Problem 1 (16 points)

(a, 4pts) True of false:

$$\forall p, p \text{ prime} \geq 2: \forall a \in \mathbb{Z}_p: a^2 \equiv 1 \pmod{p} \Longrightarrow a \equiv 1 \pmod{p} \quad \text{or} \quad a \equiv p-1 \pmod{p}.$$

Please explain.

True: $p \mid a^2-1 = (a+1)(a-1) \Rightarrow$

2pts 2pts

$p \mid a+1$ or $p \mid a-1$

False for comp. p: no credit $\Rightarrow a \equiv p-1$ or $a \equiv 1$

(b, 4pts) Please show that $2821 = 7 \cdot 13 \cdot 31$ is a Carmichael number.

$2821 = p_1 p_2 p_3$

$p_1 - 1 = 6 \mid 2820 = 10 \cdot 3 \cdot 94$

$p_2 - 1 = 12 \mid 10 \cdot 3 \cdot 2 \cdot 47$

$p_3 - 1 = 30 \mid 10 \cdot 3 \cdot 94$

(c, 4pts) Please show that 3^{400} ends with 001 when written as a number with decimal digits. [Hint: prove that $3^{400} \equiv 1 \pmod{1000}$.]

$3^{\phi(n)} \equiv 1 \pmod{n}$ +1pt.

$\phi(1000) = \phi(2^3 5^3) = 1000\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)$

$= 500 \cdot \frac{4}{5} = 400$

$\phi(1000)$ not computed −1

$3^{\phi(1000)} \equiv 1 \pmod{1000}$ since $GCD(3, 1000) = 1$

L.F.T.

(d, 4pts) Please prove that the system of linear congruences

$$\begin{aligned} 7x + 2y &\equiv 4 \pmod{n}, \quad (1) \\ 3x + y &\equiv 5 \pmod{n} \quad (2) \end{aligned}$$

is solvable for $x, y \in \mathbb{Z}_n$ for all $n \in \mathbb{Z}_{\geq 2}$.

$GCD(7 \cdot 1 - 2 \cdot 3, n)$

$= GCD(1, n)$

$= 1$

full credit

$(1) - 2 \cdot (2) \quad x \equiv -6$

$7 \cdot (2) - 3 \cdot (1) \quad y \equiv 35 - 12 = 23$

There exists a solution, $(x, y) = (-6, 23) \in \mathbb{Z}^2$

$GCD(7 \cdot 1, 2 \cdot 3) = 1$ 0pts

Problem 2 (6 points): For which $n \in \mathbb{Z}$ is $6^n + 2 \cdot 4^{2n+2} \equiv 0 \pmod{11}$? Please explain.

$$6^n + 2 \cdot 4^{2n+2} \equiv 6^n + 2 \cdot 16 \cdot 16^n$$

$$\equiv 6^n + 2 \cdot 5 \cdot 5^n$$

$$\equiv 6^n + (-1)(-6)^n$$

$$\equiv 6^n (1 + (-1)^{n+1})$$

$$\equiv \begin{cases} 0 & n+1 \text{ odd, } n \text{ even} \\ 2 \cdot 6^n \not\equiv 0 & n+1 \text{ even, } n \text{ odd} \end{cases}$$

$6^n \equiv 5^n \pmod{11}$

3 pts

5pts

1pt

Problem 3 (6 points): By completing the entries in the following table, please verify the Möbius's inversion formula for $f =$ identity function and $F = \sigma$ (sum of all positive divisors) at $n = 36 = 2^2\,3^2$:

ϕ no credit

d	$\sigma(d)$	$\mu(\frac{36}{d})$	$\mu(\frac{36}{d}) \cdot \sigma(d)$	
$1 = 2^0 \cdot 3^0$	$\sigma(1) = 1$	$\mu(2^2 3^2) = 0$	0	
$2 = 2^1 \cdot 3^0$	$\sigma(2) = 1+2 = 3$	$\mu(2^1 3^2) = 0$	0	
$4 = 2^2 \cdot 3^0$	$\sigma(4) = 1+2+4 = 7$	$\mu(2^0 3^2) = 0$	0	
$3 = 2^0 \cdot 3^1$	$\sigma(3) = 1+3 = 4$	$\mu(2^2 3^1) = 0$	0	
$6 = 2^1 \cdot 3^1$	$\sigma(6) = 1+2+3+6 = 12$	$\mu(2 \cdot 3) = 1$	12	
$12 = 2^2 \cdot 3^1$	$\sigma(12) = 1+2+4+3+6+12 = 28$	$\mu(2^0 \cdot 3^1) = -1$	-28	-16
$9 = 2^0 \cdot 3^2$	$\sigma(9) = 1+3+9 = 13$	$\mu(2^2 3^0) = 0$	0	
$18 = 2^1 \cdot 3^2$	$\sigma(18) = 1+2+3+6+9+18 = 39$	$\mu(2^1 3^0) = -1$	-39	-45
$36 = 2^2 \cdot 3^2$	$\sigma(36) = 1+2+4+3+6+12+9+18+36 = 91$	$\mu(2^0 3^0) = 1$	91	
	$\sum_{d \mid 36 \text{ and } d \geq 1} \mu(\frac{36}{d}) \cdot \sigma(d)$	$=$	36	

3pts | 2pts | 1pt

Problem 4 (8 points): Consider $2310 = 14 \cdot 11 \cdot 15$ and let $a \in \mathbb{Z}_{2310}$ with

$$a \equiv 13 \pmod{14},$$
$$a \equiv 4 \pmod{11},$$
$$a \equiv 1 \pmod{15}.$$

Please compute $y_0 \in \mathbb{Z}_{14}$, $y_1 \in \mathbb{Z}_{11}$ and $y_2 \in \mathbb{Z}_{15}$ such that

$$a = y_0 + y_1 \cdot 14 + y_2 \cdot 14 \cdot 11.$$

Please show all your work.

Lagrange: no credit

$y_0 = 13$ 1pt

$13 + y_1 \cdot 14 \equiv 4 \pmod{11}$

$3 \cdot y_1 \equiv 4 - 13 \equiv -9 \equiv 2 \pmod{11}$

$\underbrace{4 \cdot 3}_{\equiv 1} y_1 \equiv 4 \cdot 2 \equiv 8 \pmod{11}$

$y_1 = 8$ 3pts

$13 + 8 \cdot 14 + y_2 \cdot 14 \cdot 11 \equiv 1 \pmod{15}$

$-2 + 8 \cdot (-1) + y_2 \cdot (-1)(-4) \equiv 1 \pmod{15}$

$4 y_2 \equiv 1 + 10 \pmod{15}$

$\underbrace{4 \cdot 4}_{\equiv 1} y_2 \equiv 4 \cdot 11 \equiv 4 \cdot (-4) \equiv -16 \equiv 14 \pmod{15}$

$y_2 = 14$ 4pts

Problem 5 (5 points): The Miller-Rabin algorithm is a *randomized algorithm of the Las Vegas kind* for the proving compositeness of an integer. Please explain what that means.

It means that in its computation, the algorithm uses random bits. The random bits speed the discovery of a witness of compositeness +1 but the algorithm is always correct. +2 For composite inputs, it produces a proof of compositeness, probably fast. +2

Monte Carlo

+2

Problem 6 (5 points): Please consider the following instance of the RSA: the public modulus is $n = 91$ $(= 7 \cdot 13)$ and the public (enciphering) exponent is $k = 17$. Please compute the private deciphering exponent j such that $(M^{17})^j \equiv M \pmod{91}$ (at least for all $M \in U_{91}$). Please show your work.

$j = k^{-1} \pmod{\phi(n)}$

$\phi(91) = 6 \cdot 12 = 72$

72		1	0
17	2	0	1
4	4	1	−4
1	4	−4	17

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

$j = 17$

$17^{-1} \bmod 91 = 75$ +2

$j \equiv 17^{-1} \pmod{72}$ 4 pts

$j = \frac{1 + 9\,\phi(n)}{k}$ +2 pts