MAS 4203 - Quiz 5 - Summer 2015

Tuesday, August 4 Solution

NAME.

Instructions: All work should be written in a proper and coherent manner, and in a way that any student in the class can follow your work. Show all necessary reasoning and working. When giving proofs your reasoning should be clear. Only scientific or basic calculators are allowed.

TOTAL:

1. [5 × 2 = 10 pts]

(a) Complete the Definition: Let p be an odd prime and let $a \in \mathbb{Z}$ with $p \nmid a$. The Legendre symbol of a mod p denoted $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) := \begin{cases} 1, & \text{if } a \text{ is a quadratic residue mod } p \\ -1, & \text{if } a \text{ is a quadratic nonresidue mod } p. \end{cases}$$

(b) Complete Euler's Criterion: Let p be an odd prime, and let $a \in \mathbb{Z}$ with $p \nmid a$. Then

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

(c) Complete Gauss's Lemma: Let p be an odd prime, $a \in \mathbb{Z}$ & $p \nmid a$. Then $\left(\frac{a}{p}\right) = (-1)^n$

where n is number of least positive residues mod p of the integers $a, 2a, \ldots, \frac{1}{2}(p-1)a$ that are $> p/2$

(d) Use Gauss's Lemma to prove that

$$\left(\frac{2}{p}\right) = (-1)^n$$

where $n = \frac{1}{2}(p-1) - \left[\frac{p}{4}\right]$ and p is any odd prime

Consider the numbers

(*) $\quad 2, 2\cdot 2, \ldots\ldots, 2\cdot\left(\frac{1}{2}(p-1)\right) = (p-1)$

Each number is already reduced mod p.

$2k \leq \frac{p}{2}$ iff $1 \leq k \leq \frac{p}{4}$ iff $1 \leq k \leq \left[\frac{p}{4}\right]$.

The # of numbers in (*) $\leq p/2$ is $\left[\frac{p}{4}\right]$. & the # of numbers in (*) $> p/2$ is $\frac{1}{2}(p-1) - \left[\frac{p}{4}\right]$.

Therefore by Gauss's Lemma, $\left(\frac{2}{p}\right) = (-1)^n$ where $n = \frac{1}{2}(p-1) - \left[\frac{p}{4}\right]$.

(e) Suppose p is an odd prime, $a \in \mathbb{Z}$ & $p \nmid a$. Prove the following case of Euler's Criterion:

If $\left(\frac{a}{p}\right) = 1$ then $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

[Hint: Use Fermat's Little Theorem]

Suppose $\left(\frac{a}{p}\right) = 1$. Then $x_0^2 \equiv a \pmod{p}$ for some $x_0 \in \mathbb{Z}$, $p \nmid x_0$ since a is a quadratic residue mod p.

$$a^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 \pmod{p}$$

by Fermat's Little Thm since p is prime & $p \nmid x_0$

Hence

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

2. [4+6 = 10 pts]

(a) Complete the Law of Quadratic Reciprocity:

Let p, q be distinct odd ... primes. Then

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

$$= \begin{cases} 1, & \text{if } p \text{ or } q \equiv 1 \pmod 4, \\ -1, & \text{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Furthermore:

If p or $q \equiv 1 \pmod 4$ .... Then $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.

If $p \equiv q \equiv 3 \pmod 4$ .... Then $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

(b) Find $\left(\frac{-158}{101}\right)$. Show all reasoning.

$\left(\frac{-158}{101}\right) = \left(\frac{44}{101}\right)$ since $202 - 158 = 44$ & $-158 \equiv 44 \pmod{101}$.

$= \left(\frac{4}{101}\right)\left(\frac{11}{101}\right)$ since $44 = 4 \cdot 11$.

$= \left(\frac{11}{101}\right)$ since $4 = 2^2$.

$= \left(\frac{101}{11}\right)$ by LQR since $101 \equiv 1 \pmod 4$.

$= \left(\frac{2}{11}\right)$ since $101 \equiv 2 \pmod{11}$

$= -1$ since $11 \equiv 3 \pmod 8$.

3. [4+6 = 10 pts]

(a) Find congruences that characterize all prime numbers p for which 3 is a quadratic residue mod p.

Let p be an odd prime, $p \neq 3$.

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right) & \text{if } p \equiv 1 \pmod 4 \\ -\left(\frac{p}{3}\right) & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

By the Law of Q.R. $(\pm 1)^2 \equiv 1 \pmod 3$ &

$$\left(\frac{p}{3}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3 \\ -1 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

$p \equiv 1, 5, 7$ or $11 \pmod{12}$.

$p \pmod{12}$	$p \pmod 3$	$p \pmod 4$	$\left(\frac{3}{p}\right)$
1	1	1	$\left(\frac{p}{3}\right) = +1$
5	2	1	$\left(\frac{p}{3}\right) = -1$
7	1	3	$-\left(\frac{p}{3}\right) = -1$
11	2	3	$-\left(\frac{p}{3}\right) = --1 = +1$

We see $\left(\frac{3}{p}\right) = +1$ iff $p \equiv 1$ or $11 \pmod{12}$.

