MAT 312/AMS 351
Midterm exam #2 with solutions
Thursday 11/14/02

1. (a) State precisely Euler's theorem.
SOLUTION Let n be a positive integer and let a be an integer that is relatively prime to n. Then

$$a^{\varphi(n)} \equiv 1 \mod n.$$

(b) Compute the last two digits of 7^{523}.
SOLUTION We need to calculate the standard representative of $7^{523} \mod 100$. Since $\varphi(100) = \varphi(2^2 5^2) = (4-2)(25-5) = 40$, we have

$$7^{523} = 7^{13\cdot 40+3} \equiv 7^3 = 343 \equiv 43 \mod 100.$$

(c) Does there exist a positive integer x such that $(23^{33})^x \equiv 23 \mod 400$? If yes, find the smallest such x. If not, explain why.
SOLUTION Certainly there exists such an x since $\varphi(400) = \varphi(2^4 5^2) = 8 \cdot 20 = 160$ and $(33, 160) = 1$. The congruence class $[x]_{\varphi(400)}$ should be the inverse of $[33]_{\varphi(400)}$. So we express the gcd of 33 and 160 as a linear combination of these integers using the Euclidean algorithm:

$$\left[\begin{array}{rr|r} 1 & 0 & 33 \\ 0 & 1 & 160 \end{array}\right] \xrightarrow{-4} \left[\begin{array}{rr|r} 1 & 0 & 33 \\ -4 & 1 & 28 \end{array}\right] \xrightarrow{-1} \left[\begin{array}{rr|r} 5 & -1 & 5 \\ -4 & 1 & 28 \end{array}\right] \xrightarrow{-5} \left[\begin{array}{rr|r} 5 & -1 & 5 \\ -29 & 6 & 3 \end{array}\right] \xrightarrow{-1}$$

$$\left[\begin{array}{rr|r} 34 & -7 & 2 \\ -29 & 6 & 3 \end{array}\right] \xrightarrow{-1} \left[\begin{array}{rr|r} 34 & -7 & 2 \\ -63 & 13 & 1 \end{array}\right].$$

Thus $(-63)(33) + (13)(160) = 1$ and $x = 160 - 63 = 97$.

2. Let n be a positive integer.
(a) How many elements are there in the group $(\mathbb{Z}_n, +)$?
SOLUTION The group $\mathbb{Z}_n$ contains n elements.

(b) Assume, for this part only, that $n \geq 10$. What is the inverse of $[7]_n$ in $(\mathbb{Z}_n, +)$? Write this inverse as $[b]_n$ for the smallest positive b.
SOLUTION $b = n - 7$.

(c) There is one element in each $(\mathbb{Z}_n, +)$ that is its own inverse. What is it? For some n there is another element that is its own inverse. What is the condition on n for there to exist precisely two elements that are their own inverses, and, in these cases, what are the two elements?

SOLUTION The congruence class $[0]_n$ is always its own inverse in $(\mathbb{Z}_n, +)$. In general $[a]_n$ is its own inverse if $2a \equiv 0 \mod n$. Since it involves no loss of generality to assume that $0 \leq a \leq (n-1)$, we see that $2a \equiv 0 \mod n$ iff $a = 0$ and in addition if n is even, $a = \frac{n}{2}$.

(d) How many elements are there in the group $(\mathbb{Z}_n^*, \cdot)$?
SOLUTION The group $\mathbb{Z}_n^*$ contains $\varphi(n)$ elements.

(e) Does $[7]_{12}$ belong to $(\mathbb{Z}_{12}^*, \cdot)$? If not, explain why. If yes, determine its inverse and write this inverse as $[c]_{12}$ for some integer c with $0 < c < 12$.
SOLUTION The congruence class $[7]_{12}$ belongs to $(\mathbb{Z}_{12}^*, \cdot)$ since $(7, 12) = 1$. By inspection $[7]_{12}$ is its own inverse. (You could, of course, use the Euclidean algorithm to find $[7]_{12}^{-1}$.)

3. (a) Let G be the set of 2×2 complex matrices whose entries are restricted to be one of the four numbers ± 1 and $\pm \imath$. Is G a group under matrix multiplication? Justify your answer.
SOLUTION Since $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \in G$ and

$$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & * \\ * & * \end{bmatrix} \notin G$$

(the $*$s in the above equation indicate that the answer to the question does NOT require the calculation of these matrix entries), G is not closed under matrix multiplication.
(ASIDE: THe set G consists of $4^4 = 256$ matrices.)

