S 2015

Problem 1 (16 points)

(a, 4pts) True or false:

$$\forall p, p \text{ prime} \geq 2\colon \forall a \in \mathbb{Z}_p\colon \exists x \in \mathbb{Z}_p\colon x^3 \equiv a \pmod{p}.$$

Please explain.

FALSE

$p=7$: $1^3 \equiv 1, 2^3 \equiv 1, 3^3 \equiv 6, 4^3 \equiv 1, 5^3 \equiv 6 \quad 6^3 \equiv 6$

$a=2$ is counterexample

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

TRUE: $1729 = (6k+1)(12k+1)(18k+1)$ with all factors prime

(c, 4pts) Please compute 2^{1000} mod 7, showing your work.

$2^3 \equiv 1 \pmod 7 \Rightarrow (2^3)^{333} = 2^{999} \equiv 1 \pmod 7$

$\Rightarrow 2^{1000} \equiv 2 \pmod 7$

(d, 4pts) Please compute the solution $(x, y) \in \mathbb{Z}_{11} \times \mathbb{Z}_{11}$ of the system of linear congruences

$$\begin{aligned} x + y &\equiv 10 \pmod{11}, \\ 10x + y &\equiv 2 \pmod{11}. \end{aligned}$$

$2y \equiv 1 \pmod{11} \Rightarrow (6 \cdot 2)y \equiv y \equiv 6 \pmod{11}$

$x \equiv 10 - y \equiv 4 \pmod{11}$

$(x, y) = (4, 6)$

S2015

Problem 2 (6 points): Please prove that there are infinitely many prime numbers that are $\equiv 2 \pmod 3$. [Hint: consider $3\times$ product of all odd such primes $+2$].

Let $p_1, \dots, p_t$ be all odd primes $\equiv 2 \pmod 3$. Then $3 \cdot p_1 \cdots p_t + 2 = q_1 \cdots q_s$ where q_i are odd, $q_i \notin \{p_1, \dots, p_t\}$, for otherwise q_i would divide 2. So $q_i \equiv 1 \pmod 3$ for all i, hence $q_1 \cdots q_s \equiv 1 \pmod 3$, a contradiction.

Problem 3 (6 points): By completing the $3 \cdot 13$ entries in the following table, please verify Gauss's theorem for Euler's totient function ϕ and its associated Möbius's inversion formula for $n = 140$:

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

S2015

Problem 4 (8 points): Consider $2145 = 15 \cdot 13 \cdot 11$ and let $a \in \mathbb{Z}_{2145}$ with

$$\begin{aligned} a &\equiv 13 \pmod{15}, \\ a &\equiv 3 \pmod{13}, \\ a &\equiv 7 \pmod{11}. \end{aligned}$$

Please compute $y_0 \in \mathbb{Z}_{15}$, $y_1 \in \mathbb{Z}_{13}$ and $y_2 \in \mathbb{Z}_{11}$ such that

$$a = y_0 + y_1 \cdot 15 + y_2 \cdot 15 \cdot 13.$$

Then compute a. Please show all your work.

$$\begin{array}{r} 15 \cdot 9 \\ 135 \cdot 13 \\ 405 \\ \hline 1755 \end{array}$$

$y_0 = 13$

$13 + y_1 \cdot 15 \equiv 3 \pmod{13}$

$7 \cdot 2 \cdot y_1 \equiv 7 \cdot 3 \pmod{13}$

$y_1 \equiv 8 \pmod{13}$

$13 + 8 \cdot 15 + y_2 \cdot 15 \cdot 13 \equiv 7 \pmod{11}$

$2 + \underbrace{(-3) \cdot 4}_{-1} + 4 \cdot 2 \cdot y_2 \equiv 7 \pmod{11}$

$8 y_2 \equiv 6 \pmod{11}$

$(-4)\, 8\, y_2 \equiv (-4)\, 6 \pmod{11}$

$y_2 \equiv 9 \pmod{11}$

11		1	0
8		0	1
3	1	1	-1
2	2	-2	3
1	1	3	-4

$3 \cdot 11 + (-4) \cdot 8 = 1$

$8^{-1} \equiv -4 \equiv 7 \pmod{11}$

$a = 13 + 8 \cdot 15 + 9 \cdot 15 \cdot 13$

$= 1888$

S2015

Problem 5 (5 points): The first pseudo-prime (for base 2) is 341: $2^{340} \equiv 1 \pmod{341}$, but 341 is a composite number. In fact, $2^{170} \equiv 1 \pmod{341}$ and $2^{85} \equiv 32 \pmod{341}$. Using the latter two congruences, please factor 341. Please show your work.

$32^2 \equiv (2^{85})^2 \equiv 2^{170} \equiv 1 \pmod{341}$

$(32+1)(32-1) \equiv 0 \pmod{341}$

$GCD(33, 341) = 11$

$GCD(31, 341) = 31$

$341 = 11 \cdot 31$

341
33
11 10
0 3

Problem 6 (5 points): Bob receives RSA-encrypted messages from Alice, for which he has provided Alice with a public modulus n and a public exponent k. However, Bob by mistake has chosen n to be a prime number. On the (toy) example $n = 101$, $k = 67$, and the ciphertext $E = (M^{67} \bmod 101) = 5$, please show how Charlie can compute M from the public key (n,k) and E. Your method should also work on larger keys where n is prime.

$k^{-1} \bmod \phi(n) = 67^{-1} \pmod{100}$

$= 3$

100	1	0
67	0	1
33	1	-1
1	2	-2
		3

$(M^{67})^3 \equiv M \pmod{101}$

$5^3 \equiv 24 \pmod{101}$

$(-2)100 + 3 \cdot 67 = 1$