2007

Problem 1 (16 points)

(a, 4pts) True of false:

$$\forall m \in \mathbb{Z}_{\geq 2}, a,b,c \in \mathbb{Z}_m \colon c \neq 0 \text{ and } ac \equiv bc \pmod{m} \Longrightarrow a \equiv b \pmod{m}.$$

Please explain.

False:

$a=0,\ b=2,\ c=2,\ m=4$

$0 \cdot 2 \equiv 2 \cdot 2 \pmod 4$ but $0 \not\equiv 2 \pmod 4$

(b, 4pts) Please compute all solutions $x \in \mathbb{Z}_{11}$ for

$$7 \cdot x^2 \equiv 10 \pmod{11}.$$

Please show your work.

x	0	1	2	3	4	5	6
x^2	0	1	4	9	5	3	3
$7x^2$	0	7	6	8	2	10	10

only 2 solutions

$x=5$ and $x=6$

(c, 4pts) Please compute $3^{2^{10}}$ mod 10. [Hint: use Euler's theorem.]

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

$3^{2^{10}} \equiv (3^{2^2})^{2^8} \equiv 1 \pmod{10}$

(d, 4pts) True or false: $1729 = 7 \cdot 13 \cdot 19$ is a Carmichael number. Please explain.

True by HW3

$1729 = (6k+1)(12k+1)(18k+1)$ for $k=1$

and 7, 13, 19 are prime.

2007

Problem 2 (6 points): For which integers $n \geq 0$ is $7^{2n+1} - 6^{n+1}$ divisible by 43? Please justify your answer.

$$
\begin{aligned}
7^{2n+1} - 6^{n+1} &\equiv 49^n \cdot 7 - 6^n \cdot 6 \\
&\equiv 6^n (7-6) \\
&\equiv 6^n \\
&\not\equiv 0 \pmod{43}
\end{aligned}
$$

For <u>no</u> $n \geqslant 0$.

Problem 3 (6 points): Please make a table of all positive divisors d of $140 = 2^2 \cdot 5 \cdot 7$ and the corresponding $\phi(d)$ values. Also, please verify Gauss's theorem: $140 = \sum_{d>0 \text{ and } d|140} \phi(d)$.

d	$\phi(d)$
$1 = 2^0 \cdot 5^0$	1
$2 = 2^1 \cdot 5^0$	1
$4 = 2^2 \cdot 5^0$	2
$5 = 2^0 \cdot 5^1$	4
$10 = 2^1 \cdot 5^1$	4
$20 = 2^2 \cdot 5^1$	$20(1-\frac{1}{2}) \cdot (1-\frac{1}{5}) = 8$
$7 = 2^0 \cdot 5^0 \cdot 7$	6
$14 = 2^1 \cdot 5^0 \cdot 7$	$14(1-\frac{1}{2})(1-\frac{1}{7}) = 6$
$28 = 2^2 \cdot 5^0 \cdot 7$	$28(1-\frac{1}{2})(1-\frac{1}{7}) = 12$
$35 = 2^0 \cdot 5^1 \cdot 7$	$35(1-\frac{1}{5})(1-\frac{1}{7}) = 24$
$70 = 2^1 \cdot 5^1 \cdot 7$	$70 \cdot (1-\frac{1}{2})(1-\frac{1}{5})(1-\frac{1}{7}) = 24$
$140 = 2^2 \cdot 5^1 \cdot 7$	$140 \cdot (1-\frac{1}{2})(1-\frac{1}{5})(1-\frac{1}{7}) = 48$

$\Sigma = 140$

2007

Problem 4 (8 points): Consider $360 = 5 \cdot 8 \cdot 9$ and let $a \in \mathbb{Z}_{360}$ with

$$\begin{aligned} a &\equiv 4 \pmod 5, \\ a &\equiv 2 \pmod 8, \\ a &\equiv 8 \pmod 9. \end{aligned}$$

Please compute $y_0 \in \mathbb{Z}_5$, $y_1 \in \mathbb{Z}_8$ and $y_2 \in \mathbb{Z}_9$ such that

$$a = y_0 + y_1 \cdot 5 + y_2 \cdot 5 \cdot 8.$$

Please show all your work.

