MA2316-Introduction to Number Theory
Tutorial 7

Callum MacIver, Jack Geary, Benjamin Levai, Darragh Monnin, Eoghan Sheridan

20th March 2014

Question 1:

We consider a^k-1, k<n.
Since a has order n in ($\mathbb{Z}$/p$\mathbb{Z}$) we know that a^k-1 $\not\equiv$0 (mod p) (otherwise it would not be of order n in ($\mathbb{Z}$/p$\mathbb{Z}$)). We also know that, since d|d, Φ_d(a)|(a^d-1)

=>p $\nmid$ Φ_d(a), d|n, d<n

But a^n-1≡0(mod p) and $\prod_{d|n} \Phi_d(a)=a^n-1$

=>p| Φ_n(a)

Question 2:

q| Φ_n(a) => q| Φ_n(a)f(a)
Let f(a)= $\prod_{d|n,d<n} \Phi_d(a)$ then q|(a^n-1), so a^n≡1(mod q)
Let n=ms+b, b<s
$a^n=a^{ms}a^b\equiv 1.a^b$(mod q)≡1(mod q). This is a contradiction unless b=0.
So n=sm for some m => s|n

Similarly if we let q-1=rs+c, c<s
$a^{q-1}=a^{rs}a^c\equiv 1.a^c$(mod q)≡1(mod q) (by Fermat's Little Theorem). This is a contradiction unless c=0.
So q-1=sr for some r => s|q-1

Question 3:

a^h-1=$\prod_{d|h}$ Φ_d(a), a^n-1=$\prod_{d|n}$ Φ_d(a)

So $\frac{a^n-1}{a^h-1}$=$\prod_{d|n, d\nmid h}$ Φ_d(a), but n∤h, n|n,

$\frac{a^n-1}{a^h-1}$ has a factor of Φ_n(a), and can be divided by it.

Let h=sk, with s being the order of a, => k=$\frac{s}{h}$

$\frac{a^n-1}{a^h-1}$=$\sum_{j=r}^{1}$ c^{j-1}= $\sum_{j=r}^{1}$ $(a^s)^{k(j-1)}$≡ $\sum_{j=r}^{1}$ $1^{k(j-1)}$≡ r(mod q)

But Φ_n (a) ≡ 0(mod q), so r ≡ 0(mod q), so r=q.

Question 4:

- p, prime factor of Φ_n(a)
  => p |a^n-1, so a^n≡1 (mod p)
  We know the order of a must divide p-1,but p ∤p-1
  We also know that the only factors that n can have such that p| Φ_n(a) are p, and the order of a, so we find that the order of a=m.

- Once again, we know that any product of the order of a in $(\mathbb{Z}/l\mathbb{Z})^x$ by some other factor to get n.
  This only gives l| Φ_n(a) if the factor of n by the product is l raised to some power, so as long as gcd(l,m)=1, the order of a in ($\mathbb{Z}/l\mathbb{Z}$) is m.

Question 5:

To show that (i)=>(iii): n|q-1,=> q-1 ≡0 (mod n), => q≡ 1(mod n)

To show that (iii)=> (ii): unless n>q, q∤n, but q prime, so q=mn+1, m≥1, so q∤n

To show that (ii) =>(i): If q∤n, and Φ_n(a)≡ 0(mod p), then by question 4, a must have order n.

So (i)=>(iii)=>(ii)=>(i)

So the statements are equivalent

Question 6:

$n^n k^n$-1≡ 0(mod p)

$p\nmid n$ otherwise ($n^n k^n$-1)≡ -1(mod p)

(It will also be useful later on to note that $p\nmid k$ otherwise ($n^n k^n$-1)≡ -1(mod p))

n is the order of nk, so p≡1(mod n)

Assume there are only a finite number,m, of primes p_i such that $p_i \mid \Phi_n$(nk).

Let k=$\prod_{i=1}^{m} p_i$

Then $p_i \nmid \Phi_n$(nk) ∀i, but as Φ_n(nk)≠1,

Φ_n(nk)= $\prod_{d\nmid n, d<n}$ (nk-$e^{i\pi \frac{d}{n}}$) and ‖nk-$e^{i\pi \frac{d}{m}}$‖ > 1, ∀d, then ‖Φ_n(nk)‖ > 1

So Φ_n(nk)≠1, so it must bepossible for it to be expressed as the product of its prime factors, that is, there exists at least one q, q≠ p_i ∀i,such that $q\nmid \Phi_n$(nk), a contradiction