MA2316: Introduction to Number Theory
Tutorial problems for March 20, 2014

"Prime divisors of values of cyclotomic polynomials"

The goal of this tutorial is to outline another proof of the particular case of Dirichlet's theorem we discussed in class.

1. Using the formula $\prod_{d|k} \Phi_d(x) = x^k - 1$, show that if a has order n in $(\mathbb{Z}/p\mathbb{Z})^\times$ then p divides $\Phi_n(a)$.

2. Let q be a prime number, and let a be an integer that has order s in $(\mathbb{Z}/q\mathbb{Z})^\times$ for which $q \mid \Phi_n(a)$. Show that $s \mid n$ and $s \mid q-1$.

3. Let q be a prime number, and let a be an integer that has order s in $(\mathbb{Z}/q\mathbb{Z})^\times$ for which $q \mid \Phi_n(a)$. Assume that $s < n$, and let r be a prime factor of $\frac{n}{s}$. We denote $h = \frac{n}{r}$, and $c = a^h$. (Clearly, $s \mid h$, so $c \equiv 1 \pmod{q}$). Show that $\Phi_n(a)$ divides

$$\frac{a^n - 1}{a^h - 1} = \frac{c^r - 1}{c - 1} = c^{r-1} + c^{r-2} + \cdots + c + 1,$$

and deduce that $r = q$, so q is the only prime factor of $\frac{n}{s}$. (That is, $n = sq^t$ for some t; recall that $s \mid q-1$, so in particular $\gcd(q, s) = 1$.)

4. Let p be the largest prime factor of n, $n = p^k m$, where $\gcd(p, m) = 1$. Deduce from the previous questions that

- if p is a prime factor of $\Phi_n(a)$, then a has order m in $(\mathbb{Z}/p\mathbb{Z})^\times$,
- if l is another prime factor of $\Phi_n(a)$, then a has order n in $(\mathbb{Z}/l\mathbb{Z})^\times$.

5. Show that if q is a prime factor of $\Phi_n(a)$, then the following three statements are equivalent: (i) a has order n in $(\mathbb{Z}/q\mathbb{Z})^\times$; (ii) q is not a divisor of n; (iii) $q \equiv 1 \pmod{n}$.

6. Show that for every $k \geqslant 1$, every $n \geqslant 2$, and every prime divisor p of $\Phi_n(kn)$ we have $p \equiv 1 \pmod{n}$, and deduce that there are infinitely many primes congruent to 1 modulo n.