$y_0 = 4$

$4 + 5 \cdot y_1 \equiv 2 \pmod 8$

$5 y_1 \equiv -2 \equiv 6 \pmod 8$

$5 \cdot 5\, y_1 \equiv \boxed{y_1 = 5 \cdot 6 \equiv 6} \pmod 8$

Check $4 + 5 \cdot 6 = 34 \equiv 2 \pmod 8$

$$\begin{array}{cccc} & 8 & 1 & 0 \\ & 5 & 0 & 1 \\ 1 & 3 & 1 & -1 \\ 1 & 2 & -1 & 2 \\ 1 & 1 & 2 & -3 \\ 2 & 0 & & \end{array}$$

$2 \cdot 8 - 3 \cdot 5 = 1$

$5^{-1} \equiv -3 \equiv 5 \pmod 8$

check: $5 \cdot 5 = 25 \equiv 1 \pmod 8$

$4 + 5 \cdot 6 + 5 \cdot 8 \cdot y_2 \equiv 8 \pmod 9$

$5 \cdot 8\, y_2 \equiv 4 y_2 \equiv 8 - 4 - 30 \equiv 8 + 5 + 6 \equiv 1 \pmod 9$

$$\begin{array}{cccc} & 9 & 1 & 0 \\ & 4 & 0 & 1 \\ 2 & 1 & 2 & -2 \\ 4 & 0 & & \end{array}$$

$2 \cdot 9 - 2 \cdot 4 = 1$

$4^{-1} \equiv -2 \equiv 7 \pmod 9$

Check $7 \cdot 4 = 28 \equiv 1 \pmod 9$

$7 \cdot 4\, y_2 \equiv \boxed{1\ y_2 \equiv 7} \pmod 9$

$a = 4 + 5 \cdot 6 + 5 \cdot 8 \cdot 7 = 314$

2007

Problem 5 (8 points): Consider the following instance of the RSA: the public modulus is $n = 3 \cdot 11 = 33$ and the public (enciphering) exponent is $e = 7$.

(a, 4pts) Please compute the private deciphering exponent j such that $(M^e)^j \equiv M \pmod{n}$ (at least for all $M \in \mathbb{Z}_n$ that are relatively prime to n).

$\phi(n) = 2 \cdot 10 = 20$

$j \equiv e^{-1} (\bmod\ \phi(n))$

$j = 3$

	20	1	0
	7	0	1
2	6	1	-2
1	1	-1	3
6	0		

$(-1)\, 20 + 3 \cdot 7 = 1$

(b, 4pts) Please encrypt the message $M_1 = (2 \bmod 33)$. Then decrypt the produced cypher number in $\mathbb{Z}_n$. Also try to encrypt $M_2 = (3 \bmod 33)$ and then decrypt the produced cypher number; note that 3 is not relatively prime to n. Please show all your work.

$2^7 \bmod 33 = (2^5 \cdot 2^2) \bmod 33$

$= (-1) \cdot 4 \bmod 33$

$= 29$

$29^3 \bmod 33 = (-4)^3 \bmod 33$

$= -(4 \cdot 4 \cdot 2) \cdot 2 \bmod 33$

$= -(-1) \cdot 2 = 2 \bmod 33$

$3^7 \bmod 33 = 3^3 \cdot 3^3 \cdot 3 \bmod 33$

$= (-6) \cdot (-6) \cdot 3 \bmod 33 = 3 \cdot 3 \bmod 33 = 9$

$9^3 \bmod 33 = 3^6 \bmod 33 = 3^3 \cdot 3^3 \bmod 33$

$= (-6) \cdot (-6) \bmod 33 = 3$