Number Theory: Tutorial 8 Solutions

Thomas Bourke, John Doyle, Peter Mulholland, TJ O Sullivan, Lauren Watson

March 31, 2014

1 Question 1

$\Longleftarrow$

$n = 2^m p_1 p_2 ... p_s$ with $p_i = 2^{2^k} + 1$ and p_i distinct odd primes

We know that φ is multipicative i.e. $\varphi(mn) = \varphi(m)\varphi(n)$ whenever gcd(m,n)=1

$\Rightarrow \varphi(2^m p_1 p_2 ... p_s) = \varphi(2^m)\varphi(p_1)\varphi(p_2)...\varphi(p_s)$

Also $\varphi(p^n) = p^n(1 - \frac{1}{p}) \Rightarrow \varphi(p_i) = p_i - 1$

And $\varphi(2^m) = 2^{m-1}$

Therefore $\varphi(n) = 2^{m-1}(p_1 - 1)(p_2 - 1)...(p_s - 1)$

$= 2^{m-1}(2^{2^{k_1}} - 1)(2^{2^{k_2}} - 1)...(2^{2^{k_s}} - 1)$

$= 2^{m-1} 2^{2^{k_1}} 2^{2^{k_2}} ... 2^{2^{k_s}}$

$= 2^{(m-1)+2^{k_1}+2^{k_2}+...+2^{k_s}}$

$\Longrightarrow$

$\varphi(n) = 2^k$

let $n = 2^m p_1^{e_1} p_2^{e_2} ... p_s^{e_s}$ with p_i odd primes and $e_i \geq 1$

For m $\neq$ 0

$\varphi(n) = 2^{m-1} p_1^{e_1 - 1} ... p_s^{e_s - 1}(p_1 - 1)...(p_s - 1)$

For m=0

$\varphi(n) = p_1^{e_1 - 1} ... p_s^{e_s - 1}(p_1 - 1)...(p_s - 1) = 2^k$

Also $e_i = 1$ otherwise $\rightarrow p_i | 2^k$ which is a contradiction

Then $\varphi(n) = (p_1 - 1)(p_2 - 1)...(p_s - 1) = 2^k$

$\Rightarrow p_i - 1 = 2^q$

$2^q + 1$ can only be prime if $q = 2^k$

$\Rightarrow p_i = 2^{2^k} + 1$C

2 Question 2

We need to show $\varphi(n) = 6$
$\varphi(ab) = \varphi(a)\varphi(b) \iff gcd(a,b) = 1$
$n = 2^m p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$ p_i odd distinct primes

case s=0:
$\implies \varphi(2^m) \neq 6$ ∀m

Case s≥ 2:
$\implies \varphi(n) = \varphi(2^m)\varphi(p_1^{a_1})\varphi(p_2^{a_2})...$
$\implies 4 \mid \varphi(n) \implies \varphi(n) \neq 6$

Case s=1:$\implies n = 2^m p^a$
$\implies \varphi(n) = \varphi(2^m)\varphi(p^a)$
$n > 2$ $\varphi(n) = 2x$ x ϵ $\mathbb{Z}$
$\implies \varphi(b) = 6$ $\forall b$
Solutions: $3^2, 2(3^2), 7, 2(7)$
$= 7, 9, 14, 28$

$\varphi(\varphi(n)) = 6 \implies \varphi(n) = 7, 9, 14, 18$
$\varphi(n)$ ≠7 or 9
$n = 2^m p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$
Take s=1 $\implies n = 2^m p^a$
m=2$\implies \varphi(4) = 2 \implies \varphi(p^a) = 7 \implies contradiction$
Leaves m=0,1$\implies \varphi(2^m) = 1 \implies \varphi(p^a) = 14 \implies contradiction$
$\varphi(n) = \varphi(2^m)\varphi(p^a) = 18$
∄ n s.t $\varphi(n)$ =3 or 9
$\implies \varphi(2^m) = 1 \implies m = 0, 1$
and $\varphi(p^a) = 18 \implies$ p=19,a=1 or p=3,a=3
Solutions 19,2(19),3^3, $2(3^3)$
$\implies$ 19,27,38,54

3 Question 3

Solve the equation **a)** $\varphi(n) = n/2$; **b)**$\varphi(n) = 2n/3$

a) $\varphi(n) = n/2 \Leftrightarrow \phi/n = 1/2$
$\phi(p^k) = p^k \Pi_{p|p^k}(1 - 1/p) = p^k(1 - 1/p) = p^{k-1}(p - 1)$
As the function is multiplicative;

$$\phi(n) = \phi(p^{a_1}...p_k^{a_k})$$

$$= \phi(p_1^{a_1}...\phi(p_k^{a_k}$$

$$= (p_1 - 1)p_1^{a_1-1}...(p_k - 1)p_k^{a_k-1}$$

$\frac{\phi(n)}{n} = \frac{(p_1-1)p_1^{a_1-1}...(p_k-1)p_k^{a_k-1}}{p_1^{a_1}...p_k^{a_k}}$

$\frac{(p_1-1)...(p_k-1)}{p_1...p_k} = 1/2$

$\Rightarrow 2(p_1-1)...(p_k-1) = p_1...p_k$
$\Rightarrow$ 2 must divide $p_1...p_k$
Say $p_1 = 2$
$(p_2-1)(p_3-1)...(p_k-1) = p_2...p_k$
The LHS is strictly smaller than RHS. $p_2...p_k$ cannot be prime factors of n because if they were then $p_i - 1$ wouldn't divide the RHS.

b) This follows similar reasoning to part **a)**, up to
$3(p_1-1)...(p_r-1) = 2p_1...p_r$

Given $3|p_1...p_r$, we can say $2|p_i - 1$ for some $1 \leq i \leq r$
Thus the LHS is divisible by 2, so we can write
$(p_1-1)...(p_r-1) = p_1...p_r$ which has no solutions.
Hence $p_1 = 3$ is the only prime.

