Re: Probable Prime Number

Source: http://sci.tech−archive.net/Archive/sci.math/2006−09/msg05693.html

- *From*: mjtg@xxxxxxxxxxxxx (M.J.T. Guy)
- *Date*: 28 Sep 2006 12:58:52 GMT

In article <17937020.1159429765953.JavaMail.jakarta@xxxxxxxxxxxxxxxxxxxxxx>,
bassam king karzeddin <bassam@xxxxxxxxxx> wrote:

> Dear All
>
> I would like to introduce the following conjecture about prime factorization without having a proof or a counter example or a reference.
>
> The Conjecture:
>
> "If, n = (p^2 + q^2) / 2, where, (p, q) are odd prime numbers, then, (n) has at most three distinct odd prime numbers factors"

Obviously false. Instead we have:

Given any set of primes p_1, ... p_k each of the form 4a+1, we can find infinitely many n = (p^2 + q^2)/2 with p, q prime and n divisible by all the p_i.

Proof: First we find a solution without the condition that p, q be prime. We can express 2*p_i as a sum of squares, so we can find a suitable n for each primne separately. If (p, q) gives a solution, so does (p + a*p_i, q + b*p_i) for all (a, b). So we can combine the individual solutions using the Chinese Remainder Theorem to find an n divisible by S = p1*p2*...*p_k.

If (p, q) is a solution, so is (p + a*S, q + b*S), so we can find infinitely many solutions with (p, q) prime, since there are infinitely many primes in each of the arithmetic series p + a*S and q + b*S.

Mike Guy
.