The oldest open problem of mathematics

Oliver Knill, Harvard University
at Math Circle, Northeastern,
December 2, 2007
Perfect numbers
Perfect number

the sum of the proper divisors is the number itself.

6 = 1 + 2 + 3

28 = verify yourself

496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248
Why relevant?

Related to largest prime numbers known.

$2^{p-1} \left( 2^p - 1 \right)$ perfect

<table>
<thead>
<tr>
<th>$p$</th>
<th>digits</th>
<th>discovered</th>
<th>mersenne</th>
</tr>
</thead>
<tbody>
<tr>
<td>32582657</td>
<td>9808358</td>
<td>2006</td>
<td>44?</td>
</tr>
<tr>
<td>30402457</td>
<td>9152052</td>
<td>2005</td>
<td>43?</td>
</tr>
<tr>
<td>25964951</td>
<td>7816230</td>
<td>2005</td>
<td>42?</td>
</tr>
<tr>
<td>24036583</td>
<td>7235733</td>
<td>2004</td>
<td>41?</td>
</tr>
<tr>
<td>20996011</td>
<td>6320430</td>
<td>2003</td>
<td>40?</td>
</tr>
<tr>
<td>13466917</td>
<td>4053946</td>
<td>2001</td>
<td>39</td>
</tr>
</tbody>
</table>
Open problems

Is there an odd perfect number?

Are there infinitely many perfect numbers?

No other open problem in mathematics is older. The second problem is thousands of years old, the first might too but has been written down by Dequartes.
The sigma function
\[\sigma(n) = \sum_{d \mid n} d\]

\[\sigma(p) = 1 + p\]

\[\sigma(p^n) = 1 + p + p^2 + \ldots + p^n\]

\[\sigma(p^n q^m) = (1 + p + p^2 + \ldots + p^n)(1 + p + p^2 + \ldots + p^m)\]

\[\sigma(n) = \prod_{i=1}^{k} (1 + p + p^2 + \ldots + p^{m_i})\]

\(d \mid n\) means \(d\) divides \(n\)

\(p, q\) are prime
this is a multiplicative function:

\[ \sigma(ab) = \sigma(a) \sigma(b) \]

if \( a, b \) have no nontrivial common divisor.
\[ h(n) = \frac{\sigma(n)}{n} = 2 \]

Index function is also multiplicative.

\[ h(n) = \prod_{i=1}^{k} \left(1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \ldots + \frac{1}{p_i^{m_i}} \right) \]
can be close to 1 can also become arbitrarily large because

\[ \prod \left(1 + \frac{1}{p}\right) = 1 + \frac{1}{p} \]

\( p \) prime diverges.

graph of \( h \)
An odd perfect number has more than 2 prime factors.
Proof:

use the geometric series formula. A prime factor can contribute only up to \( \frac{1}{1-1/p} = \frac{p}{p-1} \)

\[
\begin{align*}
    h(n) &< \frac{p}{p-1} \cdot \frac{q}{q-1} \\
        &< \frac{3}{3-1} \cdot \frac{5}{5-1} = \frac{15}{8} < 2
\end{align*}
\]
How close can we get to 2 with $k$ prime factors?

Nice research project in experimental mathematics!
Descartes example

\[ n = 3^2 7^2 11^2 13^2 22021 \]

\[ (1 + 3 + 3^2) (1 + 7 + 7^2) \]
\[ (1 + 11 + 11^2) (1 + 13 + 13^2) \]
\[ (1 + 22021) = 2 \cdot n \]

We have found an odd perfect number, didn’t we?
... I think I am able to prove that there are no even numbers which are perfect apart from those of Euclid; and that there are no odd perfect numbers, unless they are composed of a single prime number, multiplied by a square whose root is composed of several other prime numbers.

But I can see nothing which would prevent one from finding numbers of this sort. For example, if 22021 were prime, in multiplying it by 9018009 which is a square whose root is composed of the prime numbers 3, 7, 11, 13, one would have 198585576189, which would be a perfect number.

But, whatever method one might use, it would require a great deal of time to look for these numbers...
Mathematicians
• 580-500 BC, born in Samos
• Mentions perfect numbers
Euclid of Alexandria

- 300–275 BC
- Found structure of even perfect numbers
Euclid’s Elements
Book IX
Proposition 36

If as many numbers as we please beginning from a unit are set out continuously in double proportion until the sum of all becomes prime, let the product of the sum multiplied into the last make some number, then the product is perfect.