4 Question 4

4. f,g are two functions with complex values defined on

$$[0,\infty) \tag{1}$$

Assume that: $\sum_{k,d\geqslant 1(f(\frac{x}{kd}))} < \infty$
Show that if:

$$g(x) = \sum_{d\geqslant 1}(f(\frac{x}{d})) \tag{2}$$

Then:

$$f(x) = \sum_{d\geqslant 1}\mu(d)G(\frac{x}{d}) \tag{3}$$

Since:

$$f(x) = \sum_{d\geqslant 1}\mu(d)G(\frac{x}{d}) \tag{4}$$

$$\sum_{d\geqslant 1}\mu(d)G(\frac{x}{d}) = \sum_{d\geqslant 1}\mu(d)\sum_{d\geqslant 1}G(\frac{x}{kd}) \tag{5}$$

As this is absolutely convergent the term in it can be rearranged

$$= \sum_{d\geqslant 1}\sum_{k\geqslant 1}\mu(d)G(\frac{x}{kd}) \tag{6}$$

Now let r = xd:

$$= \sum_{r \geqslant 1} \sum_{d|r} \mu(d) G(\frac{x}{r}) \tag{7}$$

$$= \sum_{r \geqslant 1} \sum_{d|r} G(\frac{x}{r}) \mu(d) \tag{8}$$

This equation equals 0 if

$$r \neq 1 \tag{9}$$

=f(x)

5 Question 5

Prove that

$$\Phi_n(x) = \Pi_{d|n}(x^d - 1)^{\mu(n/d)}$$

Using this formula, compute $\Phi_6(x)$ and $\Phi_{10}(x)$. Also, use your favourite computer software (or do it by hand if you feel brave) to verify that $\Phi_{105}(x)$ has a coefficient not equal to 0, -1, 1. What is that coefficient, and at which power of x does it occur?

$$x^n - 1 = \Pi_{d|n} \Phi_d(x) \qquad \text{where } x|n$$

We are going to use Moebius inversion but there is a slight problem with this, in that x^{n-1} is expressed in terms of a product instead of a sum. So we take the logarithm of it.

$$ln(x^n - 1) = \sum_{d|n} ln\Phi_d(x)$$

$$ln(\Phi_n(x)) = \sum_{d|n} \mu(d) ln(x^{n/d} - 1) \qquad d \longleftrightarrow \tfrac{n}{d}$$

$$= \sum_{\substack{d'|n \\ d' = \frac{n}{d}}} \mu(\frac{n}{d'}) ln(x^{d'} - 1)$$

$$= ln(\Pi_{d'|n}(x^{d'} - 1)^{\mu(\frac{n}{d'})})$$

$$\Rightarrow \qquad \Phi_n(x) = \Pi_{d'|n}(x^{d'} - 1)^{\mu(\frac{n}{d'})} \text{ as required}$$

So we get,

$$\Phi_6(x) = \tfrac{(x^6-1)(x-1)}{(x^2-1)(x^3-1)}$$

$$= x^2 - x + 1$$

$$\Phi_{10}(x) = \tfrac{(x^{10}-1)(x-1)}{(x^2-1)(x^5-1)}$$

$$= x^4 - x^3 + x^2 + x + 1$$

$$\Phi_{105}(x) = \frac{(x^{105}-1)(x^3-1)(x^5-1)(x^7-1)}{(x^{15}-1)(x^{21}-1)(x^{35}-1)(x-1)}$$

$$= \ldots\ldots \text{ using computer } \ldots\ldots$$

$$= x^{48} + \ldots - 2x^{41} \ldots - 2x^7 \ldots + 1$$

Therefore the coefficients of x^{41} and x^7 are both -2 and not 0, 1 or -1

6 Question 6

(i)

Suppose n=$p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$

$\tau(n)$ is the 'number of divisors of n' function, its value at an integer n is equal to the number of positive integer divisors of n

We can show that $\tau(mn) = \tau(m)\tau(n)$ for gcd(m,n) = 1 i.e τ is multipicative

Also $\tau(p_i^{a_i}) = a^i + 1$

Therefore $\tau(n) = (a_1 + 1)(a_2 + 1)...(a_k + 1) = \prod_1^k (a_i + 1)$

(ii)

$\sigma(n)$ is the 'number of divisors of n' function, its value at an integer n is the sum of all positive integer divisors of n

We can show that σ is also multipicative

We know that for any prime p: $\sigma(p) = p + 1$ as p's only divisors are itself and 1

(1) For $\sigma(p_i^{a_i}) = 1 + p_i + p_i^2 + ... + p_i^{a_i}$

(2) Now $p\sigma(p_i^{a_i}) = p_i + p_i^2 + ... + p_i^{a_i+1}$

(1)-(2) = $(p_i - 1)\sigma(p_i^{a_i}) = p_i^{a_i+1}$

$\Rightarrow \sigma(p_i^{a_i}) = \frac{p_i^{a_i+1}-1}{p_i-1}$

$\Rightarrow \sigma(n) = \prod_1^k \frac{p_i^{a_i+1}-1}{p_i-1}$