No.

Date

Assignment 3

Q1. (1) $33^{15} \bmod 32 = (33 \bmod 32)^{15} = 1^{15} = 1$

$(33^{15} \bmod 32)^3 \bmod 15 = 1^3 \bmod 15 = 1 \bmod 15 = 1$

(2) Using Euclidean Algorithm.

$1638 = 210 \cdot 7 + 168$

$210 = 168 \cdot 1 + 42$

$168 = 42 \cdot 4 + 0$

$\gcd(1638, 210) = \gcd(210, 168) = \gcd(168, 42) = 42$

(3) $89 = 34 \cdot 2 + 21$

$34 = 21 \cdot 1 + 13$

$21 = 13 \cdot 1 + 8$

$13 = 8 \cdot 1 + 5$

$8 = 5 \cdot 1 + 3$

$5 = 3 \cdot 1 + 2$

$3 = 2 \cdot 1 + 1$

$1 = 3 - 2 \cdot 1 = 3 \cdot 2 - 5 = 8 \cdot 2 - 5 \cdot 3 = 13 \cdot (-3) + 8 \cdot 5 = 21 \cdot 5 - 13 \cdot 8$

$= 34 \cdot (-8) + 21 \cdot 13 = 89 \cdot 13 - 34 \cdot 34$

Hence, $-34 \cdot 34 \equiv 1 \pmod{89}$

$(-34) \cdot 34x \equiv (-34) \cdot 77 \pmod{89} \Rightarrow x \equiv (-34) \cdot 77 \pmod{89}$

$\Rightarrow x \equiv 52 \pmod{89}$, that is, $x = 89k + 52, k \in \mathbb{Z}$

~~(4) From Fermat's little theorem, gcd(3, 1000) = 1~~

(4) $3^4 = 81 \equiv 1 \pmod{10}$

$3^{1000} = (3^4)^{250}$, $3^{1000} \bmod 10 = (3^4)^{250} \bmod 10 = (3^4 \bmod 10)^{250} \bmod 10$

$= 1^{250} \bmod 10 = 1 \bmod 10 = 1$

Hence, last digit is 1.

No.

Date

Q2. Using extended Euclidean algorithm. $s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$ at begin.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	561	234	2	93	1	0
1	234	93	2	48	0	1
2	93	48	1	45	1	-2
3	48	45	1	3	-2	5
4	45	3	15	0	3	-7
5					-5	12

$s_j = s_{j-2} - s_{j-1} q_{j-1}$

$t_j = t_{j-2} - t_{j-1} q_{j-1}$

$\gcd(561, 234) = 3 = (-5) \times 561 + 12 \times 234$

Q3. Suppose $c = \gcd(m,c) \cdot x$, x is an integer because $\gcd(m,c) \mid c$.

$ac \equiv bc \pmod m \Rightarrow \exists\, k \in \mathbb{Z}$, s.t. $ac - bc = mk$

Since $c \mid ac - bc$, $c \mid mk$

$ac - bc = mk \Rightarrow a - b = \frac{mk}{c} = \frac{m}{\gcd(m,c)} \cdot \frac{k}{x}$

From definition of greatest common divisor, $\gcd(m, \frac{c}{\gcd(m,c)}) = 1$,

that is, $\gcd(m, x) = 1$

From, $\gcd(m,c) \cdot x \mid mk$, $\gcd(m,x) = 1$, we get $x \mid k$, so $\frac{k}{x}$ is an integer.

$\exists$ integer $\frac{k}{x}$, s.t. $a - b = \frac{k}{x} \cdot \frac{m}{\gcd(c,m)}$, from definition, $\cancel{a \equiv b (m/gc}$

$a \equiv b \pmod{m/\gcd(c,m)}$

Q4. Prove by contradiction.

Suppose $\gcd(\cancel{a\equiv b}\ b+a, b-a) = x > 2$, then $x \mid b+a$, $x \mid b-a$.

$x \mid (b+a) - (b-a) = 2a$, $x \mid (b+a) + (b-a) = 2b$

↓ Next Page

① x is even, $x|2b$, $x|2a \Rightarrow \frac{x}{2}|a$, $\frac{x}{2}|b$

Then $\gcd(a,b) = \frac{x}{2} > 1$ (because $x > 2$), contradiction.

② x is odd, $x|2b$, $x|2a \Rightarrow x|a$, $x|b$

Then $\gcd(a,b) = x > 1$, contradiction.

Above all, $\gcd(b+a, b-a) \le 2$

Q5. (a) $2^{10} = 1024 \equiv 463 \pmod{561}$

$2^{20} \equiv (1024)^2 \equiv 463^2 \equiv 214369 \equiv 67 \pmod{561}$

$2^{40} \equiv (2^{20})^2 \equiv 67^2 \equiv 4489 \equiv 1 \pmod{561}$

Hence, $2^{560} \equiv (2^{40})^{14} \equiv 1^{14} = 1 \pmod{561}$

(b) No. Because 561 is not a prime ($561 = 3\times11\times17$), but it still pass the 'Fermat primality test'.

