Problem 1 (16 points)

(a, 4pts) Please compute 2^{100} mod 10. Please show your work.

$$\left.\begin{array}{l} 2^{100} \equiv 0 \pmod 2 \\ 2^{100} \equiv (2^4)^{25} \equiv 1 \pmod 5 \end{array}\right\} 2^{100} \equiv 6 \pmod{10}$$

(b, 4pts) True of false: For all integers $x,y,z \in \mathbb{Z}_{>0}$ with $x^2+y^2=z^2$ one has $xyz \geq 60$. Please explain your answer.

True: $60 \mid xyz$ (HW4) $\Rightarrow xyz \geqslant 60$

(c, 4pts) Let $p=11$ and $i=\sqrt{-1}$, which does not exist in $\mathbb{Z}_{11}$. Please simplify the fraction $\frac{2+7i}{1+i}$ to form $a+ib$, where $a,b \in \mathbb{Z}_{11}$. Please show your work.

$$\frac{2+7i}{1+i} = \frac{(2+7i)(1-i)}{2} = \frac{9+5i}{2} = 6\cdot(9+5i) = 10+8i$$

$a \neq 0$

(d, 4pts) Please give a modulus $m \in \mathbb{Z}_{\geq 2}$ and a quadratic equation $ax^2+bx+c \equiv 0 \pmod m$, where $a,b,c \in \mathbb{Z}_m$, that has 3 or more solutions in the unknown residue $x \in \mathbb{Z}_m$.

$x^2-1 \equiv x^2+7 \pmod 8$ $\quad x=1,3,5,7$

$x^2-1 \equiv x^2+14 \pmod{15}$ $\quad x=1,4,11,14$

Problem 2 (5 points): **Using the quadratic reciprocity law**, please compute the value of the Jacobi symbol $\left(\frac{168}{179}\right)$. Please show all your work.

$$-1 = \left(\frac{21}{179}\right) = \left(\frac{3}{179}\right)\left(\frac{7}{179}\right) \quad +1 \quad -1$$

$$\left(\frac{168}{179}\right) = \left(\frac{2^3}{179}\right)\left(\frac{21}{179}\right) = (-1)^{3\frac{179^2-1}{8}}\left(\frac{21}{179}\right) = -\left(\frac{21}{179}\right) = -1$$

$$\left(\frac{21}{179}\right)\cdot\left(\frac{179}{21}\right) = (-1)^{\frac{21-1}{2}\cdot\frac{179-1}{2}} = +1,$$

$$-1 = \left(\frac{179}{21}\right) = \left(\frac{11}{21}\right), \left(\frac{11}{21}\right)\cdot\left(\frac{21}{11}\right) = (-1)^{\frac{11-1}{2}\cdot\frac{21-1}{2}} = +1,$$

$$-1 = \left(\frac{21}{11}\right) = \left(\frac{10}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{5}{11}\right) = (-1)^{\frac{11^2-1}{8}}\left(\frac{5}{11}\right) = -\left(\frac{5}{11}\right),$$

$$+1 = \left(\frac{5}{11}\right)\left(\frac{11}{5}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{11-1}{2}} = +1, \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = +1.$$

$$\Longrightarrow \left(\frac{168}{179}\right) = +1.$$

$$\left(\frac{3}{179}\right)\left(\frac{179 \bmod 3}{3}\right) = (-1)^{\frac{3-1}{2}\frac{179-1}{2}} = (-1)$$

$$\left(\frac{3}{179}\right) = +1 \qquad \left(\frac{179 \bmod 3}{3}\right) = \left(\frac{2}{3}\right) = -1$$

$$+1 = \left(\frac{-11}{179}\right) = \left(\frac{-1}{179}\right)\cdot\left(\frac{11}{179}\right) = -\left(\frac{11}{179}\right)$$

$$\left(\frac{7}{179}\right)\cdot\left(\frac{179}{7}\right) = -1$$

$$\left(\frac{7}{179}\right) = -1 \qquad \left(\frac{179}{7}\right) = \left(\frac{4}{7}\right) = 1$$

$$\left(\frac{11}{179}\right)\cdot\left(\frac{179}{11}\right) = -1 \qquad \left(\frac{11}{179}\right) = -1 \qquad \left(\frac{179}{11}\right) = 1$$

$$\left(\frac{3}{11}\right)\cdot\left(\frac{11}{3}\right) = -1 \qquad \left(\frac{3}{11}\right) = +1 \qquad \left(\frac{11}{3}\right) = \left(\frac{2}{3}\right) = -1$$

