Problem 1 (16 points)

(a, 4pts) Please describe how Bob, using his private keys of a public key crypto system, can provide a digital signature that Alice can verify using Bob's public keys.

Bob decrypts his signature F with his private key: $S = D_p(F)$
Alice encrypts S: $E_K(S) = F$ and checks F.

(b, 4pts) True or false: $6^{\phi(1000)} = 6^{400} \equiv 1 \pmod{1000}$. Please explain.

False
$1000 \mid 6^{400} - 1 \Rightarrow 2 \mid 6^{400} - 1 \Rightarrow 2 \mid -1$
Or: $1000 \cdot x = 6^{400} - 1$, $1 = 6^{400} - 1000x$, but the right side is div. by 2.

Will Long: The right side ends in 001, hence is odd, but 6^{400} is even.

(c, 4pts) Please construct a primitive Pythagorean triple $(8, y, z) \in \mathbb{Z}^3_{>0}$ such that $8^2 + y^2 = z^2$.

$8 = 2st$. $s = 4$, $t = 1$
$y = s^2 - t^2 = 15$
$z = s^2 + t^2 = 17$

(d, 4pts) Please state the recent progress (by Yitang Zhang and followed-up by others) towards proving that there are infinitely prime twins.

Let $\delta_n = p_n - p_{n-1}$, the gap between the n-th prime and the $(n-1)$-st prime
There is an integer $g \leq 70 \cdot 10^6$ such that $g = p_n - p_{n-1}$ for infinitely n.

Public key:

g, p, h_B

Private key: s_B with $g^{s_B} \equiv h_B$

random r_A A $\xrightarrow{h_A}$ B

$h_A \equiv g^{r_A}$

B $\xleftarrow{F = S \cdot h_A^{-s}}$

Alice checks:

$F \cdot h_B^{r_A} \equiv S$

Problem 2 (5 points): The following is a trace of the computation of the Legendre symbol $\left(\frac{-146}{233}\right)$ using Jacobi's reciprocity law. Please fill in the blanks.

$\left(\frac{-146}{233}\right) = \left(\frac{-1}{233}\right)\left(\frac{146}{233}\right)$; $\left(\frac{-1}{233}\right) = \underline{(-1)^{\frac{232}{2}} = (-1)^{116} = +1}$

$\left(\frac{146}{233}\right) = \left(\frac{2}{233}\right)\left(\frac{73}{233}\right)$; $\left(\frac{2}{233}\right) = \underline{(-1)^{(233^2-1)/8} = (-1)^{\frac{116}{2}\cdot\frac{234}{2}} = (-1)^{11\cdot 58} = +1}$

$\left(\frac{73}{233}\right)\left(\frac{233}{73}\right) = \underline{(-1)^{\frac{72}{2}\cdot\frac{232}{2}} = +1}$; 233 mod 73 = 14;

$\left(\frac{14}{73}\right) = \left(\frac{2}{73}\right)\left(\frac{7}{73}\right)$; $\left(\frac{2}{73}\right) = \underline{(-1)^{\frac{72\cdot 74}{8}} = (-1)^{13\cdot 74} = +1}$

$\left(\frac{7}{73}\right)\left(\frac{73}{7}\right) = \underline{(-1)^{\frac{6}{2}\cdot\frac{72}{2}} = +1}$; 73 mod 7 = 3

$\left(\frac{3}{7}\right)\left(\frac{7}{3}\right) = \underline{(-1)^{\frac{2}{2}\cdot\frac{6}{2}} = -1}$; 7 mod 3 = 1; $\left(\frac{-146}{233}\right) = \underline{-1}$

Problem 3 (8 points): Let p be a prime integer with $p \equiv 5 \pmod 8$, that is, $p-1 \equiv 0 \pmod 4$, $p+3 \equiv 0 \equiv 3p+1 \pmod 8$. Let a be a quadratic residue and c a quadratic non-residue modulo p. Please prove that $b^2 \equiv a \pmod p$ for

$$b \equiv 2^{-1}\left((1+c^{\frac{p-1}{4}})a^{\frac{3p+1}{8}} + (1-c^{\frac{p-1}{4}})a^{\frac{p+3}{8}}\right) \pmod p.$$

$$\left(\left(1+c^{\frac{p-1}{4}}\right)a^{\frac{3p-1}{8}} + \left(1-c^{\frac{p-1}{4}}\right)a^{\frac{p+3}{8}}\right)^2$$

$$= \left(1+c^{\frac{p-1}{4}}\right)^2 a^{\frac{3p-1}{4}} + \left(1-c^{\frac{p-1}{4}}\right)^2 a^{\frac{p+3}{4}} + 2\left(1+c^{\frac{p-1}{4}}\right)\left(1-c^{\frac{p-1}{4}}\right)a^{\frac{4p+4}{8}}$$

$$= \left(1+c^{\frac{p-1}{2}}+2c^{\frac{p-1}{4}}\right)a^{\frac{p-1}{2}+\frac{p+3}{4}} + \left(1+c^{\frac{p-1}{2}}-2c^{\frac{p-1}{4}}\right)a^{\frac{p+3}{4}}$$

