2016

Problem 1 (16 points)

(a, 4pts) In public key cryptography, Alice encodes her clear text using no secret. Please explain why such a cipher text can be secure, in particular what assumption guarantees the security of an RSA cipher.

To reverse the encryption takes too much computation without the secret. In RSA $k^{-1} \bmod \phi(n)$ seems to require the factoring of n, which is hard

(b, 4pts) True or false: if n is a **composite** integer ≥ 4 then $\phi(n) \leq \frac{n}{2}$, where ϕ is Euler's function. Please explain.

FALSE: $\phi(9) = 9 \cdot (1 - \frac{1}{3}) = 6 > \frac{9}{2}$

(c, 4pts) True or false: for all non-negative integers $n \in \mathbb{Z}_{\geq 0}$ there exist four non-negative integers $x, y, z, w \in \mathbb{Z}_{\geq 0}$ such that $n = x^2 + y^2 + z^2 + w^2$. Please explain.

TRUE This is LAGRANGE's THM.

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

TRUE. N. ELKIES found a solution, disproving EULER.

Sol 2016

Problem 2 (5 points): The following is a trace of the computation of the Legendre symbol $\left(\frac{-142}{239}\right)$ using Jacobi's reciprocity law. Please fill in the blanks.

$\left(\frac{-142}{239}\right) = \left(\frac{-1}{239}\right)\left(\frac{142}{239}\right)$; $\left(\frac{-1}{239}\right) = \underline{(-1)^{119} = -1}$

$\left(\frac{142}{239}\right) = \left(\frac{2}{239}\right)\left(\frac{71}{239}\right)$; $\left(\frac{2}{239}\right) = \underline{(-1)^{238\cdot 240/8} = +1}$

$\left(\frac{71}{239}\right)\left(\frac{239}{71}\right) = \underline{(-1)^{35\cdot 119} = -1}$; 239 mod 71 = 26;

$\left(\frac{26}{71}\right) = \left(\frac{2}{71}\right)\left(\frac{13}{71}\right)$; $\left(\frac{2}{71}\right) = \underline{(-1)^{70\cdot 72/8} = +1}$

$\left(\frac{13}{71}\right)\left(\frac{71}{13}\right) = \underline{(-1)^{6\cdot 35} = +1}$; 71 mod 13 = 6

$\left(\frac{6}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{3}{13}\right)$; $\left(\frac{2}{13}\right) = \underline{(-1)^{12\cdot 14/8} = -1}$;

$\left(\frac{3}{13}\right)\left(\frac{13}{3}\right) = \underline{(-1)^{1\cdot 6} = +1}$; $\left(\frac{13}{3}\right) = \underline{+1}$; $\left(\frac{-142}{239}\right) = \underline{-1}$

Problem 3 (8 points):

(a, 4pts) Please show that $a = p-2 \equiv -2 \pmod{p}$ is a quadratic residue modulo a prime $p \geq 3$ if and only if $p \equiv 1 \pmod 8$ or $p \equiv 3 \pmod 8$. [Hint: Legendre symbol.]

$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\cdot\left(\frac{2}{p}\right) = \begin{cases} 1\cdot 1 = 1 & p \equiv 1 \pmod 8 \\ (-1)(-1) = 1 & p \equiv 3 \pmod 8 \\ 1\cdot(-1) = -1 & p \equiv 5 \pmod 8 \\ (-1)\,1 = -1 & p \equiv 7 \pmod 8 \end{cases}$

(b, 4pts) Suppose that $p \equiv 1 \pmod 8$. Let c be a quadratic non-residue modulo p, and let $b = c^{(p-1)/8} - c^{7(p-1)/8}$; note that $(p-1)/8 \in \mathbb{Z}$. Please show that $b^2 \equiv -2 \pmod p$.

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

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

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

$\equiv c^{\frac{p-1}{4}} - 2 + (-1)^3 c^{\frac{p-1}{4}} \equiv -2 \pmod p$

2016

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

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

(a, 4pts) For the primitive root $g' = 5$ there is a constant residue $k \in \mathbb{Z}_{22}$ such that for all residues $a \in \mathbb{Z}_{23} \setminus \{0\}$ one has $\mathrm{ind}_5(a) \equiv k \cdot \mathrm{ind}_{10}(a) \pmod{22}$. Please compute k (using the above table) and show your work.