Problem 3 (8 points): We know for all prime numbers $p \geq 3$ that $\left(\frac{2}{p}\right) = +1 \Longleftrightarrow p \equiv \pm 1 \pmod 8$. Please prove that

(a, 4pts) if $p \equiv 1 \pmod 8$, c is a quadratic non-residue modulo p, and $b = c^{(p-1)/8} + c^{7(p-1)/8}$, then we have $b^2 \equiv 2 \pmod p$. Note that $(p-1)/8 \in \mathbb{Z}$.

$$\left(c^{\frac{p-1}{8}} + c^{7\frac{p-1}{8}}\right)^2 = c^{\frac{p-1}{4}} + 2c^{p-1} + c^{7\frac{p-1}{4}}$$

$$= 2 + c^{\frac{p-1}{4}} + c^{p-1}\cdot c^{3\frac{p-1}{4}}$$

$$= 2 + c^{\frac{p-1}{4}} + c^{\frac{p-1}{2}}\cdot c^{\frac{p-1}{4}} = 2 + c^{\frac{p-1}{4}} - c^{\frac{p-1}{4}} = 2$$

(b, 4pts) if $p \equiv 7 \pmod 8$ and $b = 2^{(p+1)/4}$, then we have $b^2 \equiv 2 \pmod p$. Note that $(p+1)/4 \in \mathbb{Z}$.

$$\left(2^{\frac{p+1}{4}}\right)^2 = 2^{\frac{p+1}{2}} = 2\,2^{\frac{p-1}{2}} = 2$$

Since $\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} \equiv 1 \pmod p$

Problem 4 (10 points): Consider the following table of indices (discrete logarithms) for the prime number 23 with respect to the primitive root $g = 5$:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
$\mathrm{ind}_5(a)$	0	2	16	4	1	18	19	6	10	3	9	20	14	21	17	8	7	12	15	5	13	11

(a, 4pts) From the above index table, compute the multiplicative order modulo 23 of the following residues (the exponent that belongs to the following residues module 23):

$$1, \quad 2, \quad 10, \quad 22 \quad \in \mathbb{Z}_{23}.$$

Exponent of 1 *is* 1, *of* 2 *is* $22/\gcd(22,2) = 11$, *of* 10 *is* 22, *of* 22 *is* $22/\gcd(22,11) = 2$.

(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

$$10x^8 \equiv 22 \pmod{23}, \quad y^{13} \equiv 2 \pmod{23}, \quad 4^z \equiv z^4 \pmod{23}.$$

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

$8 \cdot ind_5(x) + ind_5(10) \equiv ind_5(22) \pmod{22}$,
$8ind_5(x) \equiv (11-3) \equiv 8 \pmod{22}$, $ind_5(x) \equiv 1 \pmod{11}$: *so* $x = 5, 18$.

$13 \cdot ind(y) \equiv 2 \pmod{22}$, $ind(y) \equiv 13^{-1}2 \pmod{22}$, $ind(y) = 13$, $y = 18$.

$z\,ind(4) \equiv 4z \equiv 4\,ind(z) \pmod{22}$, $z \equiv ind(z) \pmod{11}$: $z = \underset{2,}{\wedge} 4, 22$.

Problem 5 (6 points): Taher El Gamal's 1984 public key cryptosystem realizes probabilistic cryptography. Please explain how Bob chooses his public key, how Alice encrypts her messages to him, and how Bob decrypts them with his secret private key. In particular, explain why randomization is necessary for the system's security.

Bob's private key: $k \in \mathbb{Z}_p \setminus \{0\}$

public key: p prime, g prim. root

$h \equiv (g^k \bmod p)$

Alice encrypts M by selecting random $l \in \mathbb{Z}_p$ and sending the pair

$(g^l \bmod p, M \cdot h^l \bmod p) = (x, y)$

Bob decrypts $y \cdot (x^k)^{-1} \equiv M \pmod p$

If Alice does not choose l random, $x^k \equiv M \cdot y^{-1} \pmod p$ by knowing a single (M, y) pair ("lunch-time attack")

Problem 5 (5 points): Please find three positive integers $x, y, z \in \mathbb{Z}_{>0}$ such that $x^2 + 5y^4 = z^2$. Please show your work.

$y = 2\sqrt{5}t$, $t = 2$, $x = 5 - t^2 = 1$, $z = 5 + t^2 = 9$: $1 + 5 \cdot 16 = 81$.

$2^2 + 5 \cdot 1^4 = 3^2$ $(2, 1, 3)$

$1^2 + 5 \cdot 2^4 = 9^2$ $(1, 2, 9)$

$(12, 2, 8)$