Instructor: Leo Goldmakher

NAME: _____

**Williams College**
**Department of Mathematics and Statistics**

# MATH 313 : NUMBER THEORY

**Problem Set 7 – due Thursday, November 15th**

**INSTRUCTIONS:**
This assignment should be turned in to me in person (i.e. don't leave them in my mailbox or ask someone else to submit on your behalf) at the beginning of Thursday's class. Late assignments may be left in my mailbox (just inside the entrance to Bascom) by **4pm** on Friday; however, 5% will be deducted for late submission. *Assignments submitted later than 4pm on Friday will not be graded.*

Please print and attach this page as the first page of your submitted problem set.

| **PROBLEM** | **GRADE** |
|---|---|
| 7.1 | |
| 7.2 | |
| 7.3 | |
| 7.4 | |
| 7.5 | |
| 7.6 | |
| **Total** | |

Please read the following statement and sign **before starting this problem set:**

*I understand that I am not allowed to use the internet to assist with this assignment. I also understand that I must write down the final version of my assignment in isolation from any other person, and to not copy from any set of written notes created when another person was present. I pledge to abide by the Williams honor code.*

**SIGNATURE:**_____

# Problem Set 7

**7.1** In class I mentioned the following formula for $\left(\frac{2}{p}\right)$:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

(a) Determine (with proof) an analogous formula for $\left(\frac{3}{p}\right)$.

(b) Determine (with proof) an analogous formula for $\left(\frac{5}{p}\right)$.

**7.2** Compute (using whatever tricks you like, including the previous problem) the following Legendre symbols:

(a) $\left(\frac{22}{31}\right)$

(b) $\left(\frac{12}{31}\right)$

(c) $\left(\frac{77}{103}\right)$

**7.3** Prove the Chinese Remainder Theorem v1 (see Lecture 16 summary).

**7.4** As in our proof of QR, let

$$L := \{k \in \mathbb{Z}_{pq}^\times : k < {}^{pq}/_2\} \qquad \text{and} \qquad R := \{(a,b) \in \mathbb{Z}_p^\times \times \mathbb{Z}_q^\times : b < {}^{q}/_2\}.$$

Prove that for every $(a,b) \in R$ there is a unique $k \in L$ such that $\beta(k) = \pm(a,b)$.

**7.5** When a group of soldiers is arranged in a rectangle with 17 people per row, there are 3 soldiers left over. When the same group is lined up in rows of 33, there are 7 soldiers left over. How many soldiers are in the group? *You will not receive credit for a brute force solution.*

**7.6** Fix $p \geq 3$ and $a \in \mathbb{Z}_p^\times$. In this problem we explore how to solve the quadratic congruence

$$(*) \qquad x^2 \equiv a \pmod p.$$

(a) Prove the existence of $n \in \mathbb{Z}_p^\times$ such that $n^{(p-1)/2} \equiv -1 \pmod p$. In practice, how difficult would you expect it to be to find such an $n$? Justify your answer.

**• For the rest of the problem, fix a suitable choice of $n$ from part (a).**

(b) In class we saw a method for solving (*) in the case $p \equiv -1 \pmod 4$. Apply this method to find all solutions to the congruence $x^2 \equiv 2 \pmod{19}$, and then find all solutions to the congruence $x^2 \equiv 3 \pmod{19}$. *You will not receive credit for a brute force solution.*

(c) Suppose $p \equiv 1 \pmod 4$ and that (*) has a solution. Prove that there exists an integer $k \geq 0$ such that $n^{2k} a^{(p-1)/4} \equiv 1 \pmod p$. If $p \not\equiv 1 \pmod 8$, find a solution to (*).

(d) Suppose $p \equiv 1 \pmod 8$. Prove that there exists an integer $k \geq 0$ such that $n^{2k} a^{(p-1)/8} \equiv 1 \pmod p$. If $p \not\equiv 1 \pmod{16}$, find a solution to (*).

(e) Find all solutions to $x^2 \equiv 1326 \pmod{1777}$. *You will not receive credit for a brute force solution.*

(f) Set $\mathcal{S}_j := \left\{p-1, \frac{p-1}{2}, \frac{p-1}{4}, \cdots, \frac{p-1}{2^j}\right\}$, and for any subset $\mathcal{A} \subseteq \mathcal{S}_j$ define

$$\Sigma(\mathcal{A}) := \sum_{\ell \in \mathcal{A}} \ell;$$

in words, $\Sigma(\mathcal{A})$ is the sum of all elements of $\mathcal{A}$. Prove that for any $j \leq \nu_2(p-1)$ there exists $\mathcal{A} \subseteq \mathcal{S}_{j-1}$ such that $n^{\Sigma(\mathcal{A})} a^{(p-1)/2^j} \equiv 1 \pmod p$. Why should we care about this result, in the context of the rest of this problem?