Let as many numbers as we please, $A$, $B$, $C$, and $D$, beginning from a unit be set out in double proportion, until the sum of all becomes prime, let $E$ equal the sum, and let $E$ multiplied by $D$ make $FG$.

I say that $FG$ is perfect.

For, however many $A$, $B$, $C$, and $D$ are in multitude, take so many $E$, $HK$, $L$, and $M$ in double proportion beginning from $E$.

Therefore, *ex aequali* $A$ is to $D$ as $E$ is to $M$. Therefore the product of $E$ and $D$ equals the product of $A$ and $M$. And the product of $E$ and $D$ is $FG$, therefore the product of $A$ and $M$ is also $FG$.

Therefore $A$ multiplied by $M$ makes $FG$. Therefore $M$ measures $FG$ according to the units in $A$. And $A$ is a dyad, therefore $FG$ is double of $M$.

But $M$, $L$, $HK$, and $E$ are continuously double of each other; therefore $E$, $HK$, $L$, $M$, and $FG$ are continuously proportional in double proportion.

Subtract from the second $HK$ and the last $FG$ the numbers $HN$ and $FO$, each equal to the first $E$. Therefore the excess of the second is to the first as the excess of the last is to the sum of those before it. Therefore $NK$ is to $E$ as $OG$ is to the sum of $M$, $L$, $KH$, and $E$.

And $NK$ equals $E$, therefore $OG$ also equals $M$, $L$, $HK$, $E$. But $FO$ also equals $E$, and $E$ equals the sum of $A$, $B$, $C$, $D$ and the unit. Therefore the whole $FG$ equals the sum of $E$, $HK$, $L$, $M$, $A$, $B$, $C$, $D$, and the unit, and it is measured by them.

I say also that $FG$ is not measured by any other number except $A$, $B$, $C$, $D$, $E$, $HK$, $L$, $M$, and the unit.

If possible, let some number $P$ measure $FG$, and let $P$ not be the same with any of the numbers $A$, $B$, $C$, $D$, $E$, $HK$, $L$, or $M$.

And, as many times as $P$ measures $FG$, so many units let there be in $Q$, therefore $Q$ multiplied by $P$ makes $FG$.

But, further, $E$ multiplied by $D$ makes $FG$, therefore $E$ is to $Q$ as $P$ is to $D$.

And, since $A$, $B$, $C$, and $D$ are continuously proportional beginning from a unit, therefore $D$ is not measured by any other number except $A$, $B$, or $C$. 

Nicomachus of Gerasa

- 60–120 AD
- Introduction to Arithmetic
- Abundant and deficient numbers
NIKOMACHOY GErasingHOU
PYHAnOYIKOU
APHEOMATIKH EISAGOGH.

NICOMACHI Geraseni Pythagorei
INTRODUCTIONIS ARITHMETICAE LIBRI II.

RECENSIVIT
Ricardus Hoche.

ACCEDVNT CODICIS CIZENSIIS PROBLEMATA
ARITHMETICA.

Lipsiae
in aedibus B. G. Teubneri.
MDCCCLXVI.
Theon of Smyrna

- 70–135 AD
- Music of Spheres
- Abundant and deficient numbers
Dickson mentions Kings II, 13,19

but even the Hebrew text does not seem to mention perfect numbers.

Some religious context is because 6 is the number of days in which God created the world.

Some astronomical context comes from the fact that the moon month is 28 days.
Thabit ibn Qurra

- 836–901 AD
- Amicable numbers
Marin Mersenne

- 1588-1648
- tried to get formula for all primes
- studied primes of the form $2^p - 1$
Rene Descartes

- 1596-1650
- almost perfect numbers
- 4’th and 5’th perfect number

6,28,140,270,496,672 ...
Leonard Euler

- 1707-1783
- classification of even perfect numbers
- odd perfect numbers are product of special prime and square.
Benjamin Peirce

A local!

