School Mathematics

- Some conjectures are easy to state but so challenging to prove
  - Fermat's Last Theorem (proved by Andrew Wiles, 1995)
  - Four Colour Problem (proved 1976)
  - Twin Primes Conjecture (there are infinitely many primes just 2 whole numbers apart such as 3 and 5; 11 and 13; 17 and 19; etc.) (unproven)
- Through failed attempts at solving a difficult problem, new mathematics can be and continue to be created

Andrews Text page 81 #7:

C. Goldbach conjectured that every even number greater than 2 is a sum of two primes. P. Erdos conjectured that, for any even number $2n$, there exist integers q and r such that $\varphi(q) + \varphi(r) = 2n$. Does the conjecture of Goldbach imply that of Erdos?

Solution:

Recall that the Euler phi-function, $\varphi(n)$, is the number of positive integers not exceeding n that are relatively prime to n.

$\varphi(p) = p - 1$ for any prime p, since every integer $< p$ is relatively prime to it.

e.g., $\varphi(5) = 4$ since the positive integers not exceeding 5 that are relatively prime to 5 are 1, 2, 3, and 4.

For Goldbach's Conjecture, let $2n + 2$, with $n \geq 1$.

$2n + 2 = q + r$, where q and r are primes.

Since $\varphi(p) = p - 1$, then $\varphi(q) = q - 1$ or $q = \varphi(q) + 1$.
Further, $\varphi(r) = r - 1$ or $r = \varphi(r) + 1$

It follows that

$2n + 2$
$= q + r$
$= \varphi(q) + 1 + \varphi(r) + 1$
$= \varphi(q) + \varphi(r) + 2$

So, $2n = \varphi(q) + \varphi(r)$.

Activity 1

For each even number, write all possible sums of 2 prime numbers.

4 = 2+2	6 = 3+3	8 = 3+5
10 = *3* + *7* = *5* + *5*	12 = 5+7	14 = 7+7
16 = 13+3	18 = 13+5	20 = 13+7
22 = 11+11	24 = 11+13	26 = 13+13
28 = 11+17	30 = 17+13 = 11+19	32 = 13+19
34 = 5+29	36 = 13+23 = 17+19	38 = 19+19
40 = 11+29	42 = 31+11	44 = 31+13
46 = 23+23	48 = 29+19	50 = 19+31

Verison 1: Any integer greater than 5 can be written as the sum of 3 primes.

Version 2: Any even integer greater than 2 can be written as the sum of 2 primes.

We want to show that version 1 implies version 2.

Using a numerical example, let's first choose an even integer, say 6:

$6 = 2 + 2 + 2$	(version 1)
or $6 - 2 = 2 + 2$	
so $4 = 2 + 2$	(version 2)

Choosing an odd integer, say 7:

$7 = 2 + 2 + 3$	(version 1)
or $7 - 3 = 2 + 2$	(since we want the sum of 2 primes to be even)
so $4 = 2 + 2$	(version 2)

In general, we consider 2 cases: when the integer in version 1 is even and when the integer is odd

Case 1: integer, n, is even and greater than 5

$n = p_1 + p_2 + p_3$
Since n is even, then either (a) $p_1 = p_2 = p_3 = 2$ or (b) one of $p_1, p_2, p_3 = 2$ and the other 2 primes are odd

(a) $n = 2 + 2 + 2$	(version 1)
or $n - 2 = 2 + 2$	(version 2)

LHS is even.

(b) $n = 2 + p_2 + p_3$	(version 1)
or $n - 2 = p_2 + p_3$	(version 2)

LHS, $n - 2$, is even.
RHS is also even since the sum of 2 odd primes is even.

So, version 1 implies version 2 when the integer is even.

Case 2: integer, n, is odd and greater than 5

$n = p_1 + p_2 + p_3$
Since n is odd, then either (a) all p_1, p_2, p_3 are odd or (b) any two of $p_1, p_2, p_3 = 2$ and the other is odd

maassen ähnlich ist dem Fermatiano, dass $pp+qq+rr+ss$ alle mögliche Zahlen hervorbringe. Ich habe noch viel mehr dergleichen theoremata, als $3aa+3bb+7cc$ kann niemals ein quadratum seyn; item $2aa+6bb+21cc$ quadratum esse nequit und dergleichen. Ich habe aber noch keine dergleichen formulam finden können, in welcher 4 litterae a se invicem non pendentes enthalten wären.

Dass im Uebrigen meine jüngst überschickte Demonstration bei Ew. Beifall gefunden, erfreuet mich sehr. Dass aber diese Formul $(a+b)^p-a^p-b^p$ auch durch p oder einen divisorem des p, praeter unitatem, wenn p kein numerus primus ist, divisibilis seyn sollte, kann durch meine Demonstration nicht nur nicht erwiesen werden, sondern es trifft auch in vielen Fällen nicht zu. Als wenn $a=1$ et $b=1$, et $p=35$, so lässt sich $2^{35}-2$ weder durch 5 noch durch 7 theilen.

