$3^{-1} \bmod 16 \equiv -5 \equiv 11$

$(a^{11})^3 \equiv a^{33} \equiv a^{2\cdot 16} \cdot a \equiv a \pmod{17}$

2010

x	$10 \equiv -7$	$11 \equiv -6$	$12 \equiv -5$
x^3	$-3 \equiv 14$	$-12 \equiv 5$	$-6 \equiv 11$
x	$13 \equiv -4$	$14 \equiv -3$	$15 \equiv -2$
x^3	$-13 \equiv 4$	$-10 \equiv 7$	$-8 \equiv 9$
	$16 \equiv -1$		
	$-1 \equiv 16$		

Problem 1 (12 points)

(a, 4pts) True of false: for all $a \in \mathbb{Z}_{17}$ the cubic equation

2010

$$x^3 \equiv a \pmod{17}$$

has a solution $x \in \mathbb{Z}_{17}$. Please explain.

TRUE

x	0	1	2	3	4	5	6	7	8	$9 \equiv -8$
$x^3 \bmod 17$	0	1	8	10	13	6	12	3	2	$-2 \equiv 15$

This is also the RSA for exp. 3: $GCD(3, \phi(17))$
$= GCD(3, 16) = 1$

(b, 4pts) Please compute residues $x, y \in \mathbb{Z}_{10}$, or prove that none exist, such that $3x + 4y \equiv 0 \pmod{10}$ and $x + 2y \equiv 1 \pmod{10}$. Please show all your work.

$3x + 4y \equiv 0$

$2x + 4y \equiv 2$

$x \equiv -2 \equiv 8 \pmod{10}$

$2(4 + y) \equiv 1 \pmod{10}$

$0 \equiv 1 \pmod{2}$

No solution

(c, 4pts) True or false: Let $n \in \mathbb{Z}_{\geq 2}$. If $\forall a \in \mathbb{Z}_n$: $a^n \equiv a \pmod{n}$ then n must be a prime number. Please explain.

False for Carmichael numbers which are absolute pseudoprimes

2010

Problem 2 (6 points): Please prove for all prime and composite Fermat numbers $F_n = 2^{2^n} + 1$ that

$$2^{F_n - 1} \equiv 1 \pmod{F_n} \quad \text{for all} \quad n \geq 0.$$

Hint: for $M = 2^n$ first prove that $2^{2M} \equiv 1 \pmod{2^M + 1}$.

$$2^M \equiv -1 \pmod{2^M+1} \quad \text{so} \quad 2^{2M} \equiv (-1)^2 \equiv 1 \pmod{2^M+1}$$

$$2^{F_n - 1} = 2^{(2^{2^n})} \equiv \left(2^{2M}\right)^{2^{2^n}/(2M)}$$

$$\equiv \left(2^{2M}\right)^{2^{2^n-(n+1)}} \equiv 1 \pmod{F_n}$$

Problem 3 (6 points): Please verify the following identity, where ϕ is Euler's totient function and μ is Möbius's function:

$$\phi(60) = \sum_{d|n \text{ and } d \geq 1} \mu(d) \frac{60}{d}$$

Please show your work.

$60 = 2^2 \cdot 3 \cdot 5$

$\phi(60) =$

$60 \cdot \left(1-\frac{1}{2}\right) \cdot \left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$

$= \cancel{60}^{\cancel{12}\,2} \cdot \frac{1}{\cancel{2}} \cdot \frac{2}{\cancel{3}} \cdot \frac{4}{\cancel{5}}$

$= 16$

d	$\mu(d)$	$\frac{60}{d}$
$1 = 2^0 \cdot 3^0 \cdot 5^0$	1	60
$2 = 2^1 \cdot 3^0 \cdot 5^0$	-1	-30
$4 = 2^2 \cdot 3^0 \cdot 5^0$	0	
$3 = 2^0 \cdot 3^1 \cdot 5^0$	-1	-20
$6 = 2^1 \cdot 3^1 \cdot 5^0$	$+1$	$+10$
$12 = 2^2 \cdot 3^1 \cdot 5^0$	0	
$5 = 2^0 \cdot 3^0 \cdot 5^1$	-1	-12
$10 = 2^1 \cdot 3^0 \cdot 5^1$	$+1$	$+6$
$20 = 2^2 \cdot 3^0 \cdot 5^1$	0	
$15 = 2^0 \cdot 3^1 \cdot 5^1$	$+1$	$+4$
$30 = 2^1 \cdot 3^1 \cdot 5^1$	-1	-2
$60 = 2^2 \cdot 3^1 \cdot 5^1$	0	
		16

2010

Problem 4 (8 points): Consider $630 = 7 \cdot 9 \cdot 10$ and let $a \in \mathbb{Z}_{630}$ with

$$\begin{aligned} a &\equiv 6 \pmod{7}, \\ a &\equiv 8 \pmod{9}, \\ a &\equiv 6 \pmod{10}. \end{aligned}$$

Please compute $y_0 \in \mathbb{Z}_7$, $y_1 \in \mathbb{Z}_9$ and $y_2 \in \mathbb{Z}_{10}$ such that

$$a = y_0 + y_1 \cdot 7 + y_2 \cdot 7 \cdot 9.$$

Please show all your work.

$y_0 = 6$

$7y_1 + 6 \equiv 8 \pmod{9}$

$y_1 \equiv 7^{-1} \cdot (8-6)$

$\equiv 4 \cdot 2 \equiv 8$

$\pmod{9}$

$7 \cdot 9 \cdot y_2 + 6 + 7 \cdot 8 \equiv 6 \pmod{10}$

$3 \cdot y_2 + 2 \equiv 6 \pmod{10}$

$y_2 \equiv 3^{-1}(6-2)$

$\equiv 7 \cdot 4 \equiv 8 \pmod{10}$

$a = \underbrace{6 + 8 \cdot 7}_{62} + \underbrace{8 \cdot 7 \cdot 9}_{\substack{56 \cdot 9 \\ 504}} = 566$

2010

Problem 5 (12 points):

(a, 4pts) Please describe the difference between a *private* key cryptosystem and a *public* key cryptosystem. How old is public key cryptography and who has invented it?

Clifford Cocks 1973 UK GCHQ
James H. Ellis, Malcolm Williamson

Whitfield Diffie & Martin Hellman 1976
RSA (Leonard Adleman)

(b, 4pts) Please consider the following instance of the RSA: the public modulus is $n = 77$ and the public (enciphering) exponent is $k = 11$. Please compute the private deciphering exponent j such that $(M^{11})^j \equiv M \pmod{77}$ (at least for all $M \in U_{77}$).

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

$11^{-1} \bmod 60 = 11 = j$

60		1	0
11		0	1
5	5	1	-5
1	2	-2	11

$-2 \cdot 60 + 11 \cdot 11 = 1$

(c, 4pts) Suppose Alice has encrypted M as $2 = (M^{11} \bmod 77)$. What is M? Please show all of Bob's computations using j from Part b.

$2^{11} \equiv 2^6 \cdot 2^5 \equiv 64 \cdot 2^5 \equiv (-13) \cdot 2^5$
$\equiv (-52) \cdot 2^3 \equiv 25 \cdot 2^3 \equiv 100 \cdot 2 \equiv 23 \cdot 2 \equiv 46$
$\pmod{77}$