$5^{\mathrm{ind}_5(a)} \equiv 10^{\mathrm{ind}_{10}(a)} \equiv a \pmod{23}$

$\mathrm{ind}_5(a)\ \underbrace{\mathrm{ind}_{10}(5)}_{15} \equiv \mathrm{ind}_{10}(a) \pmod{22}$

$k = 15^{-1} \bmod 22$

22	1	0
15	0	1
7	1	−1
1	−2	3

$3 \cdot 15 = 45 \equiv 1 \pmod{22}$

$K = 3$

(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

$$15x^{15} \equiv 16 \pmod{23}, \quad 18y^{16} \equiv 13 \pmod{23}, \quad 10^{-2z} \equiv 2z^2 \pmod{23}.$$

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

$15 \cdot \mathrm{ind}(x) + \underbrace{\mathrm{ind}(15)}_{13} \equiv \underbrace{\mathrm{ind}(16)}_{10} \pmod{22}$

$\mathrm{ind}(x) \equiv \underbrace{15^{-1}}_{3}(-3) \pmod{22}$

$-9 \equiv 13 \pmod{22}$

$x = 15$

11	1	0
8	0	1
3	1	−1
2	2	−3
1	3	−4

$3 \cdot 11 - 4 \cdot 8 = 1$

$16 \cdot \mathrm{ind}(y) + \underbrace{\mathrm{ind}(18)}_{4} \equiv \underbrace{\mathrm{ind}(13)}_{12} \pmod{22}$

$8 \cdot \mathrm{ind}(y) \equiv (12-4)/2 \equiv 4 \pmod{11}$

$\mathrm{ind}(y) \equiv \underbrace{8^{-1}}_{-4} \cdot 4 \equiv 6 \pmod{11}$

$\equiv 6, 17 \pmod{22}$

$y = 6, 17$

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

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

$20 + 9 = 22 + 7$

$21 + 19 \equiv 33 + 7$

$z = 20$

$z = 21$

2016

Problem 5 (5 points): Suppose Alice requests a digital signature from Bob using Taher El-Gamal's public key system with $p = 23$ and $g = 10$ by sending $h_A = (10^{r_A} \bmod 23) = 15$. Here r_A is a one-time random choice. Bob replies with his digital signature $\tau = (\sigma \cdot (h_A^{s_B})^{-1} \bmod 23) = 19$, where $h_B = (10^{s_B} \bmod 23) = 20$ is Bob's public key and s_B is Bob's secret private key. Please show how Alice can retrieve σ from her r_A and h_B. You may use the previous page for deriving Alice's r_A, and for powering, multiplication, and reciprocal modulo 23.

$\tau \cdot h_A^{s_B} \equiv \sigma\,(h_A^{s_B})^{-1}\; h_A^{s_B} \equiv \sigma \pmod{23}$

$h_A^{s_B} \equiv (10^{r_A})^{s_B} \equiv (10^{s_B})^{r_A} \equiv h_B^{r_A} \pmod{23}$

$20^{\underbrace{\text{ind}_{10}(15)}_{r_A}} \equiv 20^{13} \equiv x \pmod{23}$

$\text{ind}(x) \equiv 13 \cdot \text{ind}(20) \equiv 13 \cdot 9 \equiv -9 \cdot 9 \equiv 88 - 81 \equiv 7 \pmod{22}$

$x = 14 \equiv h_B^{r_A} \pmod{23}$

$\sigma = 19 \cdot 14 \equiv (-4)(-9) \equiv 36 \equiv 13 \pmod{23}$

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

$z = s^2 + t^2 = y + 2 = s^2 - t^2 + 2 \Rightarrow 2t^2 = 2 \Rightarrow t = 1$

$x = 2s,\; y = s^2 - 1,\; z = s^2 + 1$ with $s^2 - 1$ even

$s = 3$: $x = 6,\; y = 8,\; z = 10$

$6^2 + 8^2 = 10^2$

$s = 5$

$10^2 + 24^2 = 26^2$