S2008

Problem 1 (16 points)

(a, 4pts) Fermat's last theorem is a famous impossibility theorem of mathematics. Please state another impossibility theorem of mathematics.

- trisecting an angle with ruler & compass
- constructing a square of equal area as a circle with ruler and compass

(b, 4pts) True of false: For all integers x,y,z with $xyz \neq 0$ we have $x^4+y^4 \neq z^2$. Please explain your answer.

True, as proven in class.

(c, 4pts) True or false: If p is a positive prime integer and a,b,c are quadratic non-residue modulo p, then $(abc \bmod p)$ must be a quadratic non-residue modulo p. Please explain.

True:

If $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = \left(\frac{c}{b}\right) = -1$, *then* $\left(\frac{abc}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \cdot \left(\frac{c}{o}\right) = -1$, *so abc is a Q.N.R.*

(d, 4pts) Let $p > 1$ be a prime integer. How many residues in $\mathbb{Z}_p$ are primitive roots?

$\phi(p-1)$

Problem 2 (5 points): **Using the quadratic reciprocity law**, please compute the value of the Jacobi symbol $\left(\frac{58}{101}\right)$. Please show all your work.

$\left(\frac{58}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{29}{101}\right) = (-1)^{\frac{101^2-1}{8}}\left(\frac{29}{101}\right) = (-1)\cdot\left(\frac{29}{101}\right)$

$\left(\frac{29}{101}\right)\cdot\left(\frac{101}{29}\right) = (-1)^{\frac{29-1}{2}\cdot\frac{101-1}{2}} = +1$

$\left(\frac{101}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{7}{29}\right)$, $\left(\frac{7}{29}\right)\cdot\left(\frac{29}{7}\right) = (-1)^{\frac{29-1}{2}\cdot\frac{7-1}{2}} = +1$

$\left(\frac{29}{7}\right) = \left(\frac{1}{7}\right) = +1 \Longrightarrow \left(\frac{58}{101}\right) = +1.$

$\overset{+1}{\left(\frac{43}{101}\right)}\overset{+1}{\left(\frac{101}{43}\right)} = (-1)^{21\cdot 50} = +1$

$\underset{+1}{\left(\frac{101}{43}\right)} = \left(\frac{15}{43}\right)$

$\overset{+1}{\left(\frac{15}{43}\right)}\overset{-1}{\left(\frac{43}{15}\right)} = (-1)^{21\cdot 7} = -1$

$\underset{-1}{\left(\frac{43}{15}\right)} = \underset{-1}{\left(\frac{13}{15}\right)}, \left(\frac{13}{15}\right)\left(\frac{15}{13}\right) = (-1)^{6\cdot 7} = +1$

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

Problem 3 (5 points): The El Gamal public key cryptosystem is a *probabilistic* cryptosystem because clear text is encrypted using a different random residue for each cyphertext. Show that if instead a single fixed residue is used for all encryptions, the resulting *non*-probabilistic system can be broken by the *chosen ciphertext attack.*

The public keys are $g, p, h\ (= g^s \bmod p)$

The cipher text is $(\underbrace{g^r \bmod p}_{x}, \underbrace{M\cdot h^r \bmod p}_{y_M})$

One probes the encryption device (r fixed) with chosen cipher C and gets $(x, \underbrace{C\cdot h^r \bmod p}_{y_C})$

So $h^r \equiv y_C \cdot C^{-1} \bmod p$

and $M \equiv (h^r)^{-1} y_M \equiv y_C^{-1}\, C\, y_M \bmod p$.

r and S are not needed.

S 2008

Problem 4 (10 points): Consider the following table of indices (discrete logarithms) for the prime number 19 with respect to the primitive root $g = 2$:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\mathrm{ind}_2(a)$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

(a, 5pts) There are $\phi(9)$ residues in $\mathbb{Z}_{19} \setminus \{0\}$ that have (multiplicative) order 9 modulo 19 (belong to the exponent 9 modulo 19). By inspecting the above table, please list all those residues.

a has order $9 \Longleftrightarrow a = g^i$ *with* $\gcd(i, 18) = 2$.
So $a = 2^2 = 4, 2^4 \equiv 16, 2^8 \equiv 9, 2^{10} \equiv 17, 2^{14} \equiv 6, 2^{16} \equiv 5$ *are those residues.*
In numeric order: $4, 5, 6, 9, 16, 17$.

(b, 5pts) Using the above table, please solve $x \in \mathbb{Z}_{19}$ and all $y \in \mathbb{Z}_{19}$ the two congruences

$$x^3 \equiv 7 \pmod{19}, \quad 5y^5 \equiv 12 \pmod{19}$$

Please give all solutions and show your work.

$7 \equiv 2^6 \equiv 2^{6+18} \equiv 2^{6+2\cdot 18} \pmod{19}$
$x_1 \equiv 2^2 \equiv 4$, $x_2 \equiv 2^8 \equiv 9$, $x_3 \equiv 2^{14} \equiv 6 \pmod{19}$.

$5 \cdot ind_2(y) + ind_2(5) \equiv ind_2(12) \pmod{18}$,
$ind_2(y) \equiv 11(15 - 16) \equiv 7 \pmod{18}$ *(by extended Euclidean algorithm not shown), so* $y = 14$.

Problem 5 (6 points): Let $p > 2$ be a prime integer with $p \equiv 5 \pmod 8$, i.e., 8 divides $p+3$ and 4 divides $p-1$, and let $a \in \mathbb{Z}_p$ be a quadratic residue modulo p.
Since $a^{\frac{p-1}{2}} \pmod p = \left(\frac{a}{p}\right) = 1$ we must have $a^{\frac{p-1}{4}} \equiv \pm 1 \pmod p$.

(a, 3pts) Case $a^{\frac{p-1}{4}} \equiv 1 \pmod p$: Show that for $x = (a^{\frac{p+3}{8}} \bmod p)$ one has $x^2 \equiv a \pmod p$.

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

(b, 3pts) Case $a^{\frac{p-1}{4}} \equiv -1 \pmod p$: Let c be an arbitrary quadratic non-residue.
Show that for $x = (a^{\frac{p+3}{8}} c^{\frac{p-1}{4}} \bmod p)$ one has $x^2 \equiv a \pmod p$.

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

$$\equiv a \pmod p$$

Problem 6 (4 points): Please find three integers $x, y, z \in \mathbb{Z}_{>0}$ such that $x^2 + y^2 = z^4$. Please show your work.

$z^2 = s^2 + t^2$, *so we can choose* $s = 4$ *and* $t = 3$. *Thus* $x = 2st = 24$, $y = s^2 - t^2 = 7$, $z = 5$.

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