Problem 1 (16 points)

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

$100 = 2^2 5^2$ $\quad 2^{100} \bmod 2^2 = 0$

$2^{100} \equiv (2^{20})^5 \equiv 1 \pmod{25}$, $\phi(25) = 25 \cdot (1 - \frac{1}{5}) = 5 \cdot 4 = 20$

$26 \not\equiv 0,\ 51 \not\equiv 0,\ 76 \equiv 0 \pmod 4$

$2^{100} \bmod 100 = 76$

mod 10 $\quad$ ~~no~~ +1

(b, 4pts) True or false: If p is a prime number then $\sigma(p^2 - p) = (p+1)\sigma(p-1)$. Please explain.

2pts True: σ is a multiplicative number theoritic function, $GCD(p, p-1) = 1$

2pts $\sigma(p(p-1)) = \sigma(p)\sigma(p-1) = (1+p)\sigma(p-1)$

$GCD(p, p-1) = 1$ not stated: no penalty

(c, 4pts) Please construct a primitive Pythagorean triple $(x, 7, z) \in \mathbb{Z}^3_{>0}$ such that $x^2 + 7^2 = z^2$.

$\underbrace{\left(\frac{7+1}{2}\right)}_{s}^2 - \underbrace{\left(\frac{7-1}{2}\right)}_{t}^2 = 4^2 - 3^2 = 16 - 9 = 7$

$x = 2st = 2 \cdot 3 \cdot 4 = 24$

$z = s^2 + t^2 = 25$

$24^2 + 7^2 =$

$(25-1)^2 + 7^2 =$

$25^2 - 50 + 1 + 49 = 25^2$

$GCD(24, 7) = 1$

(d, 4pts) Please state a conjecture in number theory, which is yet to be proven.

There exist infinitely many prime twins

proven theorem: +1

Riemann hypo $\quad |\{p \mid 2 \text{ has order } p-1\}| = \infty$

Gold bach $\quad$ inf. Mersenne primes / Fermat

$3^5 \equiv 3^2\cdot 3^2\cdot 3 = (-2)(-2)\cdot 3 = +12 = 11$

$\frac{988\cdot 986}{8} = 247\cdot 493$

$\left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right)$, $= -1$, $+1$, $(-1)^{\frac{10\cdot 12}{8}} = -1$

$5\cdot 1$

$\left(\frac{3}{11}\right)\left(\frac{11}{3}\right) = (-1) = -1$, $= +1$, $= -1$

Problem 2 (5 points): **Using the quadratic reciprocity law**, please compute the value of the Jacobi symbol $\left(\frac{610}{987}\right)$. Please show all your work.

$\left(\frac{610}{987}\right) = \left(\frac{2\cdot 305}{987}\right) = (-1)^{\frac{987^2-1}{8}} \left(\frac{305}{987}\right) = -\left(\frac{305}{987}\right)$

$\left(\frac{305}{987}\right)\left(\frac{987}{305}\right) = (-1)^{\frac{304}{2}\cdot\frac{986}{2}} = (-1)^{152\cdot 493} = +1$

76, $153 \quad 152$, $306\cdot 304$, $8 \quad 72$

$987 \bmod 305 = 72 = 2^3\cdot 3^2$

$\left(\frac{72}{305}\right) = (-1)^{3\cdot\frac{305^2-1}{8}} \left(\frac{9}{305}\right) = (+1)\cdot(+1) = 1$

$\left(\frac{610}{987}\right) = -1$

$\left(\frac{9}{305}\right)\left(\frac{305}{9}\right) = (-1)^{\frac{8}{2}\cdot\frac{304}{2}} = +1$

$305 \bmod 9 = 8$

$\left(\frac{8}{9}\right) = \left(\frac{2^3}{9}\right) = (-1)^{3\cdot\frac{9^2-1}{8}} = +1$

$-1\left(\frac{610}{987}\right) = \left(\frac{1}{3}\right)\left(\frac{1}{7}\right)\left(\frac{46}{47}\right)$

$+1 = \left(\frac{2}{47}\right)\left(\frac{23}{47}\right)$, $(-1)^{11\cdot 23}\left(\frac{1}{47}\right)$

Problem 3 (8 points):

(a, 4pts) Show that $a = 13$ is a quadratic residue and $c = 14$ is a quadratic non-residue, both modulo 29.

$\left(\frac{610}{987}\right) = \left(\frac{2}{987}\right)\left(\frac{5}{987}\right)\left(\frac{61}{987}\right) = -1$

$\left(\frac{5}{987}\right)\left(\frac{987}{5}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{988}{2}} = +1$

$\left(2/5\right) = (-1)^{\frac{24}{8}} = -1$

$\left(\frac{61}{987}\right)\left(\frac{987}{61}\right) = (-1)^{\frac{60}{2}\cdot\frac{988}{2}} = +1$

$\left(\frac{987}{61}\right) = \left(\frac{11}{61}\right)$

$\left(\frac{11}{61}\right)\left(\frac{61}{11}\right) = (-1)^{5\cdot 30} = +1$

listing residues: no penalty

$\left(\frac{13}{23}\right)\left(\frac{23}{13}\right) = (-1)^{\frac{12}{2}\cdot\frac{22}{2}} = +1$

$\left(\frac{23}{13}\right) = \left(\frac{10}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right) = (-1)^{\frac{13^2-1}{8}}\left(\frac{5}{13}\right)$

$\left(\frac{5}{13}\right)\left(\frac{13}{5}\right) = (-1)^{\frac{4}{2}\cdot\frac{12}{2}} = +1$, $\left(\frac{3}{5}\right)$

(b, 4pts) Using the algorithm from class, compute $b \in \mathbb{Z}_{29}$ such that $b^2 \equiv 13 \pmod{29}$. If you need a quadratic non-residue, please use 14.