(b) Construct a multiplication table for a group with 4 elements e, a, b and c, where e is the identity of G. Justify your conclusions.
SOLUTION Since e is the identity element. Part of the multiplication table is obvious:

	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

.

(The ij entry in our matrices representing the products will be the product of the row entry to the left of the double bar times the column entry above the first double line – although as will be seen below since all groups with 4 elements are abelian, the consideration of the order of multiplication is not needed in these cases.) The identity e can only be the inverse of the identity. Hence one of the other three elements, say a, must also be its own inverse. Now there are two possibilities: either both b and c are their own inverses or $bc = cb = e$.

We thus have that

	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

or

	e	a	b	c
e	e	a	b	c
a	a	e		
b	b			e
c	c		e	

.

The products in each column and in each row must be a permutation of the four entries. Let's call this *the permutation principle*. This is enough to determine the entire multiplication table. In the first case, ba cannot be e (this would say that $b^{-1} = a$) nor a (this would say that $b = e$) nor b (this would say that $a = e$). Hence $ba = c$. This suffices to determine all other entries in the multiplication by the permutation principle. The reasoning in the second case is similar. We end up with

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	q	e

or

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

.

Since each multiplication table is symmetric about its diagonal, we have shown that there are precisely 2 groups with 4 elements and both are abelian.

4. (a) Show that the square of an arbitrary integer x is congruent to either 0 or 1 $\mod 4$.
SOLUTION Write $x \equiv r \mod 4$ with $r = 0, 1, 2$ or 3. Then $x^2 \equiv r^2 \mod 4$. We now observe that $0^2 = 0$, $1^2 = 1$, $2^2 \equiv 0 \mod 4$ and $3^2 \equiv 1 \mod 4$.

(b) Let x and $y \in \mathbb{Z}$ and assume that $x^2 + y^2 \equiv r \mod 4$ for a non-negative integer r which is chosen as small as possible. What are the possible values of r? Why?
SOLUTION From part (a), $x^2 \equiv a \mod 4$, with $a = 0$ or 1 and $y^2 \equiv b \mod 4$, with $b = 0$ or 1. Thus $x^2 + y^2 \equiv a + b \mod 4$. The only possible values for $a + b$ are 0, 1 or 2.

(c) Show that not every positive integer is the sum of two squares (of integers).
SOLUTION By part (b), positive integers congruent to 3 mod 4 cannot be sums of two squares.

(d) List the first 4 positive integers that are not sums of two squares (note that $1 = 1^2 + 0^2$ is a sum of two squares).
SOLUTION 3, 7, 11 and 15 are candidates. But there may be smaller integers. Perhaps 2 or 6 or 10 is also not the sum of two squares. Since every square is the sum of itself and 0, we need only examine 2, 5, 6, 8, 10, 12, 13 and 14. We can argue as follows if $a = x^2 + y^2$, then we can always assume that $x \geq y \geq 0$. Each square must be at most a and the first square x^2 must contribute at least $\frac{a}{2}$ to the sum. There are few choices for the small integers: $2 = 1^2 + 1^2$, $5 = 2^2 + 1^2$, $6 = 2^2 + ?$ (so 6 is not a sum of two squares), $8 = 2^2 + 2^2$ and $10 = 3^2 + 1^2$. Thus the first 4 positive integers that are not sums of two squares are 3, 6, 7

and 11.

5. This question deals with the permutation group $S(n)$, $n \geq 1$.
(a) How many elements does $S(n)$ contain? For what values of n, is $S(n)$ an abelian group?
SOLUTION The group $S(n)$ contains $n!$ elements. It is abelian only for $n = 1$ and 2.

(b) Give an example of two elements of $S(n)$ that do not commute. What value of n are you using?
SOLUTION We can use any $n \geq 3$ and observe that

$$(1,2)(1,3) = (1,3,2) \neq (1,2,3) = (1,3)(1,2).$$

(c) Define the order of a permutation.
SOLUTION The *order* m of a permutation π is the smallest positive integer such that π^m is the identity.

(d) Describe the collection of elements of $S(n)$ that are their own inverses.
SOLUTION The following are two characterizations of elements of $S(n)$ that are their own inverses:
(a) Elements of order 1 or 2.

or

(b) The identity permutation and those that can be written as products of disjoint transpositions.