3 is a q.r. mod p iff $p \equiv 1$ or $11 \pmod{12}$ (assuming p is a odd prime, $p \neq 3$).

(b) Do ONE part.

(i) Prove or disprove that there is an integer n such that n^2+2 is divisible by 2013.

(ii) Let p, q be odd distinct primes where $p = q + 4a$ & $a \in \mathbb{Z}$. Prove that

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

(i) $2013 = 3 \cdot 11 \cdot 61$

Suppose by way of contradiction that for some $n \in \mathbb{Z}$.

$2013 \mid n^2+2$ then $61 \mid (n^2+2)$ &

$n^2 \equiv -2 \pmod{61}$ &

$\left(\frac{-2}{61}\right) = +1.$

But $\left(\frac{-2}{61}\right) = \left(\frac{-1}{61}\right)\left(\frac{2}{61}\right)$

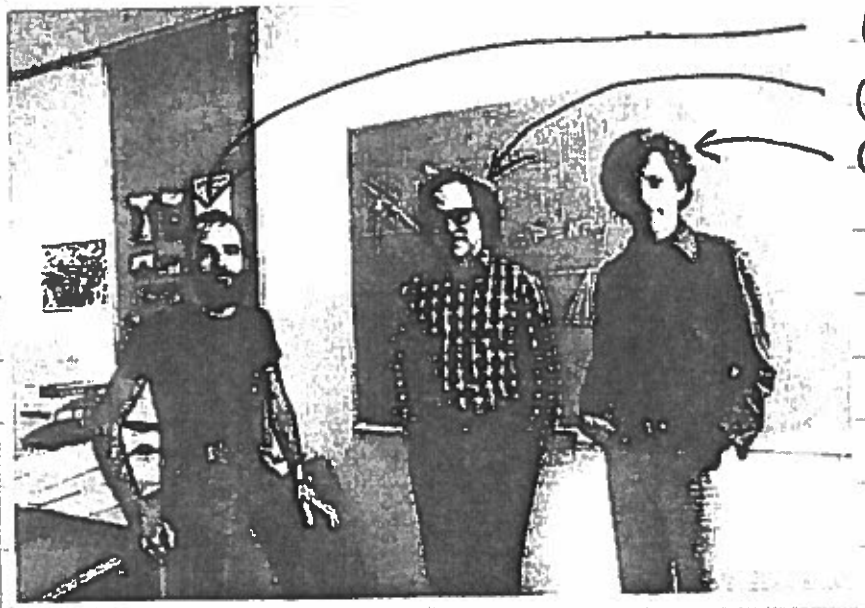
$= \left(\frac{2}{61}\right)$ since $61 \equiv 1 \pmod 4$

$= -1$ since $61 \equiv 5 \pmod 8$,

which is a contradiction.

The statement is false. There are no integers n such that n^2+2 is divisible by 2013.

4. [2 Bonus pts]



RSA is one of the first practicable _____ cryptosystems and is widely used for _____ data transmission. In such a cryptosystem the encryption key is _____ and differs from the decryption key which is kept _____. In RSA, this asymmetry is based on the practical difficulty of _____ the product of two large _____. RSA stands for R___ R_____, A___ S_____, and L_____ A_____, who first publicly described the algorithm in _____.

Suppose p, q distinct odd primes, $p = q + 4a$ say at $\mathbb{Z}$. Since p, q are distinct primes $p \nmid a$ & $q \nmid a$.

$$\left(\frac{p}{q}\right) = \left(\frac{q+4a}{q}\right) = \left(\frac{4a}{q}\right) \quad \text{since } q+4a \equiv 4a \pmod{q}$$

$$= \left(\frac{4}{q}\right)\left(\frac{a}{q}\right) = \left(\frac{a}{q}\right) \quad \text{since } 4 = 2^2 \text{ \& } \left(\frac{4}{q}\right) = 1.$$

$$\left(\frac{q}{p}\right) = \left(\frac{p-4a}{p}\right)$$

$$= \left(\frac{-4a}{p}\right) \quad \text{since } p - 4a \equiv -4a \pmod{p}.$$

$$= \left(\frac{4}{p}\right)\left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)$$

$$= \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) \quad \text{since } 4 = 2^2.$$

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \pmod{4} \\ -\left(\frac{p}{q}\right) & \text{if } p \equiv 3 \pmod{4} \end{cases}$$

by LQR since $p \equiv q \pmod 4$.

$$\text{So } \left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{q}\right) \text{ since } \left(\frac{-1}{p}\right) = \begin{cases} 1 \text{ if } p \equiv 1 \pmod 4 \\ -1 \text{ if } p \equiv 3 \pmod 4. \end{cases}$$

Now $\left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{q}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{q}\right)$ &

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$