2009

Problem 1 (12 points)

(a, 4pts) True of false:

$$\forall n \in \mathbb{Z}_{\geq 2}, a \in \mathbb{Z}_n:\ a^2 \equiv 1 \pmod{n} \Longrightarrow a = 1 \text{ or } a = n-1.$$

Please explain.

$3^2 \equiv 1 \pmod{8}$

(b, 4pts) Applying Möbius's inversion formula to $F(n) = n$, namely, $f(n) = \Sigma_{d|n, d\geq 0}\, \mu(d)\frac{n}{d}$ yields what number theoretic function for f? Please explain.

$\phi(n)$ bec. $\sum_{\substack{d|n \\ d\geq 1}} \phi(d) = n$

(c, 4pts) Please show that $1105 = 5 \cdot 13 \cdot 17$ is a Carmichael number.

$p-1 \mid n-1 \Rightarrow a^{n-1} \equiv 1 \pmod{n}$

$4 \mid 1104$

$12 \mid 1104$

$16 \mid 1104$

2009

Problem 2 (6 points): For which integers $n \in \mathbb{Z}$, ~~including negative integers~~, is $2^n - 4$ divisible by 7. Please justify your answer.

$2^3 \equiv 1 \pmod 7$

$n \equiv 2 \pmod 3$

$2^0 - 4$

$2^1 - 4$

$2^2 - 4$

$2^3 - 4 \equiv 2^0 - 4$

Problem 3 (6 points): Please compute residues $x, y \in \mathbb{Z}_{11}$ such that $3x + 4y \equiv 0 \pmod{11}$ and $4x + 3y \equiv 1 \pmod{11}$. Please show all your work.

2009

Problem 4 (8 points): Consider $315 = 5 \cdot 7 \cdot 9$ and let $a \in \mathbb{Z}_{315}$ with

$$\begin{aligned} a &\equiv 3 \pmod{5}, \\ a &\equiv 5 \pmod{7}, \\ a &\equiv 7 \pmod{9}. \end{aligned}$$

Please compute $y_0 \in \mathbb{Z}_5$, $y_1 \in \mathbb{Z}_7$ and $y_2 \in \mathbb{Z}_9$ such that

$$a = y_0 + y_1 \cdot 5 + y_2 \cdot 5 \cdot 7.$$

Please show all your work. After seeing the answer, could you have determined y_1 and y_2 without any computation?

$y_0 = 3$

$5 \equiv 3 + 5 \cdot y_1 \pmod{7}$

$2 \equiv 5 \cdot y_1 \pmod{7}$

$6 \equiv 5^{-1} \cdot 2 \equiv y_1$

$7 \equiv 3 + 5 \cdot 6 + 5 \cdot 7 \cdot y_2 \pmod{9}$

$1 \equiv 5 \cdot 7 \, y_2 \pmod{9}$

$1 \cdot (-1) \equiv y_2 \pmod{9}$

2009

Problem 5 (12 points): Consider the following instance of the RSA: the public key $K = P \cdot Q$ where P and Q are primes with $P \not\equiv 1 \pmod 5$, $Q \not\equiv 1 \pmod 5$; the public (enciphering) exponent is $Y = 5$, i.e., the ciphertext of a message M is $N = E_K(M) = (M^5 \bmod K)$. Please prove the following.

(a, 5pts) $\lambda = ((P-1)(Q-1) \bmod 5) \neq 0$
and $X = \dfrac{\mu(P-1)(Q-1)+1}{5}$ is an integer for $\mu = (4\lambda^{-1} \bmod 5)$.

$$5 \nmid P-1, \quad 5 \nmid Q-1 \Rightarrow 5 \nmid (P-1)(Q-1)$$

$$\underbrace{\mu}_{4\lambda^{-1}} \underbrace{(P-1)(Q-1)}_{\lambda} + 1 \equiv 0 \pmod 5$$

(b, 5pts) The integer X as defined in (a) is the private (recovery) exponent, that is for all residues $M \in \mathbb{Z}_K$ with $\mathrm{GCD}(M,K) = 1$ one has $(M^5)^X \equiv M \pmod K$.

$$(M^5)^X = M^{\mu(P-1)(Q-1)+1}$$
$$\equiv (M^{\phi(K)})^{\mu} \cdot M$$
$$\equiv M \pmod K$$

(c, 2pts) What is X in this case (namely, $Y = 5$) for $P = 3$ and $Q = 5$?

$$\lambda \equiv 2 \cdot 4 \equiv 3 \pmod 5$$
$$\mu = 4 \cdot 3^{-1} \pmod 5$$
$$= 3$$

$$X = \frac{3 \cdot 8 + 1}{5} = 5$$