2007

Problem 1 (16 points)

(a, 4pts) Please state Fermat's little theorem and Euler's generalization to composite moduli.

Let p prime: $\forall a \in \mathbb{Z}_p, a \neq 0: a^{p-1} \equiv 1 \pmod{p}$

Euler's gen: Let $n \in \mathbb{Z}_{\geq 2}$: $\forall a \in \mathbb{Z}_n$, $GCD(a,n)=1: a^{\phi(n)} \equiv 1 \pmod{n}$

(b, 4pts) Let p be a positive prime integer and let ϕ be Euler's ϕ function. True or false: there are $\phi(\phi(p))$ primitve roots modulo p. Please explain your answer.

True:

Let g be a prim. root. Then all prim. roots are: g^i with $i \in \mathbb{Z}_{p-1}$, $GCD(i, p-1)=1$.

There are $\phi(p-1) = \phi(\phi(p))$ such residues

(c, 4pts) True or false: If p is a positive prime integer and a is a quadratic non-residue modulo p, then (a^3 mod p) must be a quadratic non-residue modulo p. Please explain.

True

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

(d, 4pts) Please explain the Diffie-Hellman private key exchange protocol.

Alice choses $a \in \mathbb{Z}_{p-1}$, publiches $g^a \bmod p$

Bob choses $b \in \mathbb{Z}_{p-1}$, publiches $g^b \bmod p$

Their common private key is

$$(g^b)^a \equiv g^{ab} \equiv (g^a)^b \pmod{p}.$$

Problem 2 (4 points): Please give the value of the sum $\sum_{d|300, d>0} \phi(d)$.

By Gauss's theorem, $\sum_{d|n, d>1} \phi(d) = n$,
so the sum is 300.

Problem 3 (5 points): **Using the quadratic reciprocity law**, please compute the value of the Legendre symbol $\left(\frac{232}{123}\right)$ Please show all your work.

$$\underbrace{\left(\frac{232}{123}\right)}_{-1} = \left(\frac{2^3 \cdot 29}{123}\right) = \left(\frac{2}{123}\right)^3 \cdot \left(\frac{29}{123}\right) = \left[(-1)^{\frac{(123 \bmod 16)^2 - 1}{8}}\right]^3 \cdot \left(\frac{29}{123}\right)$$

$$= (-1)^3 \cdot \underset{+1}{\left(\frac{29}{123}\right)}$$

$$\underset{+1}{\left(\frac{29}{123}\right)} \cdot \left(\frac{123}{29}\right) = (-1)^{\frac{29-1}{2} \cdot \frac{123-1}{2}} = (-1)^{14 \cdot *} = +1$$

$$\left(\frac{123}{29}\right) = \left(\frac{7}{29}\right) \cdot \left(\frac{29}{7}\right)$$

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

$$\left(\frac{29}{7}\right) = \left(\frac{1}{7}\right) = +1$$

$$\left(\frac{232}{123}\right) = \left(\frac{109}{123}\right),$$

$$\underset{-1}{\left(\frac{109}{123}\right)} \cdot \underset{-1}{\left(\frac{123}{109}\right)} = (-1)^{\frac{109-1}{2} \cdot \frac{123-1}{2}} = (-1)^{54 \cdot *} = +1$$

$$\left(\frac{109}{123}\right) = \left(\frac{2}{109}\right) \cdot \left(\frac{7}{109}\right), \quad \left(\frac{2}{109}\right) = (-1), \quad \left(\frac{7}{109}\right) = +1$$

$$\underset{+1}{\left(\frac{7}{109}\right)} \cdot \left(\frac{109}{7}\right) = (-1)^{* \cdot 54} = +1$$

$$\left(\frac{109}{7}\right) = \left(\frac{4}{7}\right) = +1$$

S 2007

Problem 4 (11 points): Consider the following table of indices (discrete logarithms) for the prime number 17 with respect to the primitive root $g = 3$:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\mathrm{ind}_3(a)$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

(a, 5pts) Using the above table, please solve in $x \in \mathbb{Z}_{17}$ and $y \in \mathbb{Z}_{17}$ the two congruences

$$x^3 \equiv 2 \pmod{17}, \quad y^5 \equiv 2 \pmod{17}$$

Please give all solutions.

$2 = 3^{14}$ $\quad 3^{3\alpha} = 3^{14}$ $\quad 3\alpha \equiv 14 \pmod{16}$

16 1 0
3 0 1
5 1 1 −5

$16 - 5 \cdot 3 = 1$

$3^{-1} \equiv -5 \equiv 11 \pmod{16}$

$\alpha \equiv 3^{-1} \cdot 14 \equiv (-5)\cdot(-2) \equiv 10 \pmod{16}$

$X = 3^{\boxed{10}} \equiv \boxed{8} \pmod{17}$

$3^{5\beta} \equiv 3^{14}$ $\quad \beta \equiv 5^{-1} \cdot (-2) \equiv (-3)(-2) \equiv 6$

16 1 0
5 0 1
3 1 1 −3

$y \equiv 3^{\beta} = 3^{\boxed{6}} \equiv \boxed{15} \pmod{17}$

(b, 6pts) Suppose a residue $M \in \mathbb{Z}_{17}$ has been encrypted by the el-Gamal public key system with public keys $p = 17$, $g = 3$ and $h \equiv 3^s \equiv 7 \bmod 17$. The ciphertext is

$$N = (g^r \bmod 17,\ M \cdot h^r \bmod 17) = (14, 14).$$

Please compute from N the encryption N' of $M' = M/3$, with $r' = (r + 1 \bmod 16)$, that **without** computing r or s. Please show your derivation.

$N' = (g^r \cdot g \bmod 17,\ M \cdot h^r \cdot h \cdot 3^{-1} \bmod 17)$

$= (14 \cdot 3 \bmod 17,\ 14 \cdot 7 \cdot 3^{-1} \bmod 17)$

$= ((-3) \cdot 3 \bmod 17,\ (-3) \cdot \underbrace{7 \cdot 6}_{8} \bmod 17)$

$= (8,\ 10)$

S2007

Problem 5 (5 points): Let $p > 2$ be a prime integer with $p \equiv 3 \pmod 4$ and let $a \in \mathbb{Z}_p$ be a quadratic non-residue modulo p. Show that for $x = (a^{\frac{p+1}{4}} \bmod p)$ one has $x^2 \equiv -a \pmod p$.

$$x^2 \equiv \left(a^{\frac{p+1}{4}}\right)^2 \equiv a^{\frac{p+1}{2}} \equiv a \cdot a^{\frac{p-1}{2}} \equiv -a$$
$$(\mathrm{mod}\ p)$$

because for a Q.N.R. a we have $a^{\frac{p-1}{2}} \equiv -1$
$(\mathrm{mod}\ p)$

Problem 6 (5 points): Please find integers $x, y, z \in \mathbb{Z}_{>0}$ such that $x^4 + y^2 = z^2$. Please show your work.

$x = 2st$ $\quad y = s^2 - t^2$ $\quad z = s^2 + t^2$

$= 2 \cdot 2 \cdot 1$ $\quad = 2^2 - 1^2$ $\quad = 2^2 + 1^2$

$= 2^2$ $\quad = 3$ $\quad = 5$

A solution is $2^4 + 3^2 = 5^2$