

Name:

Collaborator(s)¹:

Math 453, Section X13, Prof. Hildebrand, Spring 2011

HW Assignment 8, due Friday, 4/8/2011

Instructions

- **Rules:** The usual: Write your name on the cover sheet and staple the sheet to the assignment. The assignment is due in class at the above due date. Do the problems in order, and make sure that each problem is clearly labelled. Write legibly, using proper mathematical notation and terminology. As always, solutions, rather than answers, are expected for all problems; you have to clearly show how you arrived at the answer, using appropriate techniques, algorithms, and theorems.

- **Hints for this assignment:** The first few problems (from 4.3) are exercises in computing Legendre symbols, similar to the examples worked in class in 3/18 and 3/28. As illustrated in class, using the full array of tools (multiplicativity and periodicity of the Legendre symbol, Quadratic Residue Law), computations of this type can easily be done by hand.

Two of the problems in 4.3 are non-numerical and couched as proof questions, but the “proofs” needed are just the same kind of manipulations using periodicity and multiplicativity of the Legendre symbol and the Quadratic Residue Law, etc., that you have to do for the purely numerical questions.

The remaining problems are from Chapter 5 and deal with primitive roots and orders. Most of these are stated as computational exercises, but the main point of these problems is not the actual calculation (nor the final answer), but the theorems and algorithms that enable one to do the computations efficiently. Trying brute force approaches, or using the primitive root table in the back of the book, would defeat this purpose and would leave you unprepared in exam situations.

- **Additional resources:** For additional examples and practice material, see the chapter on primitive roots in Rosen’s “Elementary Number Theory” (on course reserve in the Math Library), which is structured in the same way as Strayer, but has many more problems and examples at all levels. (Strayer’s text is essentially a “light” version of the Rosen text. The latter is more than double the size of Strayer ...)

HW 8 Problems (from Sections 4.3, 5.1, 5.2 of Strayer)

1. *4.3:28(b)(d)
2. *4.3:30
3. *4.3:32 (Hint: Rephrase in terms of Legendre symbols)
4. *4.3:36(b) (Hint: The same problem, with 3 in place of -5 , was worked out in class.)
5. *5.1:1(a)(b)(c)
6. *5.1:3(a)(b)(c)
7. *5.2:11(b) (Hint: You may use the fact that $r = 2$ is a primitive root modulo 37.)
8. *5.2:12(a)(b) (Hint: (a) Try contradiction. (b) Use part (a).)
9. *5.2:17(a)(b) (Fermat strikes again! Hint: See an earlier problem.)

***** Extra Credit Problem on Back of Page *****

¹If you worked with another student or in a small group on this assignment, list the names of all students involved.

10. **Extra credit.**² **The quadratic residue random walk.** Let \vec{v}_α denote the vector in the plane of length 1 and forming an angle $(2\pi\alpha)$ with respect to the positive x -axis. (Thus, $\vec{v}_0 = (1, 0)$ points in direction of the positive x -axis, $\vec{v}_{1/8} = (1/\sqrt{2}, 1/\sqrt{2})$ points in direction $\pi/4$, i.e., the main diagonal, $\vec{v}_{1/4} = (0, 1)$ points in direction $\pi/2$, i.e., the positive y -axis, etc.) Think of \vec{v}_α as a “move”, and a sequence of such vectors \vec{v}_α (with different α 's) as a “random walk” consisting of unit steps.

Now, let p be an odd prime and consider moves of the form $\vec{v}_{a/p}$. It is easy to convince yourself that the path obtained by performing *all* p moves $\vec{v}_{a/p}$, for $a = 0, 1, 2, \dots, p-1$, is a regular polygon, and you end up at the exact spot you started out at.

More interesting is the case when only moves $\vec{v}_{a/p}$ with $(a, p) = 1$ are allowed. This amounts to deleting those vectors of the polygonal path that correspond to an a that is not relatively prime with p , and recombining the remaining vectors. Again one can ask at what point you end up. This problem was mentioned in class some time ago, and it has a surprising answer: You end up either at your original spot, or one unit to the left, or one unit to the right, depending on the value of the Moebius function at the denominator p . (For this version, p can be any natural number, not necessarily prime.)

Now lets add one more (devilish!) twist to the situation: Instead of moving in direction $\vec{v}_{a/p}$ at each stage, you move in direction $\vec{v}_{a/p}$ or $-\vec{v}_{a/p}$, with the \pm sign determined by the Legendre symbol $(\frac{a}{p})$. In other words, if a is a quadratic residue modulo p , you move in direction $\vec{v}_{a/p}$, if it is a quadratic nonresidue, you move in direction $-\vec{v}_{a/p}$. Thus, the sequence of moves performed is the following:

$$(1) \quad \left(\frac{1}{p}\right) \vec{v}_{1/p}, \left(\frac{2}{p}\right) \vec{v}_{2/p}, \left(\frac{3}{p}\right) \vec{v}_{3/p}, \dots, \left(\frac{p-1}{p}\right) \vec{v}_{(p-1)/p}.$$

We will call the random walk formed by moves (1) the **quadratic residue random walk modulo p** .

The \pm signs coming from the Legendre symbols throw things off balance quite a bit, add a random element to the situation, and raise the following problem:

PROBLEM: *Where do you end up if you perform the quadratic residue random walk modulo p , starting at the origin?*

You can earn extra credit by exploring this question in one of two ways:

- **Numerical exploration:** This is a lot more fun, but requires solid programming skills, or a good deal of experience with Mathematica, Matlab, or a similar tool. Plot the paths of a quadratic residue random walk for different choices of the prime p , and focus on the location of the end points of the path. Try to guess the answer to the above question. You'll have to work with primes in the hundreds or thousands to get enough evidence for a reasonable guess. An interesting side note is the shape of these plots. Most shapes seem random except for some obvious symmetries, but $p = 7561$ leads to a distinctive oval-type shape. (The reasons for this are mysterious to me. If you find other primes leading to the same shape, I'd be curious.)
- **Theoretical exploration:** This is more difficult and not for the faint of heart. Try to analyze the situation theoretically and *prove* a (simple) formula for the endpoint the path (or the distance between the endpoint and the starting point).

²No hints, help, or group work on extra credit problems, as this would defy the intent of these problems.