Problem 1 (12 points)

(a, 4pts) True of false:

$$\forall p, p \text{ prime} \geq 5 : \forall a \in \mathbb{Z}_p : a^3 \equiv 1 \pmod{p} \Longrightarrow a \equiv 1 \pmod{p}.$$

Please explain.

False. $2^3 = 1 \pmod 7$ and $2 \not\equiv 1 \pmod 7$

2pts

$\| \| \|$ 2pts

4^3

p not prime

−1pt

(b, 4pts) Please compute residues $x, y \in \mathbb{Z}_{10}$, or prove that none exist, such that $3x+4y \equiv 5 \pmod{13}$ and $6x+7y \equiv 8 \pmod{13}$. Please show all your work.

$3x+4y \equiv 5$

$6x+7y \equiv 8 \quad (-6)$

$-\ 3x + 7\cdot(-6)y \equiv 8\cdot(-6)$

$46y \equiv 53$

$36+8 = 44 \equiv 5$

$6\cdot 2 \equiv 12 \equiv -1 \pmod{13}$

$6\cdot(-2) \equiv 1, \quad 6\cdot(-6) \equiv -10 \equiv 3$

$7y \equiv 1$

$2\cdot 7y \equiv 2$

$\boxed{y \equiv 2}$

$6\cdot(-1) + 7\cdot 2 \equiv 8$

$6x + 2\cdot 7 = 8$

$6x \equiv 7$

$x \equiv (-2)\,7 \equiv -14 \equiv -1 \equiv 12$

calc. mistakes

−2

(c, 4pts) Please compute $7^{10^{10}}$ mod 10. Please show your work. [Hint: use Euler's theorem.]

$7^{\phi(10)} \equiv 7^4 \equiv 1 \pmod{10}$

Confusion w. $\mathbb{Z}_{10}$: credit

$(7^4)^{10^{10}/4} \equiv 1 \pmod{10}$

bad explan.

−1 − −3

Problem 2 (6 points): For which $n \in \mathbb{Z}$ is $2 \cdot 3^{n+1} + 4^n \equiv 0 \pmod 7$? Please explain.

$$2 \cdot 3^{n+1} + 4^n \equiv 6 \cdot 3^n + (-3)^n$$
$$\equiv (6 + (-1)^n)\, 3^n \equiv \begin{cases} 0 & \text{if } n \text{ even} \\ 5 \cdot 3^n \not\equiv 0 & \text{if } n \text{ odd} \end{cases}$$

even 2pts
Proof 3pts
odd $\not\equiv 0$ 1pt

Problem 3 (6 points): By completing the entries in the following table, please verify Gauss's theorem for Euler's totient function ϕ and its associated Möbius's inversion formula for $n = 72$:

d	$\phi(d)$	$\mu(d)$	$\mu(d) \cdot \frac{72}{d}$
$1 = 2^0 \cdot 3^0$	1	1	72
$2 = 2^1 \cdot 3^0$	1	-1	-36
$4 = 2^2 \cdot 3^0$	2	0	0
$8 = 2^3 \cdot 3^0$	4	0	0
$3 = 2^0 \cdot 3^1$	2	-1	-24
$6 = 2^1 \cdot 3^1$	2	1	12
$12 = 2^2 \cdot 3^1$	$(2^2-2)(3-1) = 4$	0	0
$24 = 2^3 \cdot 3^1$	$(2^3-2^2)(3-1) = 8$	0	0
$9 = 2^0 \cdot 3^2$	$3^2 - 3 = 6$	0	0
$18 = 2^1 \cdot 3^2$	$(2-1)(3^2-3) = 6$	0	0
$36 = 2^2 \cdot 3^2$	$(2^2-2)(3^2-3) = 12$	0	0
$72 = 2^3 \cdot 3^2$	$(2^3-2^2)(3^2-3) = 24$	0	0
$\sum_{d\mid 72 \text{ and } d\geq 1}$	72		$24 = \phi(72)$

3pts 3pts

Problem 4 (8 points): Consider $1716 = 13 \cdot 12 \cdot 11$ and let $a \in \mathbb{Z}_{1716}$ with

$$\begin{aligned} a &\equiv 9 \pmod{13}, \\ a &\equiv 7 \pmod{12}, \\ a &\equiv 3 \pmod{11}. \end{aligned}$$

Please compute $y_0 \in \mathbb{Z}_{13}$, $y_1 \in \mathbb{Z}_{12}$ and $y_2 \in \mathbb{Z}_{11}$ such that

$$a = y_0 + y_1 \cdot 13 + y_2 \cdot 13 \cdot 12.$$

Please show all your work.

1pt

$y_0 = 9$

$9 + 13 \cdot y_1 \equiv 7 \pmod{12}$

$y_1 \equiv -2 \equiv 10 \pmod{12}$ 3pts

$9 + 13 \cdot 10 + 13 \cdot 12 \cdot y_2 \equiv 3 \pmod{11}$

$-2 + 2 \cdot (-1) + 2 \cdot 1 \; y_2 \equiv 3 \pmod{11}$

$2 \; y_2 \equiv 7 \pmod{11}$

11	1	0	
2	0	1	
1	5	1	-5

$11 + (-5) \cdot 2 = 1$

$2^{-1} \bmod 11 = 6$

$y_2 \equiv (-4) \cdot 6 \equiv -24 \equiv 9$

4pts

no penalty if y_1 is incorrect

Problem 5 (9 points): This problem shows an instance of the Miller-Rabin Monte Carlo primality test. Let $n = 1105$ and $a = 511 \in \mathbb{Z}_{1105}$. Note that $n - 1 = 1104 = 2^4 \cdot 69$. The following has been computed by repeated squaring modulo n:

$$a^{69} \equiv 511^{69} \equiv 766 \pmod{1105} \quad \text{and} \quad 766^2 \equiv 1 \pmod{1105}. \tag{1}$$

(a, 4pts) Please explain why (1) already proves that $n = 1105$ is a composite integer.

Because $1105 \mid \underbrace{(766+1)}_{765} \cdot \underbrace{(766-1)}_{767}$

which is not possible if 1105 is prime

(b, 5pts) Using (1), please compute a non-trivial factor of 1105. Please show all your work.

1105
765
340 1
680
85 2
340 4
0

GCD(1105, 765)
= 85

1105 : 85 = 13
85
255
255
0

$1105 = 5 \cdot 13 \cdot 17$

Factorization w/o (1) +2

One factor +1

Problem 6 (5 points): Please prove: if for an integer $N \geq 2$ the integer $2^N + 1$ is a prime number, then N must be a pure power of 2, i.e., there exists an integer $n \geq 1$ such that $N = 2^n$ (N has no odd factor > 1).

Suppose $N = u \cdot 2^n$, u odd, $u > 1$, $n \geq 0$

$$2^N + 1 \equiv \left(2^{2^n}\right)^u + 1 \equiv (-1)^u + 1 \equiv 0 \pmod{2^{2^n}+1}$$

So $2^{2^n}+1 \mid 2^N+1$ and $2^{2^n}+1 \geq 2^{2^0}+1 = 3$