- 1809-1880
- At least 4 prime factors
James Joseph Sylvester

- 1814-1897
- Series of papers
Oystein Ore

- 1899-1968
- Harmonic integers
Quotes
Leonard Euler:

Whether ... there are any odd perfect numbers is a most difficult question.
J. J. Sylvester

“The existence of an odd perfect number -- its escape, so to say, from the complex web of conditions which hem it in on all sides -- would be little short of a miracle.”
"Perfect numbers certainly never did any good but then they never did any particular harm"
“Maybe some simple combination of a dozen or so primes in fact yield an odd perfect number!”
Conway and Guy

“There probably aren’t any!”
"This is probably the oldest unsolved problem in all of mathematics."
T.M. Putnam in 1910:

“It is a problem of much historic interest.”
“It is one of the oldest unsolved mysteries of mathematics, as it goes back to the ancient Greeks.”
Ribenboim

“I think the problem stands like an unconquerable fortress.”
Even perfect numbers
Theorem (Euclid-Euler)

$n$ is an even perfect number if and only if

$$n = 2^{p-1} (2^p - 1)$$

where $2^p - 1$ is prime.

$2^p - 1$ is called a Mersenne prime.
Proof by Stan Wagon in Intelligencer:

There is a one–one correspondence between even perfect numbers and Mersenne primes.

Suppose $2^n - 1$ is prime. Then $\sigma(2^n - 1) = \sigma(2^n - 1) = 1 + 2 + \ldots + 2^{n-1} = 2 \cdot 2^{n-1} (2^n - 1)$. Conversely (this proof is due to Dickson), suppose $2^{n-1}m$ is perfect, where $n > 1$ and $m$ is odd. Then $2^n m = \sigma(2^{n-1}m) = (2^n - 1)\sigma(m)$, whence $\sigma(m) = m + m/(2^n - 1)$. But then both $m$ and $m/(2^n - 1)$ are integers dividing $m$, so the expression for $\sigma(m)$ yields that $m/(2^n - 1) = 1$ and $m$ has no proper divisors. Thus $m = 2^n - 1$ is prime, as desired.
The currently largest known prime number has 9,808,358 digits. The Electronic Frontier Foundation offers a $100,000 award for the first 10 million digit prime. The GIMPS project is working on that. A new prime is now expected any moment.

**Search Status**

September 2006: New Mersenne Prime!

The page summarizes the current search status for Mersenne numbers with exponents below 79,300,000. The PrimeNet server also has a status page updated every hour.

It can easily be proven that a Mersenne prime must have a prime number as an exponent. This table summarizes the current search status of Mersenne numbers with prime exponents.

<table>
<thead>
<tr>
<th>Range</th>
<th>Mersenne</th>
<th>Composite</th>
<th>Status Unknown</th>
<th>Expected New Primes</th>
<th>P-90 CPU Years</th>
<th>PI-400 Speed (sec.)</th>
<th>FFT Size (in K)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>High</td>
<td>Numbers</td>
<td>Primes</td>
<td>Factored</td>
<td>TwoLL</td>
<td>OneLL</td>
<td></td>
</tr>
<tr>
<td>0,000,000</td>
<td>15,000,000</td>
<td>988,851</td>
<td>36</td>
<td>627,356</td>
<td>361,446</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>15,000,000</td>
<td>17,850,000</td>
<td>153,447</td>
<td>0</td>
<td>96,036</td>
<td>55,490</td>
<td>1,921</td>
<td>0</td>
</tr>
<tr>
<td>17,850,000</td>
<td>20,400,000</td>
<td>152,058</td>
<td>0</td>
<td>95,591</td>
<td>37,998</td>
<td>18,464</td>
<td>5</td>
</tr>
<tr>
<td>20,400,000</td>
<td>25,350,000</td>
<td>252,031</td>
<td>2</td>
<td>184,100</td>
<td>2,292</td>
<td>105,396</td>
<td>239</td>
</tr>
<tr>
<td>25,350,000</td>
<td>30,150,000</td>
<td>260,298</td>
<td>1</td>
<td>175,629</td>
<td>1,999</td>
<td>98,894</td>
<td>2,769</td>
</tr>
<tr>
<td>30,150,000</td>
<td>40,250,000</td>
<td>265,825</td>
<td>2</td>
<td>179,010</td>
<td>2,228</td>
<td>95,470</td>
<td>9,115</td>
</tr>
<tr>
<td>35,100,000</td>
<td>50,000,000</td>
<td>265,420</td>
<td>0</td>
<td>184,190</td>
<td>639</td>
<td>66,158</td>
<td>44,445</td>
</tr>
<tr>
<td>40,250,000</td>
<td>50,000,000</td>
<td>353,232</td>
<td>0</td>
<td>327,241</td>
<td>2</td>
<td>387</td>
<td>225,602</td>
</tr>
<tr>
<td>40,250,000</td>
<td>50,000,000</td>
<td>527,413</td>
<td>1</td>
<td>300,868</td>
<td>1</td>
<td>7</td>
<td>226,537</td>
</tr>
<tr>
<td>50,000,000</td>
<td>69,100,000</td>
<td>509,696</td>
<td>0</td>
<td>303,873</td>
<td>1</td>
<td>13</td>
<td>235,779</td>
</tr>
<tr>
<td>69,100,000</td>
<td>79,300,000</td>
<td>562,700</td>
<td>0</td>
<td>318,804</td>
<td>0</td>
<td>8</td>
<td>243,888</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td>4,950,918</td>
<td>44</td>
<td>2,792,704</td>
<td>462,098</td>
<td>387,690</td>
<td>988,379</td>
</tr>
</tbody>
</table>
100,000,000 dollars
Why not try?

