Problem 1 (16 points)

(a, 4pts) Please compute $2^{1000000}$ mod 55. Hint: use Chinese remaindering and Euler's generalization of the little Fermat theorem.

$$2^{1000000} \bmod 5 = 2^{1000000 \bmod 4} = 2^0 = 1$$

$$2 \bmod 11 = 2^{\bmod 10} = 2^0 = 1$$

$$\overline{}$$
$$1 \bmod 55$$

(b, 4pts) True of false: For all integers x,y,z with $xyz \neq 0$ we have $x^4 + 4y^4 \neq z^4$. Please explain your answer.

TRUE

$z^4 - 4y^4 \neq (x^2)^2$ from HW

(c, 4pts) True or false: if p is a prime number with $p \equiv 3 \pmod 4$ then for all $a \in \mathbb{Z}_p$, $a \neq 0$ exactly one of a and $p-a$ ~~are~~ are quadratic residues.

TRUE

$$\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = -\left(\frac{a}{p}\right)$$

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

Quadratic Reciprocity Law

(d, 4pts) The Riemann zeta function

$$\zeta(z) = \frac{1}{1^z} + \frac{1}{2^z} + \cdots + \frac{1}{i^z} + \cdots$$

is defined for complex values $z \in \mathbb{C}$ (but not everywhere, e.g., not for $z = 1$). The Riemann hypothesis conjectures a property for all complex zeros $w \in \mathbb{C}$ of ζ, i.e., $\zeta(w) = 0$. Which property?

$\mathrm{Re}\,(w) = \frac{1}{2}$ Riemann hypothesis

Problem 2 (5 points): **Using the quadratic reciprocity law,** please compute the value of the Jacobi symbol $\left(\frac{70}{151}\right)$. Please show all your work.

$$\left(\frac{35}{151}\right)\left(\frac{151}{35}\right) = (-1)^{odd} = -1$$

$$\left(\frac{35}{151}\right) = -1$$

$$\left(\frac{151}{35}\right) = \left(\frac{11}{35}\right) = +1$$

$$\left(\frac{110}{199}\right) = \left(\frac{2}{199}\right)\left(\frac{55}{199}\right) = (-1)^{\frac{199^2-1}{8}}\left(\frac{55}{199}\right) = +\left(\frac{55}{199}\right)$$
$$\left(\frac{55}{199}\right)\cdot\left(\frac{199}{55}\right) = (-1)^{\frac{55-1}{2}\cdot\frac{199-1}{2}} = -1,$$
$$\left(\frac{199}{55}\right) = \left(\frac{34}{55}\right) = \left(\frac{2}{55}\right)\left(\frac{17}{55}\right) = +\left(\frac{17}{55}\right),\ \left(\frac{17}{55}\right)\cdot\left(\frac{55}{17}\right) = (-1)^{\frac{55-1}{2}\cdot\frac{17-1}{2}} = +1$$
$$\left(\frac{55}{17}\right) = \left(\frac{4}{17}\right) = +1 \Longrightarrow \left(\frac{110}{199}\right) = -1.$$

$$\left(\frac{11}{35}\right)\left(\frac{35}{11}\right) = (-1)^{odd} = -1$$

$$\left(\frac{11}{35}\right) = +1$$

$$\left(\frac{35}{11}\right) = \left(\frac{2}{11}\right) = (-1)^{\frac{11^2-1}{8}} = -1.$$

$$\left(\frac{70}{151}\right) = \left(\frac{2}{151}\right)\left(\frac{35}{151}\right) = -1$$

$$\left(\frac{70}{151}\right) = -1$$

$$\left(\frac{2}{151}\right) = (-1)^{\frac{151^2-1}{8}} = 1$$

Problem 3 (5 points): Using Newton iteration discussed in class compute consecutively residues $b_0 \in \mathbb{Z}_3$, then $b_1 \in \mathbb{Z}_3$ and finally $b_2 \in \mathbb{Z}_3$ such that $b_0 + 3b_1 + 9b_2 = b \in \mathbb{Z}_{27}$ satisfies $b^2 \equiv 7 \pmod{27}$.

