2017

Problem 1 (17 points)

(a, 4pts) Please consider the multiplication table for non-zero residues modulo 14, that is a 13×13 matrix A with entries $a_{i,j} = (i\,j \bmod 14)$ for $1 \le i, j \le 13$.
True or false: A is a Latin square. Please explain.

False

i \ j	1	2	3	4	5	6	7	8	9	10	11	12	13
i=2	2	4	6	8	10	12	0	2	4	6	8	10	12

does not have any even residues

(b, 4pts) True of false: $2^{2016} \equiv 2018 \pmod{4034}$. Please explain. [Hint: $4034 = 2 \cdot 2017$ with 2017 a prime number.]

True: $2^{2016} \bmod 2 = 0 \equiv 2018 \pmod 2$

$2^{2016} \bmod 2017 = 1 \equiv 2018 \pmod{2017}$

By the CRT 2018 is the residue mod 4034

(c, 4pts) True or false: $\forall s, t$ such that $s \not\equiv t \pmod 2$ and $\mathrm{GCD}(s,t) = 1$: $(2st, s^2 - t^2, s^2 + t^2)$ form a **primitive** Pythagorean triple. Please explain.

TRUE: $g = \mathrm{GCD}(s^2 - t^2, s^2 + t^2)$

$\Rightarrow g \mid 2s^2$, $g \mid 2t^2 \Rightarrow g \mid 2$

$s \not\equiv t \pmod 2 \Rightarrow s^2 + t^2$ is odd

$\Rightarrow g = 1$

(d, 5pts) True or false: there exist positive integers $x, y, z \in \mathbb{Z}_{>0}$ such that $x^4 + y^4 = z^3$. Please explain.

TRUE: $4^4 + 4^4 = 2^8 + 2^8 = 2 \cdot 2^8$

$= 2^9 = 8^3$

2017

Problem 2 (5 points): The following is a trace of the computation of the Legendre symbol $\left(\frac{-122}{211}\right)$ using Jacobi's reciprocity law. Please fill in the blanks.

$\left(\frac{-122}{211}\right) = \left(\frac{-1}{211}\right)\left(\frac{122}{211}\right)$; $\left(\frac{-1}{211}\right) = \underline{(-1)^{210/2} = (-1)^{105} = -1}$

$\left(\frac{122}{211}\right) = \left(\frac{2}{211}\right)\left(\frac{61}{211}\right)$; $\left(\frac{2}{211}\right) = \underline{(-1)^{(211^2-1)/8} = (-1)^{105 \cdot 53} = -1}$

$\left(\frac{61}{211}\right)\left(\frac{211}{61}\right) = \underline{(-1)^{\frac{61-1}{2}\cdot\frac{211-1}{2}} = +1}$; 211 mod 61 = 28;

$\left(\frac{28}{61}\right) = \left(\frac{2^2}{61}\right)\left(\frac{7}{61}\right)$; $\left(\frac{2^2}{61}\right) = \underline{(-1)^{(61^2-1)/8 \cdot 2} = +1}$

$\left(\frac{7}{61}\right)\left(\frac{61}{7}\right) = \underline{(-1)^{\frac{7-1}{2}\cdot\frac{61-1}{2}} = +1}$; 61 mod 7 = 5

$\left(\frac{5}{7}\right) = \left(\frac{-2}{7}\right) = \left(\frac{-1}{7}\right)\left(\frac{2}{7}\right)$; $\left(\frac{-1}{7}\right) = \underline{(-1)^{\frac{7-1}{2}} = -1}$;

$\left(\frac{2}{7}\right) = \underline{(-1)^{\frac{7^2-1}{8}} = +1}$; $\left(\frac{-122}{211}\right) = \underline{-1}$

Problem 3 (8 points): Let p be a prime with $p \equiv 5 \pmod 8$ and let $a \in \mathbb{Z}_p$ be a quadratic residue modulo p. Please prove:

(a, 3pts) If $a^{(p-1)/4} \equiv 1 \pmod p$ then for $b = (a^{(p+3)/8} \bmod p)$ one has $b^2 \equiv a \pmod p$.

$b^2 \equiv a^{(p+3)/4} \equiv a^{(p-1)/4} \cdot a \equiv a \pmod p$

(b, 5pts) If $a^{(p-1)/4} \equiv -1 \pmod p$ then for $b = (a^{(p+3)/8} 2^{(p-1)/4} \bmod p)$ one has $b^2 \equiv a \pmod p$.

