User group for PFGW & PrimeForm programs

Public Group, 1012 members

Pierpont primes

Chris Caldwell Message 1 of 3 , Oct 25, 2005

I was reading my copy of the new American Mathematical Monthly. David Cox and Jerry Shurman wrote an interesting article on "Geometry and Number Theory on Clovers". It generalizes both Gauss' proof that you can subdivide a circle into n parts using ruler and compass iff n is a power of two times a product of distinct Fermat primes and Pierpont's 1895 result that you can divide a circle into n parts using origami if and only if n is a product of a power of two times a power of three times a distinct product of primes of the form 2^n*3^m+1. (These primes are now called Pierpont primes.)

But here is the funny part, on page 3 of this fine article they write:

Gleason suggests that there may be infinitely many Pierpont
primes, although only finitely many have been found so far.

"Only finitely many found," grin, that is true for primes in general! so for every defined type of primes! Then they continue the unintended humor with

According to Sequence A005109 of Sloane's... the only known
Pierpont primes form the set:

Here they list the 40 such primes below 1,000,000 as if somehow this could possibly be all
known Pierpont primes! Sometimes excellent mathematicians do not pause to think about the computational questions.

The Wikipedia article http://en.wikipedia.org/wiki/Pierpont_prime does a little better:

As of 2005, the largest known Pierpont prime is 33853318889473 .

and then misstates Pierponts theorem. But of course we expect much less from Wikipedia.

Both statement are obviously silly. It is trivial to find bigger Pierpont primes. Here are a couple quick (to program) counts I did with pari's isprime:

```
------ --------------
Pierpont primes
N below N
------ --------------
10^1 2
10^2 8
10^4 23
10^8 56
10^16 123
10^32 248
10^64 503
10^128 1018
10^256 2073
10^512 4225
------ --------------
```

I used doubling exponents to show clearly the number Pierpont primes (appear to) grow with the simple pattern you'd expect. I used ispseudoprime to calculate the value to 10^1024, but turned the machine off without recording the result. I guess more than 40 are

David Broadhurst Oct 25, 2005

View Source

Chris

> I was reading my copy of the new American Mathematical Monthly

That reminds me. I have doubts whether Euclid did actually
prove the infinitude of the primes, since I could not
find a good proof of unique factorization in the Elements.

It seems that

http://www.maa.org/pubs/monthly_mar06_toc.html

will address this point:

Did Euclid Need the Euclidean Algorithm to
Prove Unique Factorization?
By David Pengelley and Fred Richman
davidp@..., richman@...
Euclid proved that if a prime divides the product of two numbers,
then it divides one of them. Or did he? We investigate what appears
to be a serious gap in Euclid's proof.

David

Phil Carmody Message 3 of 3 , Oct 27, 2005

View Source

> From: Chris Caldwell <caldwell@...>
...
> The Wikipedia article http://en.wikipedia.org/wiki/Pierpont_prime does a
> little better:
>
> As of 2005, the largest known Pierpont prime is 33853318889473 .
>
> and then misstates Pierponts theorem. But of course we expect much less from
> Wikipedia.
>
> Both statement are obviously silly. It is trivial to find bigger Pierpont
> primes. Here are a couple quick (to program) counts I did with pari's
> isprime:

Can I recommend a site which lists some large examples:

http://primepages.org/

rank prime digits who when
16 3 · 2^2478785+1 746190 g245 Oct 2003
18 3 · 2^2145353+1 645817 g245 Feb 2003

And regarding any possibility of a finite quantity, these things are
_3_ times more likely to be prime than arbitrary numbers of the same size!
(Well, they're neither even nor divisible by 3.)

Phil

() ASCII ribbon campaign () Hopeless ribbon campaign
/\ against HTML mail /\ against gratuitous bloodshed

[stolen with permission from Daniel B. Cristofani]