NO

DATE

homework 3

1. $a, b \in \mathbb{Z}$ $a \geq b > 0$, $q = \lfloor \frac{a}{b} \rfloor$

~~<+>~~ $l(x) = \lfloor \log_2 x \rfloor + 1, x > 0$

<1> $\exists r \in \mathbb{Z}$, $0 \leq r < b$

s.t. $a = bq + r$

so $l(a) = \lfloor \log_2 a \rfloor + 1 = \lfloor \log_2 (bq + r) \rfloor + 1$

$\geq \lfloor \log_2 (bq) \rfloor + 1 = \lfloor (\log_2 b) + (\log_2 q) \rfloor + 1$

$\geq \lfloor \log_2 b \rfloor + \lfloor \log_2 q \rfloor + 1$

$= l(b) + l(q) - 1$

so $l(a) \geq l(b) + l(q) - 1$

so $l(q) \leq l(a) - l(b) + 1$

<2> $\exists r \in \mathbb{Z}$, $0 \leq r < b$

s.t. $a = bq + r < bq + b = b(q+1)$

so $l(a) = \lfloor \log_2 a \rfloor + 1 = \lfloor \log_2 (bq + r) \rfloor + 1$

$< \lfloor \log_2 b(q+1) \rfloor + 1 = \lfloor \log_2 b + \log_2 (q+1) \rfloor + 1$

$\leq (\lfloor \log_2 b \rfloor + \lfloor \log_2 (q+1) \rfloor + 1) + 1$

since $a \geq b$ so $q \geq 1 \Rightarrow 2q \geq q + 1$

so $\lfloor \log_2 b \rfloor + \lfloor \log_2 (q+1) \rfloor + 2$

$\leq \lfloor \log_2 b \rfloor + \lfloor \log_2 (2q) \rfloor + 2 = \lfloor \log_2 b \rfloor + \lfloor \log_2 q + 1 \rfloor + 1$

$= \lfloor \log_2 b \rfloor + \lfloor \log_2 q \rfloor + 1 + 1$

$= l(b) + l(q) + 1$

so $l(a) < l(b) + l(q) + 1$

so $l(a) \leq l(b) + l(q) + 1$

so $l(a) - l(b) - 1 \leq l(q)$

above all $l(a) - l(b) - 1 \leq l(q) \leq l(a) - l(b) + 1$ □

NO

DATE

4. (1) $17x \equiv 11 \pmod{23}$

$d = \gcd(a, n) = \gcd(17, 23) = 1$

since $d \mid 11$ so x has a solution

notice that when $x = 2$

$17 \times 2 = 34$

$34 \bmod 23 = 11$

so 且 when $x = 2$, $17x \equiv 11 \pmod{23}$ is correct ⇒ so $x = 2$ is one of the solution

$\frac{n}{d} = \frac{23}{1} = 23$ so $x \equiv 2 \pmod{23}$

so let $x = 2 + 23z$, $z \in \mathbb{Z}$ is all the solutions

above all $x = 2 + 23z$, $z \in \mathbb{Z}$

(2) $55x \equiv 35 \pmod{75}$

$a = 55$, $b = 35$, $n = 75$

let $d = \gcd(a, n) = \gcd(55, 75) = 5$

$5 \mid 35$ so $d \mid b$ so the equation has solutions

let $t = (\frac{a}{d})^{-1} \pmod{\frac{n}{d}}$

$t = 11^{-1} \pmod{15}$

~~since~~ $\varphi(15) = (3-1) \times (5-1) = 8$

since $\gcd(t, \frac{n}{d}) = \gcd(11, 15) = 1$

notice that $11 \times 11 = 121 = 120 + 1 = 15 \times 8 + 1$

so $11 \times 11 \equiv 1 \pmod{15}$

NO

DATE

so $(11)^{-1} \pmod{15} = 11$

so $t = 11$

satisfied $(\frac{a}{d}) \cdot t \equiv 1 \pmod{\frac{n}{d}}$

so the solution

$x \equiv \frac{b}{d} \cdot t \pmod{\frac{n}{d}}$

$x \equiv \frac{35}{5} \times 11 \pmod{\frac{75}{5}}$

$x \equiv 77 \pmod{15}$

$x \equiv 2 \pmod{15}$

so $x = 2 + 15z, \ z \in \mathbb{Z}$

above all

$x = 2 + 15z, \ z \in \mathbb{Z}$

are the solutions of the equation

$55x \equiv 35 \pmod{75}$

5. Eve can learn the value m

since $\gcd(e_1, e_2) = 1$

so there exist $s, t \in \mathbb{Z}$ s.t.

$$e_1 s + e_2 t = 1$$

from RSA we know that

$$c_1 = m^{e_1} \pmod{N}$$

$$c_2 = m^{e_2} \pmod{N}$$

so $c_1^s \bmod N = (m^{e_1})^s \bmod N = m^{e_1 s} \bmod N$

$c_2^t \bmod N = (m^{e_2})^t \bmod N = m^{e_2 t} \bmod N$

so $(c_1^s) \cdot (c_2^t) \bmod N = (m^{e_1 s} \bmod N) \cdot (m^{e_2 t} \bmod N) \bmod N$

$$= m^{e_1 s} \cdot m^{e_2 t} \bmod N$$

$$= m^{e_1 s + e_2 t} \bmod N$$

since $e_1 s + e_2 t = 1$

so $(c_1^s)(c_2^t) \bmod N = m^1 \bmod N$

so $c_1^s \cdot c_2^t \equiv m \pmod{N}$

since $0 \le m < N$

so $m = c_1^s \cdot c_2^t \bmod N$

above all

we can compute m

by $m = c_1^s \cdot c_2^t \bmod N$