UM-SJTU JOINT INSTITUTE
DISCRETE MATHEMATICS
(VE203)

ASSIGNMENT 6

Name: Pan Chongdan
ID: 516370910121

Date: November 14, 2017

1 Q1

p is prime $\Rightarrow \varphi(p) = p - 1$,so when $k = 1, \varphi(p^k) = p^k - p^{k-1}$
Assume when $k = n, \varphi(p^k) = p^k - p^{k-1}$
Then when $k = n + 1$, it's clear that numbers are relative prime to p^k are still relative to p^{k+1}. If a and p^k are relative prime, then $\gcd(a, p^{k+1})$=1$\Rightarrow$$\gcd(a + n \cdot p^k, p^{k+1}) = 1(n < p)$
$\therefore$ $\forall a$,there will exist more (p-1) numbers which relative prime to $p^(k + 1)$
$\therefore, \varphi(p^{k+1}) = p \cdot \varphi(p^k) = p^{k+1} - p^k$
According to induction,$\varphi(p^k) = p^k - p^{k+1}$

2 Q2

$n^3 + 2n = n(n^2 + 2)$
$n(-n^3 - 3n) + n^4 + 3n^2 + 1 = 1 \Rightarrow n$ and $n^4 + 3n^2 + 1$ are relatively prime.
$(n^2 + 2)(n^2 + 1) - (n^4 + 3n^2 + 1) = 1 \Rightarrow n^2 + 2$ and $n^4 + 3n^2 + 1$ are relatively prime.
$\therefore n^3 + 2n$ and $n^4 + 3n^2 + 1$ are relatively prime.

3 Q3

Assume $G = \{a^n | n \in \mathbb{Z}\}, H \leq G, H = \{a^k | k \in \mathbb{Z}\}$,if i is the least number of k. According to the division algorithm, $\forall k = mi + j (j < i, m \in \mathbb{Z})$

If $j = 0 \Rightarrow i = mn \Rightarrow n \mid i \Rightarrow H$ is cyclic.

If $\exists j \neq 0$, which means H is not cyclic $\Rightarrow a^{-k} = a^{-mi-j}$

$\because a^i \in H \Rightarrow a^{mi} \in H \Rightarrow a^{mi} \cdot a^{-mi-j} = a^{-j} \in H \Rightarrow a^j \in H \Rightarrow j < i$, which leads a contradiction i is the least number of k.

$\therefore j = 0$ and H is cyclic.

4 Q4

Assume $3 \nmid ab \Rightarrow (3 \nmid a) \wedge (3 \nmid b)$
if $a = 3k + 1, (k \in \mathbb{Z}) \Rightarrow a^2 = 9k^2 + 6k + 1 \Rightarrow a^2 \equiv 1 \pmod 3$
if $a = 3k + 2, (k \in \mathbb{Z}) \Rightarrow a^2 = 9k^2 + 12k + 4 \Rightarrow a^2 \equiv 1 \pmod 3$
$\therefore a^2 \equiv b^2 \equiv 1 \pmod 3$$\Rightarrow c^2 \equiv a^2 + b^2 \equiv 2 \pmod 3$

if $c = 3k, c^2 = 9k^2 \equiv 0 \pmod 3$ So there doesn't exist c such $c^2 \equiv 2 \pmod 3$, which leads to a contradiction.

$\therefore 3 \mid ab$

5 Q5

$((\mathbb{Z}/11\mathbb{Z})^*, \otimes_{11}) = \{[1]_{11}, [2]_{11}, [3]_{11}, [4]_{11}, [5]_{11}, [6]_{11}, [7]_{11}, [8]_{11}, [9]_{11}, [10]_{11}\}$

$[2]_{11}^2 = [4]_{11}, [2]_{11}^3 = [8]_{11}, [2]_{11}^4 = [5]_{11}, [2]_{11}^5 = [10]_{11}, [2]_{11}^6 = [9]_{11}, [2]_{11}^7 = [7]_{11}$
$[2]_{11}^8 = [3]_{11}, [2]_{11}^2 = [6]_{11}, [2]_{11}^1 0 = [1]_{11}$
The generator is $[2]_{11}$

6 Q6

$e = [1]_{89}, [12]_{89} \otimes [52]_{89} = [1]_{89}$
The inverse is $[52]_{89}$

7 Q7

$[27]_{56}^2 = [1]_{56} = e$
Its order is 2.

8 Q8

$((\mathbb{Z}/14\mathbb{Z}^*, \otimes_{14}) = \{[1]_{14}, [3]_{14}, [5]_{14}, [9]_{14}, [11]_{14}, [13]_{14}\}$
$[3]_{14}^2 = [9]_{14}, [3]_{14}^3 = [13]_{14}, [3]_{14}^4 = [11]_{14}, [3]_{14}^5 = [5]_{14}, [3]_{14}^6 = [1]_{14}$
$\therefore ((\mathbb{Z}/14\mathbb{Z}^*$ is a cyclic group.

9 Q9

$\otimes 9$	$[1]_9$	$[2]_9$	$[4]_9$	$[5]_9$	$[7]_9$	$[8]_9$
$[1]_9$	$[1]_9$	$[2]_9$	$[4]_9$	$[5]_9$	$[7]_9$	$[8]_9$
$[2]_9$	$[2]_9$	$[4]_9$	$[8]_9$	$[1]_9$	$[5]_9$	$[7]_9$
$[4]_9$	$[4]_9$	$[8]_9$	$[7]_9$	$[2]_9$	$[1]_9$	$[5]_9$
$[5]_9$	$[5]_9$	$[1]_9$	$[2]_9$	$[7]_9$	$[8]_9$	$[4]_9$
$[7]_9$	$[7]_9$	$[5]_9$	$[1]_9$	$[8]_9$	$[4]_9$	$[2]_9$
$[8]_9$	$[8]_9$	$[7]_9$	$[5]_9$	$[4]_9$	$[2]_9$	$[1]_9$

Table 1: Cayley Table

It's cyclic because $[2]_9^2 = [4]_9, [2]_9^3 = [8]_9, [2]_9^4 = [7]_9, [2]_9^5 = [5]_9, [2]_9^6 = [1]_9$