(*October 13, 2010*)

Modular forms and number theory exercises 05

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/~garrett/

[mfms 05.1] Let q be a prime, and

$$\varphi_q(x) \;=\; x^{q-1} + x^{q-2} + \ldots + x^2 + x + 1 \;=\; \frac{x^q - 1}{x - 1}$$

the q^{th} cyclotomic polynomial. Show that, for an integer n, if a prime p divides $\varphi_q(n)$, then $p = 1 \bmod q$. Use this to prove that there are infinitely-many primes $p = 1 \bmod q$: given any finite list $p_1, p_2, \ldots, p_\ell$ of such, for large n the integer $\varphi_q(np_1 \ldots p_\ell)$ is larger than 1, so has a prime factor.

Hint: That $(\mathbb{Z}/p)^\times$ is *cyclic* is useful here.

[mfms 05.2] (*) Treat the general case of the above, namely, show that there are infinitely many primes $p = 1 \bmod N$.