

Re: Number with $4k+1$ prime.

Source: <http://sci.tech-archive.net/Archive/sci.math/2007-10/msg04597.html>

- *From:* magidin@xxxxxxxxxxxxxxxxxxxx (Arturo Magidin)
 - *Date:* Thu, 25 Oct 2007 13:57:44 +0000 (UTC)
-

In article <ffq4hc\$n4g\$1@xxxxxxxxxxxxxxxxxxxx>, mina_world <mina_world@xxxxxxxxxxxx> wrote:

Hello sir~

Prove that there are infinitely many primes of the form $4k+1$.

1)
Suppose that there are finite primes of the form $4k+1$.
Namely, q_1, q_2, \dots, q_r

As in the proof that there are infinitely many primes, there is no need to do this by contradiction. Simply show that given any finite list of primes congruent to 1 modulo 4, there is a prime not on the list that is also congruent to 1 modulo 4. That is what you do below anyway.

$$\text{Let } N = [2 \cdot (q_1) \cdot (q_2) \cdot \dots \cdot (q_r)]^2 + 1$$

so, N is odd.
so, $p \mid N$ for some odd prime p .
so, $[2 \cdot (q_1) \cdot (q_2) \cdot \dots \cdot (q_r)]^2 + 1 \equiv 0 \pmod{p}$
so, $[2 \cdot (q_1) \cdot (q_2) \cdot \dots \cdot (q_r)]^2 \equiv -1 \pmod{p}$

Namely, -1 is a quadratic residue modulo p since $(-1, p) = 1$.

so, $1 = (-1 / p) = (-1)^{\{(p-1)/2\}}$
so, $(p-1)/2 = 2k$
so, $p = 4k + 1$.

so, $p \in \{q_1, q_2, \dots, q_r\}$
Since $p \mid N$, $p \mid 1$. contradiction.

Since $p \equiv 1 \pmod{q_i}$ for each i , p is not equal to q_i for any i ...

Re: Number with $4k+1$ prime.

2)

Lemma)

Suppose that $p \mid (a^2) + 1$ for some odd prime p and some integer a .

Then $(a^2) + 1 = 0 \pmod{p}$

so, $a^2 = -1 \pmod{p}$

so, $a^4 = 1 \pmod{p}$

so, the order of a is 1 or 2 or 4 modulo p .

1 and 2 are impossible.

so, the order of a is 4 modulo p .

so, $4 \mid (p-1)$ --- (***)

so, $p = 4k + 1$

Suppose that there are finite primes of the form $4k+1$.

Namely, q_1, q_2, \dots, q_r

Let $N = [2 \cdot (q_1) \cdot (q_2) \dots (q_r)]^2 + 1$

so, N is odd.

so, $p \mid N$ for some odd prime p .

By lemma, $p \mid N$ for $p = 4k+1$ form.

so, $p \mid 1$. contradiction.

As above. You can do this directly instead of by contradiction.

I can understand (1).

But I can't understand (***) of (2).

Consider the multiplicative group of nonzero integers modulo p . It has $p-1$ elements. Since a is of order 4 modulo p , that means that the order of a in $(\mathbb{Z}_p)^*$ is 4. By Lagrange's Theorem, 4 must divide the number of elements in $(\mathbb{Z}_p)^*$, which is $p-1$. Thus, $4 \mid p-1$, which is (***) .

Because, I did not suppose the condition $(a, p) = 1$.

Of course you did. If $p \mid a^2+1$, then you must have $(a,p)=1$; otherwise, $p \mid 1$.

Re: Number with $4k+1$ prime.

Re: Number with $4k+1$ prime.

Even if I supposed the condition $(a,p) = 1$,
I can't use this problem.
Because, I can't guarantee $(2.(q_1).(q_2)...(q_r) , p) = 1$.

Yes, you can. Since $p \mid (2.(q_1)...(q_r))^2 + 1$, you must have that p is relatively prime to $2.(q_1)...(q_r)$. Otherwise, the prime p would divide 1.

=====
"It's not denial. I'm just very selective about
what I accept as reality."
--- Calvin ("Calvin and Hobbes" by Bill Watterson)
=====

Arturo Magidin
magidin-at-member-ams-org

.