$b_0^2 \equiv 7 \pmod 3$

$b_0 = 1$ $\qquad b_0 = 2$

$(1 + 3\cdot b_1)^2 \equiv 7 \pmod 9$

$6b_1 \equiv 7 - 1 \pmod 9$

$2b_1 \equiv 2 \pmod 3$

$b_1 = 1$

$(1 + 3 + 9\cdot b_2)^2 \equiv 7 \pmod{27}$

$16 + 2\cdot 4\cdot 9\, b_2 \equiv 7$

$2\cdot 4\cdot 9\, b_2 \equiv -9$

$8\, b_2 \equiv -1 \pmod 3$

$1+3+9 = 13$ $\qquad 13^2 \equiv$ $\qquad 169 \equiv 27\cdot 6 + 7$

$b_2 = 1$

$b_0 \equiv 2$ (mod

$(2+3b_1)^2 \equiv 7 \pmod 9$

$4 + 2 \cdot 2 \cdot 3 b_1 \equiv 7 \pmod 9$

$2 \cdot 2 \cdot 3 b_1 \equiv 3 \pmod 9$

$4 b_1 \equiv 1 \pmod 3$

$b_1 = 1$

$(2+3+b_2 \cdot 9)^2 \equiv 7 \pmod{27}$

$25 + 2 \cdot 5 \cdot 9\, b_2 \equiv 7$

$2 \cdot 5 \cdot \cancel{9}\, b_2 \equiv -\underset{2}{\cancel{18}} \pmod{27}$

$10 \cdot b_2 = -2 \pmod 3$

$b_2 = 1$

$b_0 + 3b_1 + 9b_2 = 14$

$14^2 = 196 = 27 \cdot 7 + 7$

56 189

196

Problem 4 (15 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) By inspecting the above table, please list all primitive roots modulo 23.

a has order $22 \iff a = g^i$ *with* $\gcd(i, 22) = 1$.
So $a = 5, 7, 10, 11, 14, 15, 17, 19, 20, 21$

(b, 6pts) Using the above table, please solve for $x \in \mathbb{Z}_{23}$, $y \in \mathbb{Z}_{23}$, and $z \in \mathbb{Z}_{22}$ the three congruences

$$10x^9 \equiv 22 \pmod{23}, \quad y^4 \equiv 2 \pmod{23}, \quad 7^z \equiv 10 \pmod{23}.$$

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

$9 \cdot ind_5(x) + ind_5(10) \equiv ind_5(22) \pmod{22}$,
$ind_5(x) \equiv 9^{-1}(11 - 3) \equiv 18 \pmod{22}$ *(by extended Euclidean algorithm not shown), so*
$x = 6$. $2 \equiv 5^2 \pmod{23}$

$4 \cdot ind(y) \equiv 2 \pmod{22}$, $2 \cdot ind(y) \equiv 1 \pmod{11}$, $ind(y) \equiv 6 \pmod{11}$, $ind(y) = 6$ *and* $ind(y) = 17$,
$y_1 = 8, y_3 = 15$.

$z \cdot ind(7) \equiv ind(10) \pmod{22}$, $z \equiv 19^{-1}3 \equiv 21 \pmod{22}$.

(c, 5pts) Suppose Bob has set up a public key $p = 23$, $g = 5$, and $h = 19 = g^s \pmod{23}$ for Taher ElGamal's cryptosystem. Alice has chose her random $r = 15$ and encrypts a message $M = 15$. What cipertext is Alice sending to Bob? You can use the table above part (a) for modular exponentiation (instead of repeated squaring) but not for computing Bob's secret s.

2 3

$$\left(g^r,\ M \cdot h^r \bmod p\right)$$

$$\left(5^{15} \bmod 23,\ 15 \cdot \overbrace{19^{15}}^{20} \bmod 23\right)$$

$5^{15} \bmod 23 = 19$

$(-8)\cdot(-3) = 24 = 1$

$\operatorname{ind} 19^{15} = 15 \cdot \underbrace{\operatorname{ind} 19}_{15} \bmod 22$

$(-7)(-7) = 49 = 5$

$= (19, 1)$

Problem 5 (5 points): Please find three integers $x, y, z \in \mathbb{Z}_{>0}$ such that $\mathrm{GCD}(x, y) = 1$ and $x^2 + y^5 = z^2$. Please show your work.

$32 + 49 = 81$

$2^5 + 7^2 = 9^2$

$x^2 + (y^5)^2 = z^2$

$x = s^2 - t^2$, $y^5 = 2st$, $z = s^2 + t^2$

$\mathrm{GCD}(s, t) = 1$

$2 \cdot 2^4 \cdot 1$, $s = 16$, $t = 1$

$(16^2 - 1)^2 + 4^5 = (16^2 + 1)$

$16^2 - 1 = 255$, $(255)^2 = 65{,}025$

4^5 = ~~[illegible]~~

$16^2 + 1 = 257$

$x = 255$

$y = 4$

$z = 257$