2 is a QNR mod p because $p \not\equiv 1, 7 \pmod 8$

Therefore $2^{(p-1)/2} \equiv -1 \pmod p$

Hence

$b^2 \equiv a^{(p+3)/4} \, 2^{(p-1)/2} \equiv a^{(p-1)/4} \cdot 2^{(p-1)/2} \cdot a$

$\equiv (-1) \cdot (-1) \cdot a \equiv a \pmod p$

2017

Problem 4 (10 points): Consider the following table of indices (discrete logarithms) for the prime number 23 with respect to the primitive root $g = 11$:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
$\mathrm{ind}_{11}(a)$	0	10	14	20	5	2	7	8	6	15	1	12	4	17	19	18	13	16	9	3	21	11

(a, 4pts) Please compute the average multiplicative order of the non-zero residues modulo 23, namely

$$\frac{1}{22}\sum_{d \text{ divides } 22} (\text{number of non-zero residues of order } d)\cdot d.$$

$\phi(d)$

$\phi(2)\cdot\phi(11) = 10$

$$\frac{1}{22}\left(\phi(1)\cdot 1 + \phi(2)\cdot 2 + \phi(11)\cdot 11 + \phi(22)\cdot 22\right)$$

$$= \frac{1}{22}(1 + 2 + 10\cdot 11 + 10\cdot 22) = \frac{333}{22} = 15.14$$

(b, 6pts) Using the above table, please solve for $x \in \mathbb{Z}_{23}$, $y \in \mathbb{Z}_{23}$, and $z \in \mathbb{Z}_{23}$ the three congruences

$$20x^{21} \equiv 21 \pmod{23}, \quad 13y^{10} \equiv 16 \pmod{23}, \quad 11^{-3z} \equiv 4z^3 \pmod{23}.$$

Please give **all** solutions and show your work.

$21\cdot \mathrm{ind}(x) + \mathrm{ind}(20) \equiv \mathrm{ind}(21) \pmod{22}$

$\mathrm{ind}(20) = 3$, $\mathrm{ind}(21) = 21$

$\equiv -1 \pmod{22}$

$\mathrm{ind}(x) = (-1)\cdot 18 \equiv 4 \pmod{22} \Rightarrow x = 13$

$10\cdot \mathrm{ind}(y) + \mathrm{ind}(13) \equiv \mathrm{ind}(16) \pmod{22}$

$\mathrm{ind}(13) = 4$, $\mathrm{ind}(16) = 18$

$10\cdot \mathrm{ind}(y) \equiv 14 \pmod{22} \Rightarrow 5\,\mathrm{ind}(y) \equiv 7 \pmod{11}$

$5^{-1} \bmod 11 \equiv -2 \Rightarrow \mathrm{ind}(y) \equiv -14 \equiv 8 \pmod{11}$

$\mathrm{ind}(y) = 8, 19 \pmod{22}$ $\quad y = 8, 15$

$(-3z)\,\mathrm{ind}(11) \equiv 3\,\mathrm{ind}(z) + \mathrm{ind}(4) \pmod{22}$

$-21 \equiv 1 \pmod{22}$

$\mathrm{ind}(11) = 1$, $\mathrm{ind}(4) = 20$

$7(-3)\cdot(z + \mathrm{ind}(z)) \equiv 7\cdot(-2) \equiv 8 \pmod{22}$

$z = 6, 17$

2017

Problem 5 (5 points): Suppose Alice has encrypted a residue $M \in \mathbb{Z}_{23}$ by the Taher El-Gamal's public key system with public keys $p = 23$, $g = 11$ and $h \equiv 11^s \equiv 17 \bmod 23$. Alice's ciphertext is

$$E = (g^r \bmod 23,\ M \cdot h^r \bmod 23) = (19, 1).$$

Please show how Bob computes M. [Hint: you can use the table on the previous page for deriving Bob's private key s, and for powering, multiplication, and reciprocal modulo 23.]

$s = \text{ind}_{11}(17) = 13$

$h^r = (g^s)^r = (g^r)^s = 19^s$

$\text{ind}(h^r) \equiv s \cdot \text{ind}\, 19 \equiv 13 \cdot 9 \equiv (-9) \cdot 9 \equiv -81 \equiv 7 \pmod{22}$

$h^r = 7 \pmod{23}$

$M \equiv 1 \cdot (h^r)^{-1} \equiv 7^{-1} \equiv 10 \pmod{23}$

$\text{ind}(7^{-1}) \equiv (-1) \cdot \text{ind}\, 7 \equiv -7 \equiv 15 \pmod{22}$

$7^{-1} \equiv 10 \pmod{23}$: $7 \cdot 10 \equiv 70 \equiv 3 \cdot 23 + 1$

23	1	0
7	0	1
2	3	1 −3
1	3	−3 10

$(-3) \cdot 23 + \boxed{10} \cdot 7 = 1$

Problem 6 (5 points): Please find three positive integers $x, y, z \in \mathbb{Z}_{>0}$ such that $\text{GCD}(x, y, z) = 1$, x is even, $x \geq 4$ and $x^4 + y^2 = z^2$.

$2st = x^2 \Rightarrow s = 2,\ t = 9 \Rightarrow x = 6$

$y = t^2 - s^2 = 77$

$z = t^2 + s^2 = 85$

$6^4 + 77^2 = 85^2$

$(85+77)(85-77) = 162 \cdot 8 = 81 \cdot 16 = 3^4 \cdot 4^4$

$s = 8,\ t = 1 \Rightarrow x = 4$

$y = 8^2 - 1^2 = 63$

$z = 8^2 + 1^2 = 65$

$4^4 + 63^2 = 65^2$

$(65+63)(65-63) = 128 \cdot 2 = 256 = 2^8 = 4^4$

$s = 8,\ t = 9 \Rightarrow x = 12,\ y = 17,\ z = 145$