CIS 3223 Homework 2

Dr Anthony Hughes

Name:
Temple ID (last 4 digits:

1 (6 pts) Show that $\sum_{i=1}^{n} \frac{1}{i} = \Theta(\log n)$

$$\int_1^n \frac{1}{x}\, dx = \ln x \Big|_1^n = \ln n - \cancel{\ln 1} = \Theta(\log n)$$

2 (9 pts) Determine the following:

(a) 4231 (mod 19) $\boxed{18}$

(b) -75 (mod 19) $\boxed{1}$

(c) 19^7 (mod 17) $\boxed{9}$

$$19^7 \pmod{17} \equiv 2^7 \pmod{17}$$
$$\equiv 128 \pmod{17}$$
$$\equiv 9$$

3 (15 pts) Apply the non-recursive **division algorithm** to find the quotient and remainder when 100 is divided by 7. **Show all steps** (diagram carefully).

$x = 100 \quad y = 7$ $\qquad$ $100 = 1\ 1\ 0\ 0\ 1\ 0\ 0$

	digit	q	r	$r \geq y$
		0	0	
0	1	0 0	0 1	F
1	1	0 0	2 3	F
3	0	0 0	6 6	F
6	0	0 0 1	12 12 5	T
12	1	2 2 3	10 11 4	T
25	0	6 6 7	8 8 1	T
50	0	14 14	2 2	
100				

quotient 14 $\qquad$ remainder 2

4 (15pts) Use the **extended Euclidean algorithm** (using matrices) to find integers s and t such that $91s + 11t = \gcd(91, 11)$ (show all steps).

$a = 91, \quad b = 11$ $\quad Q = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

a	b	q	r	Q
91	11	8	3	$\begin{bmatrix} 0 & 1 \\ 1 & -8 \end{bmatrix}$
11	3	3	2	$\begin{bmatrix} 0 & 1 \\ 1 & -3 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & -8 \end{bmatrix} = \begin{bmatrix} 1 & -8 \\ -3 & 25 \end{bmatrix}$
3	2	1	1	$\begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 & -8 \\ -3 & 25 \end{bmatrix} = \begin{bmatrix} -3 & 25 \\ 4 & -33 \end{bmatrix}$
2	1	2	0	$\begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix}\begin{bmatrix} -3 & 25 \\ 4 & -33 \end{bmatrix} = \begin{bmatrix} 4 & -33 \\ -11 & 91 \end{bmatrix}$

compute first

$91\,\boxed{4} + 11\,\boxed{-33} = \boxed{1}$

5 (5 pts). Exercise 1.10

$\left(a \equiv b \pmod N,\ M \mid N\right) \Rightarrow a \equiv b \pmod M$

$a \equiv b \pmod N \Rightarrow N \mid a-b \Rightarrow a-b = Ns;\ s \in \mathbb{Z}$

$M \mid N \Rightarrow N = Mz,\ z \in \mathbb{Z}$

Now $a - b = Ns = (Mz)s$

$= M(zs)$

Thus $M \mid a-b$ since $zs \in \mathbb{Z}$ and so

$a \equiv b \pmod M$