Wenn generaliter $a^{p\sqrt{-1}}+a^{-p\sqrt{-1}}=b$, so ist
$$a^{xp\sqrt{-1}}+a^{-xp\sqrt{-1}}=\left(\frac{b+\sqrt{(bb-4)}}{2}\right)^x+\left(\frac{b-\sqrt{(bb-4)}}{2}\right)^x,$$
und folglich, wenn $2^{p\sqrt{-1}}+2^{-p\sqrt{-1}}=3$, so wird $2^{xp\sqrt{-1}}+2^{-xp\sqrt{-1}}=\left(\frac{3+\sqrt{5}}{2}\right)^x+\left(\frac{3-\sqrt{5}}{2}\right)^x=\left(\frac{\sqrt{5}+1}{2}\right)^{2x}+\left(\frac{\sqrt{5}-1}{2}\right)^{2x}$. Somit kommen Ew. Observationen mit meinem General-theoremate, dass $a^{+p\sqrt{-1}}+a^{-p\sqrt{-1}}=2\cos.\text{Arc}.pla$ meistentheils überein, nur dass $2^{(4n+q)p\sqrt{-1}}+2^{-(4n+q)p\sqrt{-1}}$ nicht gleich ist $2^{qp\sqrt{-1}}+2^{-qp\sqrt{-1}}$, wenn nicht entweder $(2n+q)pl2$ oder $2npl2$ gleich ist $m\pi$ denotante $1:\pi$ rationem diametri ad peripheriam.

Euler.

LETTRE XLIII.

=

Goldbach à Euler.

Sommaire. Continuation sur les mêmes sujets. Deux théorèmes d'analyse.

Moscau d. 7 Juni n. st 1742.

— — — Ohngeachtet ich mich in meinem vorigen Briefe mit der particula vielleicht précautionniret, so hätte doch nicht geglaubet, dass die Formul $(a+b)^p-a^p-b^p$ sich nicht allezeit durch einen von den divisoribus numeri p sollte dividiren lassen, wenn solches nicht durch das von Ew. angeführte exemple deutlich bestätiget würde.

So viel ich mich erinnere, hatte ich mir in meinem letzten Briefe die Formul $2^{xp\sqrt{-1}}+2^{-xp\sqrt{-1}}$, posito $2^{p\sqrt{-1}}+2^{-p\sqrt{-1}}=0$, als applicatas einer curvae serpentiformis, deren abscissae x sind, vorgestellet, und welche den axem so oft durchschneidet, als die Formul $=0$ wird,

so dass, wenn die formula ipsa $= 2$ ist, die applicata maxima unten oder oben herauskommt, folglich unzählige andere applicatae unter sich gleich seyn müssen; nichts desto weniger ist in meiner damaligen Expression ein Fehler eingeschlichen, den Ew. mit Recht angemerket haben, und leicht verbessert werden kann, indem es heissen sollen, dass wenn q ein numerus quicunque und $2^{p\sqrt{-1}} + 2^{-p\sqrt{-1}} = 0$ gesetzet wird, alsdann posito pro n integro quocunque, seyn werde
$$2^{(8n-4-q)p\sqrt{-1}} + 2^{-(8n-4-q)p\sqrt{-1}} = 2^{qp\sqrt{-1}} + 2^{-qp\sqrt{-1}}.$$

Ew. haben gefunden, dass alle Zahlen, so nicht $4mn-m-n$ seyn können, in dieser Formul begriffen sind v^2+v+u^2, und ich finde, dass alle $4mn-m-n$ zu dieser Formul y^2+y-x^2 gebracht werden können, so dass eine jede gegebene Zahl gleich ist $p^2+p \pm q^2$, woselbst p et q numeros integros anzeigen, oder auch eine von beiden litteris 0 bedeuten kann; woraus zu sehen ist, dass eine jede Zahl aus einem duplo numeri triangularis ± numero quadrato bestehet. Weil aber auch eine jede Zahl gleich ist der Formul
$$u^2+v^2+v+y^2+y-x^2,$$
so wird, wenn man setzet $u = \frac{z^2+z}{4} + 1$, $x = \frac{z^2+z}{4} - 1$, $u^2 - x^2 = z^2 + z$, folglich jedes numeri dati dimidium
$$\frac{n}{2} = \frac{v^2+v+y^2+y+z^2+z}{2},$$
id est tribus trigonalibus.