Let's see what a linear extrapolation from previous data tells us on where the next prime will be.
$\log(p)$

$2^p - 1$

Mersenne prime

$(2^p - 1)2^{p-1}$

perfect $p$
Where is the next?

Have a line:

$$g(x) = 0.531876 + 0.394198x$$

Predict next Mersenne prime near $$p = \exp(g(45)) = 85731939$$
How large do we expect the next Mersenne prime to be?

Predict next Mersenne prime with $p$ near $\exp(g(45)) = 85731939$

Next has 25.8 Million digits

85731913 is closest prime
How does GIMPS search for Mersenne primes?

Lucas - Lehmer test:

Define $S(0) = 4$, $S(n+1) = S(n)^2 - 2$

$M(n) = 2^n - 1$ is prime

$\uparrow$

$M(n)$ divides $S(n)$
A mystery!
(with an easy proof)
All the Mersenne primes are the sum of odd consecutive cubes. See Pickover's book: wonders of numbers/

\[28 = 1 + 3^3\]
\[496 = 1 + 3^3 + 5^3 + 7^3\]

etc. There is a very easy explanation for that. Can you find it?
Odd perfect numbers
Theorem (Euler)

If $x$ is an odd perfect number then

$$x = p \cdot q^2$$

where $p$ is a prime and $q$ is an integer.

$p$ is called the special prime.
What else is known?

• n must have at least 300 digits.

• n must have a prime power factor with at least 12 digits and a prime factor with at least 8 digits.

• n gives rest 1 when divided by 12 or rest 9 when divided by 36. (this is easy to prove)

• if there are k distinct prime factors then $n < 4^k$
Ore harmonic numbers
Harmonic mean

\[ H(a,b) = \frac{2}{\frac{1}{a} + \frac{1}{b}} \]

Example:

\[ H(3,5) = \frac{1}{3} + \frac{1}{5} = 3 \frac{3}{4} \]

\[ A(a,b) = \frac{(a+b)}{2} \]

\[ G(a,b) = \sqrt{ab} \]

H < G < H

G^2 = A \times H
Ore harmonic number

The harmonic mean of all the divisors is an integer.

Example: 140. The harmonic mean of its proper divisors is 5.

1, 2, 4, 5, 7, 10, 14, 20, 28, 45, 70, 140.
Theorem (Ore)

Every perfect number is harmonic
Proof: \[ A \cdot H = n \]

H harmonic mean

A arithmetic mean

\[ H = \frac{k}{\frac{1}{d_1} + \ldots + \frac{1}{d_k}} \quad A = \frac{d_1 + \ldots + d_k}{k} = \frac{2n}{k} \] (perfect)

Use: \[ \frac{n}{d_1} + \ldots + \frac{n}{d_k} = d_1 + \ldots + d_k \] (n/d is again a divisor)

So \( (2n/k) \cdot H = n \) which implies \( H = k/2 \)

But k, the number of divisors of n is always even, if n is not a square or 2 times a square.

Squares or 2 times a square can not be perfect. (We know the even perfect numbers and odd squares satisfy \( \sigma(n) \) odd.)
The Ulam spiral
Ulam prime spiral
Color number of divisors
number of divisors gives color
Protected by the faith of one man.
Catalan-Dickson conjecture
Define \( T(x) = \sigma(x)-x \), which is the sum over all proper factors of \( x \). Define also \( T(0)=0 \).

