Assignment #6

Announcement: Office hours Monday, May 17 and Monday, May 24 will be 11:00-12:00.

Problems due **Friday, May 21**:

To do but not hand in:

p. 133, Ex. 10;

p. 203, Ex. 3;

p. 206, Ex. 1;

H-1, H-3, H-4, H-5.

To hand in:

p. 200-1, Exs. 9, 15;

p. 206, Ex. 1;

I-1, I-2, H-6, H-7.

Problem I-1. As discussed in class, the 4-element field $\mathbb{F}_4$ has characteristic 2 and elements $0, 1, \alpha, 1+\alpha$. Addition takes place in the obvious way (except that any element plus itself equals 0), while multiplication is calculated using $\alpha^2 = \alpha + 1$.

To construct this field we used matrices $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$. Then we could call the first three $0, 1, \alpha$ respectively and notice that the fourth is $1 + \alpha$. Then we could forget about where $0, 1, \alpha, 1 + \alpha$ came from.

(a) Recall from lecture the fact that in a finite field there is always a generator for the units (the nonzero elements). Decide which elements of $\mathbb{F}_4$ are generators of the units. (Show your work.)

(b) Decide whether $\mathbb{F}_4$ is isomorphic as a ring to $\mathbb{Z}/4\mathbb{Z}$. (Why?)

If your answer is yes, then you need to give a one-to-one correspondence between elements of $\mathbb{F}_4$ and elements of $\mathbb{Z}/4\mathbb{Z}$ that is compatible with addition and multiplication.

If your answer is no, then it is enough to give some property true in one and false in the other, not tied to names of elements—for example, do both have the same number of solutions to $x^2 = x$? (Well, yes in this case, but maybe no for something else?) In spite of the statement about names of elements

not mattering, for any isomorphism 0 and 1 do have to correspond, since 0 can be uniquely described as the additive identity and 1 can be uniquely described as the multiplicative identity.

(c) When you construct $\mathbb{C}$ starting with $\mathbb{R}$, you are essentially taking a real polynomial that didn't have a root, namely x^2+1, and then making a larger field in which it does have a root. The same was true in going from $\mathbb{F}_3$ to $\mathbb{F}_9$.

In starting from $\mathbb{F}_2$ $(= \mathbb{Z}/2\mathbb{Z})$ and making $\mathbb{F}_4$, you are also taking a polynomial with coefficients in $\mathbb{F}_2$ that didn't have a root and adding a root. Which polynomial? (Notice that for $\mathbb{F}_2$, x^2+1 *does* have a root in $\mathbb{F}_2$, namely 1, since $1^2+1=0$.)

(d) Just as $\mathbb{C}$ can be regarded as a two-dimensional vector space over the field $\mathbb{R}$, with a basis consisting 1 and i, $\mathbb{F}_4$ can be considered as a vector space over $\mathbb{F}_2$. What would be a good choice of basis? (You want every element of $\mathbb{F}_4$ to be a unique linear combination using this basis, with coefficients from $\mathbb{F}_2$.)

Problem I-2. In this problem, elements of $\mathbb{F}_4$ are always listed in the order $0, 1, \alpha, 1+\alpha$. So if we make a table with rows and columns indexed by these elements, the table is 4×4 and we might refer to the entry in "row $i = \alpha$, column $j = 1+\alpha$", which is in the position we would ordinarily call (3,4).

For $r =$ each of $1, \alpha, 1+\alpha \in \mathbb{F}_4$, let T_r mean the 4×4 table whose (i,j)-th entry is $i + rj$, where $i, j \in \mathbb{F}_4$. For example, T_1 is just the addition table for $\mathbb{F}_4$.

(a) Write out the three tables.

(b) As you see, each of the tables has the property that each row has four different elements (out of 4) and each column has four different elements. Such a table is called a *Latin square*. Show that in fact the T_r construction gives a Latin square when carried out in any finite field, not just $\mathbb{F}_4$.

(c) Two Latin squares of the same size are said to be *orthogonal* if, when you lay one on top of the other, you get every possible pair of elements. For example, if you had two 4×4 Latin squares and one had entries a, b, c, d and the other had entries r, s, t, u, then a would occur against r in exactly one position, c would occur against s in exactly one position, etc. To put it another way, the pairs of entries you have matched up are all distinct. For example, Problem G-1 was really asking for two orthogonal 4×4 Latin squares, where the indices were card suits and card numbers.

Show that each two of the Latin squares $T_1, T_\alpha, T_{1+\alpha}$ are orthogonal. In fact, show that using any finite field the T_r construction gives Latin squares so that for $r \neq s$, T_r and T_s are orthogonal.

So using $\mathbb{F}_4$ you can construct not just two orthogonal Latin squares but three, each two of which are orthogonal. And using a field with 9 elements you could construct eight pairwise orthogonal Latin squares, etc. Moreover, Problem G-1 can be solved by taking two of the three 4×4 Latin squares and relabeling field entries as card suits and numbers.

Problem I-3. (Diffie-Hellman key exchange) Let $p = 14,737,727$, which is prime, and let $g = 5$, which is a generator of the units of $\mathbb{Z}/p\mathbb{Z}$.

(a) If you know someone in the class, do a key exchange with him/her as follows; if you don't know someone then do it with me. Suppose you are person A and your friend is Person B.

The goal is for you both to arrange a secret number by email—a number that you can both compute, but which can't be guessed by someone else who is secretly reading your email.

Step 1. Choose some number $a < p$ at random (just a messy number), which you will keep private, even from B.

Step 2. Using the calculator on the Math 117 home page, calculate $g^a \pmod p$ and send the result in email to B. (For the calculator, leave out the commas in p.)

Meanwhile, B should do the same, choosing a number b at random and sending you $g^b \pmod p$ in email.

Step 3. When you get B's email with $g^b \pmod p$, use the calculator to take that number to the a power $\pmod p$.

B should do the corresponding calculation, taking your number g^a to the b power $\pmod p$.

Since $(g^a)^b = g^{ab} = (g^b)^a \pmod p$, you and B now know a secret number in common, namely g^{ab}, even though you never sent it in email.

(b) As a demo, send B a one-word message by choosing an English word of three or four letters, encoding it with 2 digits per letter, adding the six or or eight digits to your secret key, and sending the sum to B. B can then decode it by subtracting the secret key. Meanwhile, B should send you a message the same way. You can use the encoding in this table:

01	02	03	04	05	06	07	08	09	10	11	12	13
A	B	C	D	E	F	G	H	I	J	K	L	M
14	15	16	17	18	19	20	21	22	23	24	25	26
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Notes:

- In writing up this problem, give a record of the numbers you calculated or observed.

- If you want to use a group of three or more people, you can send messages cyclically, e.g. $A \to B \to C \to A$.
- Even though p may seem large, this is still a small "toy" problem, not a practical one, for reasons that will become clear later.