Dass in der formula polygonalium $\frac{(p-2)x^2-(p-4)x}{2}$, wenn sie gleich werden soll $4mn-m-n$, p weder 5 ± 2 noch 5 ± 1 seyn könne, sondern alle trigonales, tetragonales, hexagonales und heptagonales ausgeschlossen werden, folget ex iisdem principiis.

Ich halte es nicht für undienlich, dass man auch diejenigen propositiones anmerke, welche sehr probabiles sind, ohngeachtet es an einer wirklichen Demonstration fehlet, denn wenn sie auch nachmals falsch befunden werden, so können sie doch zu Entdeckung einer neuen Wahrheit Gelegenheit geben. Des Fermatii Einfall, dass jeder numerus $2^{2^n-1}+1$ eine seriem numerorum primorum gebe, kann zwar, wie Ew. bereits gezeiget haben, nicht bestehen; es wäre aber schon was Sonderliches, wenn diese series lauter numeros unico modo in duo quadrata divisibiles gäbe. Auf solche Weise will ich auch eine conjecture hazardiren: dass jede Zahl, welche aus zweyen numeris primis zusammengesetzt ist, ein aggregatum so vieler numerorum primorum sey, als man will (die unitatem mit dazu gerechnet), bis auf die congeriem omnium unitatum *); zum Exempel

$$4 = \begin{cases} 1+3 \\ 1+1+2 \\ 1+1+1+1 \end{cases} \qquad 5 = \begin{cases} 2+3 \\ 1+1+3 \\ 1+1+1+2 \\ 1+1+1+1+1 \end{cases}$$

$$6 = \begin{cases} 1+5 \\ 1+2+3 \\ 1+1+1+3 \\ 1+1+1+1+2 \\ 1+1+1+1+1+1 \end{cases} \qquad \text{etc.}$$

*) Nachdem ich dieses wieder durchgelesen, finde ich, dass sich die conjecture in summo rigore demonstriren lässet in casu $n+1$, si successerit in casu n, et $n+1$ dividi possit in duos numeros primos. Die Demonstration ist sehr leicht. Es scheinet wenigstens, dass eine jede Zahl, die grösser ist als 1, ein aggregatum trium numerorum primorum sey.

Hierauf folgen ein Paar observationes, so demonstriret werden können:

Si ν sit functio ipsius x ejusmodi, ut facta $\nu = c$ numero cuicunque, determinari possit x per c et reliquas constantes in functione expressas, poterit etiam determinari valor ipsius x in aequatione $\nu^{2n+1} = (2\nu+1)(\nu+1)^{n-1}$.

Note marginale d'Euler:

$$\nu^{2n+1} - (\nu\nu+\nu)(\nu+1)^{n-1} \text{ divisib. per } \nu\nu-\nu-1$$
$$\text{addatur } (\nu\nu-\nu-1)(\nu+1)^{n-1}$$
$$\nu^{2n+1} - (2\nu+1)(\nu+1)^{n-1} \text{ divisib. per } \nu\nu-\nu-1.$$

Si concipiatur curva cujus abscissa sit x, applicata vero sit summa seriei $\frac{x^n}{n\,.\,2^{2n}}$, posita n pro exponente terminorum hoc est, applicata $= \frac{x}{1.2^2} + \frac{x^2}{2.2^4} + \frac{x^3}{3.2^6} + \frac{x^4}{4.2^8} +$ etc., dico, si fuerit abscissa $=$

1, applicatam fore $= \frac{1}{3}$ $\left\{ \begin{array}{l} = l\frac{4}{3}, \text{ nam sit haec applicata} = y, \\ \text{erit } y = l\cdot\frac{4}{4-x}. \quad \textit{Note marginale d'Euler} \end{array} \right\}$

2 . . . . $l2$

3 . . . . $2l2$

4 vel major . . . infinitam.

Goldbach.

P. S. Die beiden andern formulas numerorum non quadratorum, deren Ew. Erwähnung thun, habe ich noch nicht untersuchet, ich glaube aber, dass selbige, wenn man setzet

$$a = hx + k,\ \ b = lx + m,\ \ c = nx + p$$

sich wohl möchten unter nachfolgende Formul rangiren lassen, allwo $f,\ g,\ \gamma,\ \delta$ numeri integri affirmativi sind

$$\begin{array}{l} (2f - 4\gamma\delta)x^2 + 4(f - 2\gamma\delta)(2g - \delta^2)x + (2g - \delta^2)^2 \\ \quad -4\gamma^2 \qquad\qquad\qquad\qquad -2f \qquad\qquad\quad -2g \end{array}$$

denn diese kann niemals ein quadratum geben . . . . .

Positis m et p numeris integris affirmativis, haec expressio $\frac{p+2\pm\sqrt{(4p-m+3)}}{m}$ non potest fieri numerus integer.