PMATH 145 Assignment 3

Patrick Ingram

DO NOT HAND IN

The following questions will not be collected or marked, and are mostly just for your benefit in terms of midterm preparation. I highly encourage completing all of these. I will not be posting solutions, since these are all based on things we did in class, and because the only thing worse than not knowing how to do one of these problems is to not know but *think* you know because you read the solution.

Problem 1. Find the least non-negative residue of the following, or explain why you can't. (In theory, it's possible to do all of them, but not all of them follow from theorems we covered, and it's good to be able to tell which are which.)

i. $2^{54343543} \pmod{11}$

ii. $5^{101^{197^{219}}} \pmod{23}$

iii. $6^{2342^{717}} \pmod{23}$

Problem 2. Let $f(x) = x^{36} + x^{12} + 24$. Show that if n is a natural number, and n is not divisible by 13, then $f(n)$ is composite.

Problem 3. Find the last two digits of the number $252687^{169363^{23315}}$.

Problem 4. i. Find a value $c \in \mathbb{Z}$ such that

$$x \equiv 61 \pmod{103} \quad \text{and} \quad x \equiv 19 \pmod{217}$$

if and only if $x \equiv c \pmod{22351}$.

ii. Find a value $c \in \mathbb{Z}$ such that

$$x \equiv 13 \pmod{93},$$
$$x \equiv 17 \pmod{67},$$

and

$$x \equiv 21 \pmod{55}$$

if and only if $x \equiv c \pmod{342705}$.

Problem 5. Let $p \geq 3$ be a prime, and let $Q_p \subseteq \mathbb{Z}_p$ be defined by

$$Q_p = \{[x] \in \mathbb{Z}_p : [x] \neq [0] \text{ and } [x] = [y^2] \text{ for some } [y] \in \mathbb{Z}_p\}.$$

So, for example, $Q_5 = \{[1], [4]\}$. (The Q is for "quadratic", or square.)

i. Show that Q_p contains exactly $(p-1)/2$ congruence classes (that's exactly half of the non-zero congruence classes modulo p).

ii. Show that if $[a], [b] \in Q_p$, then $[ab] \in Q_p$.

iii. Show that if $[a] \notin Q_p$ and $[b] \in Q_p$, then $[ab] \notin Q_p$.

iv. Show that if $[a] \notin Q_p$ and $[b] \notin Q_p$, then $[ab] \in Q_p$ (hint: consider the function $f([x]) = [ax]$...)

v. For $a \in \mathbb{Z}$ not divisible by p, define the Legendre Symbol of a modulo p by

$$\left(\frac{a}{p}\right)_{\mathrm{L}} = \begin{cases} +1 & \text{if } [a] \in Q_p \\ -1 & \text{if } [a] \notin Q_p. \end{cases}$$

Show that for all $a, b \in \mathbb{Z}$ not divisible by p,

$$\left(\frac{ab}{p}\right)_{\mathrm{L}} = \left(\frac{a}{p}\right)_{\mathrm{L}} \left(\frac{b}{p}\right)_{\mathrm{L}}.$$

(Actually, you can define the Legendre Symbol modulo p for all $a \in \mathbb{Z}$ by setting $\left(\frac{a}{p}\right)_{\mathrm{L}} = 0$ when $p \mid a$, and it *still* satisfies the above relation.)