# Infinitely Many Primes 1 and 4 mod 15

Uthsav Chitra

August 27, 2014

## 1 Primes 1 mod 15

First, to show that 1 mod 15 case, we present the proof that there are infinitely many primes 1 mod $n$ for any $n > 1$, and then set $n = 15$.

Let $n$ be an integer greater than 1. For the sake of contradiction, suppose there are a finite number of primes 1 mod $n$. Define $S = \{\text{primes } p > 0 : p \equiv 1 \pmod{n}\}$. Aince $S$ is finite, let $P$ be the (finite) product of all elements of $S$. Then, one can consider the evaluation of $n$-th cyclotomic polynomial at $lP$, $\Phi_n(lP)$, where $l$ is a positive integer such that $\Phi_n(lP) > 1$ (such an $l$ surely exists since the coefficient of the highest-order term of $\Phi_n(x)$ is 1. Note that, since the constant term of $\Phi_n(x)$ is $\pm 1$, $p \nmid \Phi_n(x)$ for all $p \in S$.

Now, let $q$ be a (possible the?) positive prime factor of $\Phi_n(lP)$. Thus, $\Phi_n(lP) \equiv 0 \pmod{q}$. Since $\Phi_n(x) | x^n - 1$, we have that $(lP)^n - 1 \equiv 0 \pmod{q} \Rightarrow (lP)^n \equiv 1 \pmod{q}$, so the order of $lP$ (modulo $q$) divides $n$. Note that, if the order of $lP$ is equal to $n$, then by Fermat's Little Theorem we have that $n|q-1 \Rightarrow q \equiv 1 \pmod{n}$. Because $q|\Phi_n(P)$, this means that $q \notin S$. However, since $S$ was supposed to be the set of *all* positive primes $1 \pmod{n}$, this is a contradiction! Thus, all we have to do is show that the order of $lP$ is $n$.

It's here that we use the key fact about cyclotomic polynomials: for all positive integers $n$, $x^n - 1 = \prod_{\substack{d|n \\ d<n}} \Phi_d(x) \cdot \Phi_n(x)$. Thus, if the order of $lP$ were $d$ (where $d$ is a proper factor of $n$), then we would have $(lP)^d - 1 \equiv 0 \pmod{q}$. This would imply that $x^d - 1$ has a root mod $q$ (alongside $\Phi_n(x)$ by construction), which means that $x^n - 1$ has a double root at $x = lP$. However, the derivative of $x^n - 1$ is $nx^{n-1}$. $n(lP)^{n-1}$ is not congruent to 0 mod $q$ unless $n \equiv 0 \pmod{q}$, but since $q|n-1$ and $(n, n-1) = 1$, this is impossible, so we are done.

## 2 Primes 4 mod 15

First, note that by Quadratic Reciprocity, 5 and $-3$ are both perfect squares mod $p$ (for a prime $p$) iff $p \equiv 1, 4 \pmod{15}$. This fact is crucial to the solvability of this special case of Dirichlet's Theorem!

Now, the genius insight is to consider the following polynomial: $f(x) = (x-(\sqrt{5}+\sqrt{-3}))(x-(\sqrt{5}-\sqrt{-3}))(x-(-\sqrt{5}+\sqrt{-3}))(x-(-\sqrt{5}-\sqrt{-3}))$. First, by grouping the first two terms and the second two terms, we get the following identity:

$$\begin{aligned} f(x) &= (x^2 + 8 - 2x\sqrt{5})(x^2 + 8 + 2x\sqrt{5}) \\ &= (x^2+8)^2 - 5(2x)^2 \end{aligned} \tag{1}$$

Next, by grouping the first term with the third term and the second term with the fourth term, we get:

$$
\begin{aligned}
f(x) &= (x^2 - 8 - 2x\sqrt{-3})(x^2 + 8 + 2x\sqrt{-3}) \\
&= (x^2 + 8)^2 + 3(2x)^2
\end{aligned} \tag{2}
$$

So like in the previous case, suppose for the sake of contradiction that there are a finite of primes 4 mod 15, let $S = \{\text{prime } p > 0 : p \equiv 4 \pmod{15}\}$, and let $P$ be the (finite) product of all elements in $S$. Now consider $f(15lP)$, where $l$ is a positive integer such that $f(15lP) > 1$ (which is possible since as $x \to \infty$, $f(x) \to \infty$. Again, note that $p \nmid f(15lP)$ for all $p \in S$ since the constant term of $f(x)$ is 64. Furthermore, one can easily see that $f(15lP) \equiv 4 \pmod{15}$.

Let $q$ be a positive prime factor of $f(15lP)$. From equation (1), we have that:

$$((15lP)^2 + 8)^2 - 5(30lP)^2 \equiv 0 \pmod{q} \Rightarrow \left(\frac{(15lP)^2 + 8}{30lP}\right)^2 \equiv 5 \pmod{q}$$

The careful reader can work out the cases when $30lP \equiv 0 \pmod{q}$ (since $l$ can change, one needs to essentially deal with $q = 2, 3, 5$, but this isn't too hard). Thus, 5 is a quadratic residue mod $q$. Similarly, equation 2 yields that $-3$ is a quadratic residue mod $q$. By an earlier remark, this shows that $q$ must be 1 or 4 mod 15.

We're almost at the finish line now! We've shown that no prime factor 4 mod 15 divides $f(15lP)$ (since $p \nmid f(15lP)$ for all $p \in S$, that $f(15lP) \equiv 4$ mod 15, and that every prime factor of $f(15lP)$ must be 1 or 4 mod 15. But because $1^n \equiv 1$ mod 15, not every prime factor of $f(15lP)$ can be 1 mod 15, and so we've reached a contradiction.