# mathblag

*Musings on mathematics and teaching.*

## Primes of the form 6k+1

### by David Radcliffe

Euclid's proof of the infinitude of primes is justly famous. Here is one version of this proof:

Let P be a finite set of primes, and let N be the product of the numbers in P. Then N+1 is not divisible by any number in P, since it leaves a remainder of 1. But N+1 must be divisible by at least one prime, so P cannot contain all of the primes. Therefore the set of primes is infinite.

A variation of this argument shows that there are infinitely many primes of the form $6k-1$.

Let P be a finite set of primes of the form $6k-1$, and let N be the product of the primes in P. Consider the number $6N-1$. It is not divisible by 2 or 3, nor is it divisible by any number in P. But it is not possible that all prime factors of $6N-1$ have the form $6k+1$, because the product would have the form $6k+1$ as well.

Therefore, $6N-1$ has at least one prime factor of the form $6k-1$ that does not belong to P. Therefore, P cannot contain every prime of the form $6k-1$, so the set of primes of this form is infinite.

It takes a little bit more work to prove that there are infinitely many primes of the form $6k+1$. Here is a proof of that fact.

Let P be a finite set of primes of the form $6k+1$, and let N be a number that is divisible by every number in P. Assume that N is also divisible by 6. Let p be a prime divisor of $N^2-N+1$.

Note that $(N^2-N+1)(N+1)=N^3+1$. so p divides $N^3+1$, or in other words $N^3\equiv -1 \pmod p$ and so $N^6\equiv 1 \pmod p$.

Recall that the order of N modulo p is the least positive k so that $N^k\equiv 1 \pmod p$. The order must divide 6. so k = 1, 2, 3, or 6. But $N^3\equiv -1 \pmod p$, so the order cannot be 1 or 3.

Can the order be 2? If $N^2\equiv 1 \pmod p$ and $N^3\equiv -1 \pmod p$ then $N\equiv -1 \pmod p$. This would be bad, because then p would divide both $N+1$ and $N^2-N+1$; but $\gcd(N+1, N^2-N+1)=\gcd(N+1,3)<p$, contradiction.

Thus N has order 6 mod p, and the group of units mod p has order $p-1$, so 6 divides $p-1$, which means that p has the form $6k+1$. Therefore, P does not contain all primes of the form $6k+1$, so the set of primes of this form is infinite.

PUBLISHED: August 30, 2013 (2013-08-30T02:49:52-0500)
FILED UNDER: Uncategorized

## One Comment to “Primes of the form 6k+1”

**David Feldmann** says:
*December 15, 2013 at 3:47 pm*
Your proof of 6k+1 case is cool, but here is a shorter way:

We claim that it suffices to prove that there are infinitely many primes of the form 3k+1. This is obvious: a prime that is 3k+1 but not 6k+1 is necessarily 6k+4 and thus necessarily even.

Suppose finitely many primes 3k+1, say p_1, …, p_n. Then consider (p_1 … p_n)^2 + 3. If p is a prime factor, then, -3 is a quadratic residue modulo p.

Notice that -3 is a quadratic residue modulo a prime p if and only if p = 1 (mod 3).

Thus, p, which is not any of the p_i, is 1 (miod 3), contradiction.

REPLY