2016

Problem 1 (16 points)

(a, 4pts) Let p be a prime number ≥ 19 with $p \equiv 4 \pmod 5$.

(i) please prove that $3(p-1)+1 = 3p-2$ is divisible by 5.

(ii) please prove that for all $a \in \mathbb{Z}_p$ we have for $b = a^{(3p-2)/5} \bmod p$ that $b^5 \equiv a \pmod p$.

(i) $3(p-1)+1 \equiv 3\cdot(4-1)+1 \equiv 10 \equiv 0 \pmod 5$

(ii) $\left(a^{(3p-2)/5}\right)^5 \equiv a^{3(p-1)+1} \equiv \left(a^{p-1}\right)^3 \cdot a \equiv \begin{cases} 0 & \text{if } a \equiv 0 \pmod p \\ 1^3 \cdot a \equiv a \pmod p & \text{if } a \not\equiv 0 \pmod p \end{cases}$

(b, 4pts) The integer 341 is a pseudo-prime (to base 2) but **not** a Carmichael number. Please explain what both mean.

341 is a pseudoprime $\Leftrightarrow$ $\begin{cases} 341 \text{ is composite} \\ 2^{340} \equiv 1 \pmod{341} \end{cases}$

341 is not a C.N. $\Leftrightarrow \exists a \in \mathbb{Z}_{341}, \gcd(a, 341) = 1$ and $a^{340} \not\equiv 1 \pmod{341}$

(c, 4pts) Please show that $3^{100} \equiv 1 \pmod{1000}$. [Hint: factor the modulus $1000 = 8 \cdot 125$.]

$3^{100} \equiv (3^2)^{50} \equiv 1^{50} \equiv 1 \pmod 8$

$\phi(125) = 5^3 - 5^2 = 100$, $\gcd(3, 125) = 1$

$3^{100} = 3^{\phi(125)} \equiv 1 \pmod{125}$

By CRT $3^{100} \equiv 1 \pmod{8 \cdot 125}$

(d, 4pts) Please compute residues $x, y \in \mathbb{Z}_8$, or prove that none exist, such that

$$\begin{aligned} & x + 3y \equiv 5 \pmod 8 \\ \text{and} \quad & 5x + y \equiv 6 \pmod 8. \end{aligned} \quad +$$

$6x + 4y \equiv 11 \equiv 3 \pmod 8$

$\Leftrightarrow 8 \mid 2(3x+2y) - 3$ impossible for odd $2(3x+2y)-3$

2016

Problem 2 (6 points): Please prove that there are infinitely many composite integers that are $\equiv 5 \pmod 6$.

$30k+5$ is div by 5 for all $k \geq 1$

$35^{2k+1} \equiv (35^2)^k \cdot 35 \equiv (5^2)^k \, 5 \equiv 1^k \cdot 5 \equiv 5 \pmod 6$

and div. by 5 and 7

$11^{2k+1} \equiv (-1)^{2k+1} \equiv -1 \equiv 5 \pmod 6$ div by 11

Felipe $5^{2k+1} \equiv (-1)^{2k+1} \equiv -1 \equiv 5 \pmod 6$ 5

Problem 3 (6 points): By completing the $3 \cdot 10$ entries in the following table in terms of prime numbers p and q with $p \neq q$, please verify Gauss's Theorem for Euler's ϕ function and its associate Möbius inversion formula for $n = p^2q^2$:

	d	$\phi(d)$	$\mu(d)$	$\mu(d) \cdot \frac{n}{d}$
1.	1	1	1	p^2q^2
2.	p	$p-1$	-1	$-pq^2$
3.	p^2	p^2-p	0	0
4.	q	$q-1$	-1	$-p^2q$
5.	pq	$(p-1)(q-1)$	1	pq
6.	p^2q	$(p^2-p)(q-1)$	0	0
7.	q^2	q^2-q	0	0
8.	pq^2	$(p-1)(q^2-q)$	0	0
9.	p^2q^2	$(p^2-p)(q^2-q)$	0	0
10.	$\sum$ d divides p^2q^2 and $d \geq 1$	p^2q^2	0	$p^2q^2 - pq^2 - p^2q + pq$

2016

Problem 4 (8 points): Consider $2310 = 5 \cdot 6 \cdot 7 \cdot 11$ and let $a \in \mathbb{Z}_{2310}$ with

$$\begin{aligned} a &\equiv 4 \pmod 5, \\ a &\equiv 5 \pmod 6, \\ a &\equiv 4 \pmod 7, \\ a &\equiv 7 \pmod{11}. \end{aligned}$$

Please compute $y_0 \in \mathbb{Z}_5$, $y_1 \in \mathbb{Z}_6$, $y_2 \in \mathbb{Z}_7$ and $y_3 \in \mathbb{Z}_{11}$ such that

$$a = y_0 + y_1 \cdot 5 + y_2 \cdot 5 \cdot 6 + y_3 \cdot 5 \cdot 6 \cdot 7.$$

Then compute a. Please show all your work.

$y_0 = 4$

$4 + 5 \cdot y_1 \equiv 5 \pmod 6$

$(-1)(-1) y_1 \equiv (-1)(5-4) \pmod 6$

$y_1 \equiv 5$

$4 + 5 \cdot 5 + 5 \cdot 6 \cdot y_2 \equiv 4 \pmod 7$

$(-2)(-1) y_2 \equiv 4 - 4 - (-2)(-2) \pmod 7$

$(-3) 2 \, y_2 \equiv (-3) 3 \pmod 7$

$y_2 \equiv 5 \pmod 7$

$4 + \underbrace{5 \cdot 5}_{\equiv 3} + \underbrace{5 \cdot 6 \cdot 5}_{\equiv 3 \cdot 6 \equiv 7} + \underbrace{5 \cdot 6 \cdot 7}_{\equiv 8 \equiv 1} y_3 \equiv 7 \pmod{11}$

$y_3 \equiv 7 - 7 - 3 - 4 \equiv -7 \equiv 4 \pmod{11}$

$a = 4 + 25 + 30 \underbrace{(5 + 4 \cdot 7)}_{33} = 29 + 990 = 1019$

2016

Problem 5 (5 points): Let $k = 2^4 + 2^2 + 2 + 1 = 23$. Please show how one can compute a^k mod n with 7 multiplications of residues modulo n.

1 $a^2 \bmod n = b$

2 $a^4 \bmod n = b^2 \bmod n = c$

3 $a^8 \bmod n = c^2 \bmod n = d$

4 $a^{16} \bmod n = d^2 \bmod n = e$

$a^k \equiv a^{16} \cdot a^4 \cdot a^2 \cdot a \equiv e \cdot c \cdot b \cdot a \pmod n$

+3 multipl.

a^2	
a^3	
a^5	
a^{10}	
a^{20}	
a^{23}	
mod n	6

Problem 6 (5 points): Please consider the following (toy) instance of the RSA: the public modulus is $n = 77$ and the public (enciphering) exponent is $k = 43$. Please compute the private deciphering exponent j such that $(M^{43})^j \equiv M \pmod{77}$ (at least for all $M \in U_{77}$). Please show your work.

$j = 43^{-1} \bmod \phi(77)$

$\phi(77) = \phi(7)\,\phi(11) = 6 \cdot 10 = 60$

60		1	0
43		0	1
17	1	1	−1
9	2	−2	3
8	1	3	−4
1	1	−5	7

$(-5)\,60 + 7 \cdot 43$

$= -300 + 301 = 1$

$j = 7$