2008

**Problem 1** (12 points)

(a, 4pts) True of false:

$$\forall n \in \mathbb{Z}_{\geq 2}, a, b \in \mathbb{Z}\colon a \equiv b \pmod{n} \Longrightarrow \gcd(a,n) = \gcd(b,n).$$

Please explain.

True

$a \equiv b \pmod n \Rightarrow a = b + qn$

$g = GCD(a,n)$ : $g \mid a - qn = b \Rightarrow g \mid e = GCD(b,n)$

$e = GCD(b,n)$ : $e \mid b + qn = a \Rightarrow e \mid g$

$\Rightarrow g = e$.

(b, 4pts) Please show that $\phi(10^i) = 4 \cdot 10^{i-1}$ for all $i \in \mathbb{Z}_{>0}$, where $\phi$ is Euler's totient function.

$10^i = 2^i \cdot 5^i$

$\phi(2^i \cdot 5^i) = \phi(2^i) \cdot \phi(5^i)$

$= (2^i - 2^{i-1})(5^i - 5^{i-1})$

$= 2^{i-1} 5^{i-1} (5-1) = 4 \cdot 10^{i-1}$

(c, 4pts) Please give the definition for being a pseudo-prime and the definition for being Carmichael number.

Pseudo-prime: composite $n$ s.t. $2^n \equiv 2 \pmod n$

Carmichael: composite $n$ s.t.

$\forall a, GCD(a,n) = 1 \quad a^{n-1} \equiv 1 \pmod n$

2008

**Problem 2** (6 points): Please prove for all integers $n \geq 1$ that $5^{2n} + 3 \cdot 2^{5n-2}$ is divisible by 7.

$m = n - 1 \geq 0$

$5^{2(m+1)} + 3 \cdot 2^{5(m+1)-2}$

$(25)^m \cdot 25 + 3 \cdot 32^m \cdot 2^3$

$4^m \cdot 4 + 3 \; 4^m \cdot 1 = 7 \cdot 4^m \equiv 0$

**Problem 3** (6 points): Please compute residues $x, y \in \mathbb{Z}_7$ such that $3x + 5y \equiv 0 \pmod 7$ and $5x + y \equiv 1 \pmod 7$. Please show all your work.

$y \equiv 1 - 5x$

$3x + 5(1 - 5x) \equiv 0$

$(3 - 4)x + 5 \equiv 0$

$(-1)x \equiv -5$

$x \equiv 5$ $\qquad\qquad$ $y \equiv -24 \equiv 4$

2008

**Problem 4** (8 points): Consider $504 = 7 \cdot 8 \cdot 9$ and let $a \in \mathbb{Z}_{504}$ with

$$a \equiv 6 \pmod 7, \quad a \equiv 7 \pmod 8, \quad a \equiv 8 \pmod 9.$$

Please compute $y_0 \in \mathbb{Z}_7$, $y_1 \in \mathbb{Z}_8$ and $y_2 \in \mathbb{Z}_9$ such that

$$a = y_0 + y_1 \cdot 7 + y_2 \cdot 7 \cdot 8.$$

Please show all your work. After seeing the answer, is there an easy way to interpret the result?

$y_0 = 6$

$6 + y_1 \cdot 7 \equiv 7 \pmod 8$

$\underbrace{7 \cdot 7}_{1} \cdot y_1 \equiv \underbrace{7 \cdot (7-6)}_{7} \pmod 8$ $\qquad y_1 = 7 \pmod 8$

---

$\underbrace{6 + \underbrace{7 \cdot 7}_{4}}_{1} + y_2 \underbrace{7 \cdot 8}_{2} \equiv 8 \pmod 9$

$2 y_2 \equiv 7 \pmod 9$

$2 \cdot 5 \cdot y_2 \equiv 5 \cdot 7 \pmod 9$

$y_2 \equiv 35 \equiv 8 \pmod 9$

$a = 6 + 7 \cdot 7 + 7 \cdot 8 \cdot 8 = 503 \equiv -1 \pmod{504}$

$-1 \equiv 6 \pmod 7$

$-1 \equiv 7 \pmod 8$

$-1 \equiv 8 \pmod 9$

2008

**Problem 5** (12 points):

(a, 4pts) Consider the following instance of the RSA: the public modulus is $K = 55$ and the public (enciphering) exponent is $W = 9$. Please compute the private deciphering exponent $X$ such that $(M^9)^X \equiv M \pmod{55}$ (at least for all $M \in \mathbb{Z}_{55}$ that are relatively prime to $K$).

$9^{-1} \bmod \phi(55) = 9^{-1} \bmod \phi(5 \cdot 11)$

$= 9^{-1} \bmod 4 \cdot 10$

$= 9 \bmod 40$

| | | | |
|---|---|---|---|
| 40 | 2 | 1 | 0 |
| 9 | | 0 | 1 |
| 4 | 4 | 1 | -4 |
| 1 | 2 | -2 | 9 |

$(-2) \cdot 40 + 9 \cdot 9 = 1$

(b, 4pts) In the RSA, for all public keys $K$ and encryption exponents $W$ it is unwise to encrypt messages $M$ that are not relatively prime to $K$. Why? Please explain.

Because $1 \neq \mathrm{GCD}(K, M^W \bmod K)$

(c, 4pts) The original 1977 RSA public key crypto system has the flaw that it is ***malleable***. What does that mean?

One can encrypt $\alpha \cdot M$ from $K$ and $E_K(M)$ without knowing $M$:

$E_K(\alpha \cdot M) = \alpha^W \cdot E_K(M) \bmod K$