Department of Computer & Mathematical Sciences
University of Toronto Scarborough

Term Test 1

MATC15H – Introduction to Number Theory

Examiner: J. Friedlander

Date: Feb. 2, 2018
Time: 3:00pm-4:30pm

FAMILY NAME: Poon

GIVEN NAME(S): Keegan

STUDENT NUMBER: 1002423727

SIGNATURE: [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	13 /13
2	13 /13
3	14 /14
TOTAL	40 /40

1. **[13 marks]** Using the Euclidean algorithm, find the greatest common divisor of 234 and 192.

   Then find one pair x, y of the integers which satisfy $234x + 192y = 30$.

$4(42) = 168$

$234 = 1(192) + 42$

$192 = 4(42) + 24$

$42 = 1(24) + 18$

$24 = 1(18) + 6 \Rightarrow (234, 192) = 6$

$18 = 3 \cdot (6)$

$6 = 24 - 18$

$6 = 24 - (42 - 24)$

$6 = 2(24) - 42$

$6 = 2(192 - 4(42)) - 42$

$= 2(192) - 8(42) - 42$

$= 2(192) - 9(42)$

$6 = 2(192) - 9(234 - 192)$

$= 2(192) - 9(234) + 9(192)$

$= 11(192) - 9(234)$

So $30 = 5 \cdot 6$

$= 5 \cdot [11(192) - 9(234)]$

$= 55(192) - 45(234)$

So $x = 55$, $y = -45$

Verification

$(192)(55)$

$= (100 + 90 + 2)(50 + 5)$

$= (5000 + 4500 + 100) + (500 + 450 + 10)$

$= (9600) + (960)$

$= 10560$

$(45)(234)$

$= (200 + 30 + 4)(40 + 5)$

$= (8000 + 1200 + 160) + (1000 + 150 + 20)$

$= (9360) + (1170)$

$= (10530)$

$(192)(55) - (45)(234)$

$= 10560 - 10530$

$= 30$ //

2. **[13 marks]** Let a, b, m be integers with $m>0$.

Let $P(x)$ be a polynomial with integer coefficients.

Show, using mathematical induction, that, if $a \equiv b \pmod m$ then $P(a) \equiv P(b) \pmod m$.

Let $S(n)$ be the statement that for any polynomial $p_n(x)$ of degree n or less with integer coefficients

$$a \equiv b \pmod m \Rightarrow p_k(a) \equiv p_k(b) \pmod m$$

Base case: $S(1)$

$$a \equiv b \pmod m$$
$$ca = cb \pmod m$$
$$ca + d \equiv cb + d \pmod m \quad \forall c, d$$

these being polynomials of degree 1

So $S(1)$ holds

I.H. Suppose $S(k-1)$ holds $k \in \mathbb{N}$,

I.S. if $a \equiv b \pmod m$

$p_k(a) = ca^k + p_{k-1}(a)$ for some poly p_{k-1}

& $p_k(b) = cb^k + p_{k-1}(b)$

So $p_k(a) \equiv a(ca^{k-1}+1) \pmod m$

$p_k(b) \equiv cb^k + b \pmod m$

$\equiv b(cb^{k-1}+1) \pmod m$

$a \equiv b \pmod m$

$\Rightarrow a^k \equiv b^k \pmod m$ shown in class

$ca^k \equiv cb^k \pmod m$

But we know $p_k(a) = ca^k + p_{k-1}(a)$ for some poly $p_{k-1}(x)$

& $p_k(b) = cb^k + p_{k-1}(b)$

& $p_{k-1}(a) \equiv p_{k-1}(b)$ by I.H.

So $ca^k \equiv cb^k \pmod m$

& $p_{k-1}(a) \equiv p_{k-1}(b) \pmod m$

$\Rightarrow ca^k + p_{k-1}(a) \equiv cb^k + p_{k-1}(b) \pmod m$

$\Leftrightarrow p_k(a) \equiv p_k(b)$ ✱ P.I. induction holds for $k \in \mathbb{N}$

This page is intentionally blank.

Use but do **NOT** tear out.

3. **[14 marks]** If $[a, b]$ denotes the least common multiple of a and b then prove:

i) $[a, a+2] = \frac{a(a+2)}{2}$ if a is even

And

ii) $[a, a+2] = a(a+2)$ if a is odd

i) $[a, a+2] \cdot (a, a+2) = (a)(a+2)$

so $[a, a+2] = \frac{(a)(a+2)}{(a, a+2)}$

so the common divisors of a & $a+2$ must divide $ax + (a+2)y$ $\forall x, y$

but if $x = -1$ $y = 1$

$\Rightarrow$ common divisor must divide 2.

So greatest common divisor is either 1 or 2.

Since a even, $2 \mid a$ & $2 \mid a+2$

hence $(a, a+2) = 2$

so $[a, a+2] = \frac{a(a+2)}{2}$

ii) Similarly for odd case

$[a, a+2] = \frac{a(a+2)}{(a, a+2)}$ but $(a, a+2) \in \{1, 2\}$

Since a odd, $2 \nmid a$ so 1 is the greatest common divisor

$\Rightarrow [a, a+2] = \frac{a(a+2)}{1}$

$= a(a+2)$

as wanted.