($c^{\frac{p-1}{2}} = -1$, so $1+c^{\frac{p-1}{2}} = 0$; $a^{\frac{p-1}{2}+\frac{p+3}{4}} = a^{\frac{p-1}{2}}\cdot a^{\frac{p-1}{2}+1} = +1$; $1+c^{\frac{p-1}{2}} = 0$)

$$+ 2\left(1-c^{\frac{p-1}{2}}\right)a^{\frac{p-1}{2}+1}$$

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

$$= 4a$$

$$b^2 \equiv 2^{-2}\cdot 4a \equiv a \pmod p$$

Problem 4 (10 points): Consider the following table of indices (discrete logarithms) for the prime number 23 with respect to the primitive root $g = 7$:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
$\text{ind}_7(a)$	0	14	2	6	7	16	1	20	4	21	19	8	10	15	9	12	5	18	17	13	3	11

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

$$2,\quad 3,\quad 4,\quad 5 \quad \in \mathbb{Z}_{23}.$$

$2 = 7^{14}$ order $= 22/\text{GCD}(14,22) = 11$

$3 = 7^{2}$ order $= 22/\text{GCD}(2,22) = 11$

$4 = 7^{6}$ order $= 22/\text{GCD}(6,22) = 11$

$5 = 7^{7}$ order $= 22/\text{GCD}(7,22) = 22$

(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

$$x^{19} \equiv 19 \pmod{23}, \quad 19y^{12} \equiv 14 \pmod{23}, \quad 7^{2z} \equiv z^2 \pmod{23}.$$

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

$19 \cdot \text{ind}(x) \equiv \text{ind}(19) \equiv 17 \pmod{22}$

$\text{ind}(x) \equiv 7 \cdot 17 \equiv 7 \cdot (-5) \equiv -35 \equiv 9 \pmod{22}$

$x = 15$

22	10
19	01
3	1 −1
1	6 −67

$(-6)\cdot 22 + 7 \cdot 19 = 1$

$12 \cdot \text{ind}(y) + \underbrace{\text{ind}(19)}_{17} \equiv \underbrace{\text{ind}(14)}_{15} \pmod{22}$

$12 \cdot \text{ind}(y) \equiv -2 \pmod{22}$

$6 \cdot \text{ind}(y) \equiv -1 \pmod{11}$

$\text{ind}(y) \equiv 2 \cdot (-1) \equiv 9 \pmod{11}$

$\text{ind}(y) \equiv 9, 20$ $\quad y = 15, 8$

$2z \equiv 2 \cdot \text{ind}(z) \pmod{22}$ $\quad z \equiv \text{ind}(z) \pmod{11}$

$z = 10, 18, 22$

Problem 5 (6 points): Suppose Alice has encrypted a residue $M \in \mathbb{Z}_{23}$ by the Taher El-Gamal's public key system with public keys $p = 23$, $g = 7$ and $h \equiv 7^s \equiv 16 \bmod 23$. Alice's ciphertext is

$$E = (g^r \bmod 23,\ M \cdot h^r \bmod 23) = (13, 11).$$

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.]

$S = \text{ind}_7(16) = 12$

$M \equiv (M \cdot h^r) \cdot ((g^r)^s)^{-1} \equiv 11 \cdot (13^{12})^{-1}$

$13^{12} \equiv 7^{(\text{ind}(13) \cdot 12) \bmod 22} \equiv 7^{10 \cdot 12 \bmod 22}$

$\equiv 7^{10} \equiv 13$

23	10
13	01
10	1 -1
3	1 -1 2
1	3 4 -7

$13^{-1} \equiv 16 \pmod{23}$

$M \equiv 11 \cdot 16 \equiv 7^{19} \cdot 7^{12} \equiv 7^{31 \bmod 22} \equiv 7^9 \equiv 15$

4·23
−7·13 = 1

Problem 6 (5 points): Please find three positive integers $x, y, z \in \mathbb{Z}_{>0}$, $x \neq y$, but not necessarily relatively prime, such that $x^2 + y^2 = z^3$.

$3^2 + 4^2 = 5^2$ times 5^4

$(3 \cdot 5^2)^2 + (4 \cdot 5^2)^2 = 5^6 = (5^2)^3$

$75^2 + 100^2 = 25^3$

Other solutions: $4^2 + 11^2 = 5^3$

$5^2 + 10^2 = 5^3$

$(2 \cdot 13)^2 + (3 \cdot 13)^2 = 13 \cdot 13^2 = 13^3$

$35^2 + 120^2 = 25^3$

$5^2 + t^2 = 16 + 9$