Chiriac's Practice Midterm 2 sol'n

1) (a) show that $25 \mid 2^{65} + 3^{65}$.

Answer: $\varphi(\underbrace{25}_{5^2}) = 5^2 - 5 = 20$.

Both classes $\bar{2}$ and $\bar{3}$ in $\mathbb{Z}_{25}$ are multiplicatively invertible, since $\gcd(2,25)=1$ and $\gcd(3,25)=1$. Hence,
$\bar{2}^{20} = \bar{1}$ and $\bar{3}^{20} = \bar{1}$, by Euler's Theorem.

$\bar{2}^{65} = \bar{2}^{60+5} = (\bar{2}^{20}) \cdot \bar{2}^5 = \bar{2}^5$. Similarly,
$\bar{3}^{65} = \bar{3}^5$.

$\bar{2}^5 = \overline{32} = \bar{7}$ in $\mathbb{Z}_{25}$

$\bar{3}^5 = \underbrace{\overline{81}}_{= \bar{6}} \cdot \bar{3} = \overline{18}$ in $\mathbb{Z}_{25}$. So

$\bar{2}^{65} + \bar{3}^{65} = \bar{7} + \overline{18} = \overline{25} = \bar{0}$ in $\mathbb{Z}_{25}$.

Hence, $25 \mid 2^{65} + 3^{65}$.

1(b) Let $p > 3$ be prime. Find the remainder when $3^p (p-2)!$ is divided by p.

<u>Answer:</u> $\bar{3}^p = \bar{3}$, by Fermat's Little Theorem and the fact that $\gcd(3,p) = 1$, since $p > 3$.
$(p-1)! \equiv -1 \pmod{p}$, by Wilson's Theorem,
and $p-1 \equiv -1 \pmod{p}$, so
$(p-2)! \equiv 1 \pmod{p}$. Thus,
$3^p (p-2) \equiv 3 \pmod{p}$.
The remainder is thus 3.

2) Suppose that both p and $2p-1$ are odd primes. Set $n := 2(2p-1)$. Prove that $\varphi(n) = \varphi(n+2)$.

<u>Proof:</u> $\gcd(2, 2p-1) = 1$, since $2p-1$ is odd.
Hence, $\varphi(n) = \underbrace{\varphi(2)}_{=1} \underbrace{\varphi(2p-1)}_{=2p-2} = 2p-2$.

$n+2 = 4p$. $\gcd(4,p) = 1$, since p is odd. Hence
$\varphi(n+2) = \underbrace{\varphi(4)}_{2} \underbrace{\varphi(p)}_{p-1} = 2(p-1) = 2p-2$.

The equality $\varphi(n) = \varphi(n+2)$ follows. $\square$

3) Suppose the RSA algorithm is used with modulus $n = \underbrace{91}_{13\cdot 7}$

$\varphi(n) = (13-1)(7-1) = 72.$ $\boxed{72 = 2^3 \cdot 3^2}$

(a) The encription exponent e needs to satisfy $\gcd(e, \varphi(n)) = 1$, or equivalently, $2 \nmid e$ and $3 \nmid e$. Four possible values for e are:

$e = 5, 7, 11, 13.$

(b) Let $e = 17$,

$10^e = 10^{17}$

$17 = 2^4 + 1$

$10^2 \equiv 9 \pmod{91}$

$10^4 \equiv 9^2 = 81 \pmod{91}$

$10^8 \equiv 81^2 \equiv (-10)^2 \equiv 100 \equiv 9 \pmod{91}$

$10^{16} \equiv 9^2 = 81 \pmod{91} \equiv -10$

$10^{17} \equiv -100 = 82 \pmod{91}$

$82^{17} \equiv -9^{17}$

$9^2 \equiv 81 \pmod{91}$

$9^4 \equiv (-10)^2 \equiv 100 \equiv 9 \pmod{91}$

$9^8 \equiv 81 \pmod{91} \equiv -10 \pmod{91}$

$9^{16} \equiv (-10)^2 \equiv 9 \pmod{91}$,

$-9^{17} \equiv -9^{16} \cdot 9 \equiv -9 \cdot 9 \equiv 10 \pmod{91}$

(c) We find $\overline{17}^{-1} \pmod{\varphi(n) = 72}$ using the E.E.A

$72x_i + 17y_i = r_i$

x_i	y_i	r_i	q_i
1	0	72	
0	1	17	
1	-4	4	4
-4	17	1	4

$(-4)72 + 17 \cdot 17 = 1$

So $\overline{17}^{-1} = \overline{17}$ in $\mathbb{Z}_{72}$,

So the decoding exponent is 17 as well.

3

4) (a) Show that the order of any non zero element in $\mathbb{Z}_{23}$ is 1, 2, 11, or 22.

Proof: 23 is a prime. If $\bar{a} \neq \bar{0}$, then $\bar{a}^{22} = \bar{1}$, by Fermat's Little Theorem.

Hence $\text{ord}(\bar{a}) \mid \underset{\substack{\shortparallel \\ 2\cdot 11}}{22}$, by a Theorem.

The only positive integers dividing 22 are 1, 2, 11, and 22.

(b) $\bar{5}$ is a primitive root in $\mathbb{Z}_{23}$.

$\bar{5}^2 = \overline{25} = \bar{2} \neq \bar{1}$

$\bar{5}^{11} = \bar{5}^8 \cdot \underbrace{\bar{5}^2 \cdot \bar{5}}_{\overline{10}}$

$\bar{5}^4 = \bar{2}^2 = \bar{4}$

$\bar{5}^8 = \overline{16}$

So $\bar{5}^{11} = \overline{160} = -\bar{1} \neq \bar{1}$.

So $\text{ord}(\bar{5}) \notin \{1, 2, 11\}$.

It follows from part (a) that $\text{ord}(\bar{5}) = 22$.

Hence, $\bar{5}$ is a primitive root in $\mathbb{Z}_{23}$.

(c) $\operatorname{ord}(\bar{5}^{j}) = \dfrac{\operatorname{ord}(\bar{5})}{\gcd(j, \operatorname{ord}(\bar{5}))} = \dfrac{22}{\gcd(j, 22)}$

Assume, $1 \le j \le 22$.

Then $\bar{5}^{j}$ is a primitive root $\Leftrightarrow \gcd(j, 22) = 1$.

$\Leftrightarrow j \in \{1, 3, 5, 7, 9, 13, 17, 19, 21\}$.

(d) $\operatorname{ord}(\bar{5}^{14}) = \dfrac{22}{\gcd(14, 22)} = \dfrac{22}{2} = 11$.