Department of Computer & Mathematical Sciences
University of Toronto Scarborough

Term Test 3

MATC15H – Introduction to Number Theory

Examiner: J. Friedlander

Date: March 16, 2018
Time: 7:00pm-8:30pm

FAMILY NAME: POON

GIVEN NAME(S): KEEGAN

STUDENT NUMBER: 1002423727

SIGNATURE:

DO NOT OPEN THIS BOOKLET UNTIL INSTRUCTED TO DO SO

NOTES:

- There are 6 numbered pages in the test. It is your responsibility to ensure that, at the start of the exam and at the end of the exam, this booklet has all its pages.
- No calculators or other aids.
- Justify your answers.

FOR MARKERS ONLY	
Question	Marks
1	12 /12
2	8 /12
3	10 /16
TOTAL	30 **/40**

1. **[12 marks]**

a) Define the Möbius function and state the Möbius inversion formula.

$$\mu(n) = \begin{cases} 0 & \text{if } p^2 \mid n \text{, for } p \text{ a prime} \\ (-1)^t & \text{if } n = p_1 \cdots p_t \text{ where } p_i \text{ distinct primes} \\ 1 & \text{if } n = 1 \end{cases}$$

For an arithmetic function $F(x)$,

the Möbius inversion formula

gives arithmetic function f

where $\boxed{f(n) = \sum_{d \mid n} \mu(d) F\left(\frac{n}{d}\right)}$

such that $F(n) = \sum_{d \mid n} f(d)$

b) Show that, for every positive integer *n*,

$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$.

~~Suppose this was not the case, and we had it equal (-1) or 1,~~

~~then let $a < b$ be the two odd numbers $\in [n, n+3]$~~

~~we know they are all products of distinct primes.~~

~~Consider $d = (a, b)$~~

~~if $d = 1$~~

one of $n, n+1, n+2, n+3$ is a multiple of 4.

($0, 1, 2, 3$ is a complete residue system $\Rightarrow k+0, k+1, \ldots$ also is)

therefore it is divisible by 2^2

so $\mu(2^k)\mu(\text{rest of primes}) = 0 \cdot \mu(\text{rest}) = 0$

$k \geq 2$

so $\mu(4m) \cdot \mu(n+\cdots) \cdots$

$= 0 \cdot \mu(\cdots) \cdots$

$= \emptyset$

2. **[12 marks]**

$(p-1)!$ modulo p

a) What is the least positive residue of (*p*-1)! when *p* is a prime?
(You do not need to prove it.)

$p-1$

4

$(b-1)!$ modulo b

b) For *b*>1, a composite integer, give the least positive residue of (*b*-1)!, justifying your reasoning.

For every $b>1$ composite integer, the least positive residue is simply $\emptyset$. This is because, decomposing ~~the~~ b into prime factors, $p_1^{k_1} \cdots p_n^{k_n}$, $\boxed{\text{we have}}$ $p_i^{k_i} < b \; \forall i$

this means they are in the factorial product, ~~so~~ $b \mid (b-1)!$ (since p_i all distinct) ?

$\Rightarrow (b-1)! = p_1^{k_1} \cdots p_n^{k_n} \cdot (\text{rest of prime factors})$

$\Rightarrow b \mid (b-1)!$.

4

b=2 ?

This page is intentionally blank.

Use but do **NOT** tear out.

3. **[16 marks]**
Using also the previous blank page if necessary, find prime numbers p and q and integers a_1, a_2, b_1, b_2 such that every integer x satisfying the congruence

$$x^2+x+1 \equiv 0 \pmod{91}$$

(and only those) is found in precisely one of the following four systems of 2 congruences.

$x \equiv a_i \pmod p$ (i=1,2)
$x \equiv b_j \pmod q$ (j=1,2)

$91 = 7 \cdot 13 \Rightarrow \boxed{p=7 \quad q=13}$

7, 13 prime factorization of 91, so if $P(x) \equiv 0 \pmod{91}$ $\Rightarrow P(x) \equiv 0 \pmod 7$

try $x=0$: $0+0+1 \equiv 1 \pmod 7$
$x=1$: $1+1+1 \equiv 3 \pmod 7$
2: $4+2+1 \equiv 7 \equiv 0 \pmod 7$
3: $9+3+1 \equiv 13 \equiv 5 \pmod 7$
4: $16+4+1 \equiv 21 \equiv 0 \pmod 7$
5: $25+5+1 \equiv 31 \equiv 3 \pmod 7$
6: $36+6+1 \equiv 43 \equiv 1 \pmod 7$

$\boxed{a_1 = 2 \quad a_2 = 4}$

already know $b_1 = 3$ (from system above) Now try for simultaneous solution since impossible to be 3 (mod 7)

soln 1 soln 2 soln 1+7
~~1~~, ~~4~~, ~~8~~, ~~11~~, ~~15~~, ~~18~~, 22

$x = 8 \pmod{13}$
$\Rightarrow 64+8+1 \equiv 73 \equiv 8 \pmod{13}$
$x = 11 \pmod{13}$
$\equiv -2 \quad (-2)^2+(-2)+1 \equiv 3 \pmod{13}$
$x = 15 \equiv 2 \pmod{13}$
$2^2+2+1 \equiv 7 \pmod{13}$
$x = 18 \equiv 5 \pmod{13}$
$25+5+1 \equiv 31 \equiv 5 \pmod{13}$
$x = 22 \equiv 9 \pmod{13}$
$81+9+1 \equiv 91 \equiv 0 \pmod{13}$

Verify no other solutions
1
2
3
4 $16+4+1 \equiv 21 \equiv 8 \pmod{13}$
5
6 $36+6+1 \equiv 43 \equiv 4 \pmod{13}$
7 $49+7+1 \equiv 57 \equiv 5 \pmod{13}$
8
9
10 $100+10+1 \equiv 111 \equiv 7 \pmod{13}$
11
12 $(-1)^2+(-1)+1 = 1 \pmod{13}$
$\therefore$ b_1 b_2 only 2 soln

$130-13 = 117$
$117-13 = 104$

proof?

10

So $\boxed{b_1 = 3 \;\&\; b_2 = 9}$

~~clearly 2, 19 satisfies $x^2+x+1 \equiv 0 \pmod{91}$ as it is the root of the quadratic~~