Q6. (a) Using extended Euclidean algorithm.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	778	379	2	20	1	0
1	379	20	18	19	0	1
2	20	19	1	1	1	-2
3	19	1	19	0	-18	37
4					19	-39

$\gcd(778, 379) = 1 = 778\times19 - 379\times39 \Rightarrow 19\times778 \equiv 1 \pmod{379}$

$778x \equiv 10 \pmod{379} \Rightarrow 19\times778x \equiv 190 \pmod{379} \Rightarrow x \equiv 190 \pmod{379}$

Hence $x = 190 + 379k$, $k \in \mathbb{Z}$

(b) Next Page.

Date

(b) Using extended Euclidean algorithm.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	312	97	2	18	1	0
1	97	18	5	7	0	1
2	18	7	2	4	1	-2
3	7	4	1	3	-5	11
4	4	3	1	1	11	-24
5	3	1	3	0	-16	35
6					27	-59

$\gcd(312,97)=1=312\times27-97\times59 \Rightarrow 27\cdot312\equiv1 \pmod{97}$

$312x\equiv3 \pmod{97} \Rightarrow 27\cdot312x\equiv81 \pmod{97} \Rightarrow x\equiv81 \pmod{97}$

Hence, $x=81+97k$, $k\in\mathbb{Z}$

Q7. $x\equiv5 \pmod 6 \Rightarrow x\equiv1 \pmod 2$, $x\equiv2 \pmod 3$

$x\equiv3 \pmod{10} \Rightarrow x\equiv1 \pmod 2$, $x\equiv3 \pmod 5$

$x\equiv8 \pmod{15} \Rightarrow x\equiv2 \pmod 3$, $x\equiv3 \pmod 5$

There are no contradiction between each congruences, hence this system can be solved.

Now we need to solve $x\equiv1 \pmod 2$, $x\equiv2 \pmod 3$, $x\equiv3 \pmod 5$

Using Chinese Remainder Theorem.

$m=2\cdot3\cdot5=30$, $M_1=\frac{m}{2}=15$, $M_2=\frac{m}{3}=10$, $M_3=\frac{m}{5}=6$

$1\cdot15\equiv1 \pmod 2 \Rightarrow y_1=1$

$1\cdot10\equiv1 \pmod 3 \Rightarrow y_2=1$

$1\cdot6\equiv1 \pmod 5 \Rightarrow y_3=1$

$x=1\cdot15\cdot1+2\cdot10\cdot1+3\cdot6\cdot1=53\equiv23 \pmod{30}$

Hence, $x=23+30k$, $k\in\mathbb{Z}$

No.
Date . .

Q8. (a) ① n is odd, suppose $n=2k+1$, $k\in\mathbb{Z}$.

$n^2=4k^2+4k+1$, $4\mid 4k^2+4k$, so $n^2\equiv 1 \pmod 4$

② n is even, suppose $n=2k$, $k\in\mathbb{Z}$

$n^2=4k^2$, so $n^2\equiv 0 \pmod 4$

Hence, $n^2\equiv 0$ or $1 \pmod 4$

(b) Sum of squares of two integers mod 4 can only be 0, 1, 2. But $m=4k+3$, $m\equiv 3 \pmod 4$. So m can not be the sum of squares of two integers.

Q9. Prove by contradiction.

Suppose a have an inverse of modulo m, we denote it as b.

Which means, $\exists k\in\mathbb{Z}$, $ab-1=mk$. $ab-mk=1$

Denote $\gcd(a,m)=x>1$, then $x\mid a$, $x\mid m$

So $x\mid ab$, $x\mid mk$, $x\mid ab-mk=1$, contradict to $x>1$.

Hence, a ~~done~~ dose not have an inverse modulo m.

Q10. (a) Take $a=3$, $b=7$, $c=2$, $m=8$.

$ac=6$, $bc=14$, $6\equiv 14 \pmod 8$, but $3\equiv 7 \pmod 8$ is wrong.

(b) Take $a=2$, $b=5$, $c=1$, $d=4$, $m=3$.

$2\equiv 5 \pmod 3$, $1\equiv 4 \pmod 3$, $2^1\equiv 2 \pmod 3$, $5^4\equiv 1 \pmod 3$,

so $2^1\not\equiv 5^4 \pmod 3$.

Q11. We know $n=pq$ and $(p-1)(q-1)$.

$(p-1)(q-1)=pq-p-q+1=n-(p+q)+1$, then we can calculate $p+q$.

From $p+q$ and pq, it's easy to know p and q.

No.

Date

Q12. (a) $\hat{M} = M^e \bmod n = 8^7 \bmod 65 = (64^3 \bmod 65) \cdot (8 \bmod 65)$

$= (-1)^3 \cdot 8 \bmod 65 = -8 \bmod 65 = 57$

(b) d should be the inverse of $e=7$ with modulo $(p-1)(q-1)$

$n = 65 = 5 \times 13 = pq$, $(p-1)(q-1) = 4 \times 12 = 48$

$d=7$, then $de \equiv 1 \bmod 48$.

(c) $M = \hat{M}^d \bmod n = 57^7 \bmod 65 = (-8)^7 \bmod 65 = (64 \bmod 65)^3 (-8 \bmod 65)$

$= (-1)^3 \cdot (-8) \bmod 65 = 8 \bmod 65 = 8$

The decryption succeed.