Catalan-Dickson Conjecture: all orbits of \( T \) are bounded.

about 1 percent of orbits do not terminate in the available limit of time
Fixed points: perfect numbers
period 2 points: amicable pairs
primes are in the domain of attraction of 1, unbounded orbit?
There are “drivers” which produce growth. Guy tends to believe that orbits are not bounded in general.
Amicable pairs

<table>
<thead>
<tr>
<th>220</th>
<th>284</th>
</tr>
</thead>
<tbody>
<tr>
<td>284</td>
<td>220</td>
</tr>
<tr>
<td>1184</td>
<td>1210</td>
</tr>
<tr>
<td>1210</td>
<td>1184</td>
</tr>
<tr>
<td>2620</td>
<td>2924</td>
</tr>
<tr>
<td>2924</td>
<td>2620</td>
</tr>
<tr>
<td>5020</td>
<td>5564</td>
</tr>
<tr>
<td>5564</td>
<td>5020</td>
</tr>
<tr>
<td>6232</td>
<td>6368</td>
</tr>
<tr>
<td>6368</td>
<td>6232</td>
</tr>
</tbody>
</table>

Here are the first few:
Figure 1.5. The cover of Thabit’s book on amicable numbers (by courtesy of Guedj [85]).
cube root of n’th amicable number $a(n)$

only upper bounds are known. Pomerance showed $a(n) < n \exp(-\log(n)^{1/3})$
The large law of small numbers
Richard Guy’s law of small numbers:

You can’t tell by looking at a few examples.

Superficial similarities spawn spurious statements.

Capricious coincidences cause careless conjectures.

Early exceptions eclipse eventual essentials.

Initial irregularities inhibit incisive intuition.
Example 1:

31,331, 3331,33331,333331,3333331, etc are all prime
Example 2:

\[ 2^{2^n} + 1 \] are all prime

- \( F(0) = 3 \)
- \( F(1) = 5 \)
- \( F(2) = 17 \)
- \( F(3) = 257 \)
- \( F(4) = 65537 \)

- \( F(6) = 18446744073709551617 \)
  = \( 274177 \times 67280421310721 \)

- \( F(7) = 340282366920938463463374607431768211457 \)
  = \( 5704689200685129054721 \times 59649589127497217 \)
Example 3:

\[ \gcd(n^{17} + 9, (n+1)^{17} + 9) = 1 \]

First counter example:

\[ n = 8424432925592889329288197322308900672459420460792433 \]
Note: This is a number with 51 digits. Our universe is estimated to be 10^{10} seconds old. Even if we could check 10^{10} numbers per second, we would never get through.
note: this is a number with 51 digits.  Our universe is estimated to be $10^{10}$ seconds old. Even if we could check $10^{10}$ numbers per second, we would never get through.
Example 4: A open problem by Guy: (a case for the law?)

Is for prime $p$, the number $2^p - 1$ square free?
Examples:

$2^{37} - 1 = 223 \times 16318177$

$2^{37} - 1 = 1504073 \times 20492753 \times 59833457464970183^* 
467795120187583723534280000348743236593$

It's true of course for Mersenne primes ...
Number of prime factors of $2^p - 1$
Example 5:

All amicable pairs are either both even or both odd.

This is an open problem.

12285 is the first odd pair. When looking at the first few examples, one could have conjectured that all amicable pairs are both even.
Example 6:

Even perfect numbers have a decimal expansion ending by 6 or 8

6
28
496
8128
33550336
855969056
137438691328

2305843008139952128
2658455991569831744654692615953842176
191561942608236107294793378084303638130997321548169216
13164036458569648337239753460458722910223472318386943117783728128
14474011154664524427946373126085988481573677491474835889066354349131199152128

23562723457267347065789548996709904988477547858392600710143027597506337283178622
23973036553960260056136025556646250327017505289257804321554338249842877715242701
0394496186640286445342803383143979023683862403317114359223566432197031017207131
635274872987474006478019395871659364010874193756490518549492160555646976

14105378370671206906320795808606318988148674351471566783883867599995486774265238
011410419332903769025156195056870982932716408772243663700871167312681593136524874
50652439805877296207297446723295166658228846926807786652870188920867879451478364
56931392206037069506473607357237869517647305526682625328488638371507297432446383
5300053138429460296575143368065570759537328128
A warning to the end:

The subject of perfect numbers is not a good subject to focus its research on. It is tasty and like eating chocolate not very healthy. Successful researchers in that field use it as a topic of many topics in mathematics or as an illustration for other mathematics. I used it here as an illustration of the language of dynamical systems theory.

Also, nobody would be as foolish as admitting that they are trying to settle the oldest problem of mathematics. The risk is too big to be treated as a crackpot. I myself swear that I never attempted to work on the conjecture ...
The end.