$-1 = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = (-1)^{\frac{29^2-1}{8}}\left(\frac{7}{29}\right)$

$\left(\frac{3}{5}\right)\left(\frac{5}{3}\right) = (-1)^{\frac{2}{2}\cdot\frac{4}{2}} = +1$, $\left(\frac{2}{3}\right) = -1$

$\left(\frac{7}{29}\right)\left(\frac{29}{7}\right) = (-1)^{\frac{6}{2}\cdot\frac{28}{2}} = +1$

$\left(\frac{1}{7}\right) = +1$

$13^{14} = 1, \quad 13^7 = 28$

$13^8\cdot 14^{14} = (-13)(-1) = 13$

$\underbrace{13^4}_{25}\cdot\underbrace{14^7}_{12} \equiv 10$

10, 19 w/o algo +2

$b \equiv 25$ +2

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) By inspecting the above table, for the multiplicative orders $k = 1, 2, 11, 22$ please list one residue $a_k \in \mathbb{Z}_{23} \setminus \{0\}$ each that has order k (belongs to the exponent k modulo 23).

$k=1$: $GCD(\mathrm{ind}_5(a), 22) = 22$: $a_1 = 1$

$k=2$: $GCD(\mathrm{ind}_5(a), 22) = 11$: $a_2 = 22$

$k=11$: $GCD(\mathrm{ind}_5(a), 22) = 2$: $a_{11} = 2, 3, 4, 6, 8, 9, 12, 13, 16, 18$

$k=22$: $GCD(\mathrm{ind}_5(a), 22) = 1$: a_{22}: $5, 7, 10, 11, 14, 15, 17, 19, 20, 21$

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

$$18x^6 \equiv 9 \pmod{23}, \quad y^{21} \equiv 22 \pmod{23}, \quad 5^{3z} \equiv z \pmod{23}.$$

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

$6 \cdot \mathrm{ind}(x) + \underbrace{\mathrm{ind}(18)}_{12} \equiv \underbrace{\mathrm{ind}(9)}_{10} \pmod{22}$ $\quad 18^{-1} \equiv (-5)^{-1} \equiv 9$

2pts $\quad 9 \cdot 9 \equiv 12$

$3\,\mathrm{ind}(x) \equiv -1 \pmod{11}$ $\quad 6\,\mathrm{ind}(x) \equiv 20$

$\mathrm{ind}(x) \equiv -4 \equiv 7 \pmod{11}$

$\mathrm{ind}(x) = 7, 18$ $\quad x = 17, 6$

2pts $21\,\mathrm{ind}(y) \equiv \mathrm{ind}(22) \equiv 11 \pmod{22}$

$\mathrm{ind}(y) \equiv -11 \equiv 11 \pmod{22}$ $\quad y = 22$

2pts $3z \cdot \mathrm{ind}(5) \equiv \mathrm{ind}(z) \pmod{22}$

$z \equiv 3^{-1}\,\mathrm{ind}(z) \equiv 15\,\mathrm{ind}(z)$

$z = 6, 17$ $\quad 5^{51} \equiv 5^7 \equiv 17 \pmod{23}$

Problem 5 (6 points): Taher El Gamal's 1984 public key cryptosystem in its original form is still malleable. Alice sends Bob a ciphertext

$$E(M_A) = \big(\underbrace{g^{r_A} \bmod p}_{x_A},\ \underbrace{M_A h_B^{r_A} \bmod p}_{y_A}\big), \quad r_A \text{ random and hidden,}$$

of her message M_A with his public key $h_B = (g^{s_B} \bmod p)$, s_B secret. Charlie, knowing the cipher x_A, y_A, can encrypt $\lambda_C M_A$ with his λ_C without knowing M_A. A problem is that Charlie needs to send his own x_C, and does so by using $x_C = (x_A g^{r_C} \bmod p)$ for his own random r_C. Please give Charlie's y_C for $E(\lambda_C M_A)$, and justify that Bob's decryption produces $\lambda_C M_A$.

$$y_C \equiv (\lambda_C M_A) \cdot h_B^{r_A + r_C}$$

$$\equiv \lambda_C (M_A \cdot h_B^{r_A}) \cdot h_B^{r_C} \equiv \lambda_C y_A \cdot h_B^{r_C} \pmod p$$

$\lambda_C y_A M_A h_B^{r_C}$ +2

$\lambda_C M_A h_B^{r_C}$ no credit

5pts

$$D(y_C) \equiv y_C \cdot \left(x_C^{s_B}\right)^{-1}$$

$$\equiv \lambda_C M_A h_B^{r_A} \cdot h_B^{r_C} \left[\left(g^{r_A + r_C}\right)^{s_B}\right]^{-1}$$

1pt

$$\equiv \lambda_C M_A\, g^{s_B (r_A + r_C)} \cdot \left(g^{-1}\right)^{s_B (r_A + r_C)}$$

$$= \lambda_C M_A$$

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

$z^2 = s^2 + t^2$ $\quad z = u^2 + v^2$, $s = 2uv$, $t = u^2 - v^2$

$u = 2$, $v = 1$ $\quad s = 4$ $\quad t = 3$

$z = 5$

$x = 2st = 2(2uv)(u^2 - v^2) = 2 \cdot 4 \cdot 3 = 24$

$y = s^2 - t^2 = 7$ $\quad 24^2 + 7^2 = 25^2 = 5^4$

$\mathrm{GCD}(x,y) > 1$ $\quad -2$