Math 116
Homework 3 Solutions

I graded 4 of the problems: 4, 8, 10, 12.

Each problem is worth 3 points. A grade of 0 indicates no solution or a substantially wrong solution. A grade of 3 indicates a correct or nearly correct solution. Otherwise the grade given is 1 or 2 depending upon how much work was put in and how close the solution is to being correct. How neat and clear your solution is also affects the grade I give.

If you believe a problem was misgraded, or I made some addition or other error, please write a short note explaining the situation, attach it to your homework, and return it to me (either in person, in my mailbox, or under my office door). I'll take a look and return the homework in the next section.

The following are solutions to the homework problems (excepting problems whose solutions are in the back of the text) and additional comments for the problems I graded.

General Comments
The maximum number of points was 12. The high score was 12, the median was 6 and the mean was 5.0. A few people did very well but many people did very poorly. I didn't grade problem 6 but it's important so make sure you understand the solution.

2. We must define our operation $\circ$ so that $x \circ y \in \{0,1\}$ for all $x, y \in \{0,1\}$. The only restriction for a semigroup is that $\circ$ be associative. Now there are $2^4 = 16$ possible "multiplication" tables for $\circ$. In order to save some space let me "encode" (since this is a cryptography class, after all!) each multiplication table as a binary integer from $0 = [0000]_2$ to $15 = [1111]_2$. If $0 \circ 0 = b_0$, $0 \circ 1 = b_1$, $1 \circ 0 = b_2$ and $1 \circ 1 = b_3$, then that defines a multiplication table which we encode as $[b_0 b_1 b_2 b_3]_2$. To save even more space let me write each as just the four bits, so I'll write $[1001]_2$ as simply 1001.

   Now we can check each one to see whether or not it is associative, but to save a little work we note that the cases in which $x \circ y = 0$ always or 1 always must be associative (these are 0000 and 1111), as must be the cases in which we interpret $\circ$ as addition or multiplication mod 2 (these are 0110 and 0001 respectively; as well as addition or multiplication mod 2 where the meanings of 0 and 1 are reversed (since in a semigroup there is no special meaning for these symbols); these are 1001 and 0111 respectively. That takes care of 6 of the 16 cases.

   There are two other operations that turn out to be associative. They are $x \circ y = x$ and $x \circ y = y$, or more specifically 0011 and 0101. You can check easily that these must be associative.

   And it turns out that's it! The other 8 that you can define all violate associativity. Here's an example of failure of associativity for each one:
   $0010 : (1 \circ 1) \circ 1 = 0 \neq 1 = 1 \circ (1 \circ 1)$
   $0100 : (1 \circ 1) \circ 1 = 1 \neq 0 = 1 \circ (1 \circ 1)$
   $1000 : (1 \circ 0) \circ 0 = 1 \neq 0 = 1 \circ (0 \circ 0)$
   $1010 : (0 \circ 0) \circ 0 = 1 \neq 0 = 0 \circ (0 \circ 0)$
   $1011 : (0 \circ 0) \circ 0 = 1 \neq 0 = 0 \circ (0 \circ 0)$
   $1100 : (1 \circ 0) \circ 0 = 1 \neq 0 = 1 \circ (0 \circ 0)$
   $1101 : (0 \circ 0) \circ 0 = 0 \neq 1 = 0 \circ (0 \circ 0)$
   $1110 : (1 \circ 0) \circ 0 = 1 \neq 0 = 1 \circ (0 \circ 0)$.

4. See the solution to problem 2 above for the notation used in this solution. A monoid is a semigroup which has a neutral element, and clearly the operations $x \circ y = x$ and $x \circ y = y$ cannot have a neutral element, nor can the constant operations 0000 and 1111. So that leaves addition and multiplication (0110 and 0001), for which the neutral elements are our familar 0 and 1 respectively, and the versions of addition and multiplication with 0 and 1 reversed in meaning (1001 and 0111), for which the neutral elements are 1 and 0 respectively.

   A group is a monoid in which every element has an inverse; this only happens for addition and the only groups are thus 0110 and 1001.

   Comments: A lot of people had trouble with problem 2, and therefore with this problem also which was the graded problem.

6. Name the map ϕ. We must show three things: that ϕ is well-defined, that it is a ring homomorphism, and that it is surjective. Note that homomorphism is not in the index but that it's defined in Section 2.16 on page 54.

   To show ϕ is well-defined means to show that ϕ does not depend on the representative of the equivalence class. This is similar showing addition and multiplication are well-defined mod m. So let $a \equiv b \pmod{m}$; we want to show $\phi(a + m\mathbb{Z}) \equiv \phi(b + m\mathbb{Z}) \pmod{n}$. We have $\phi(a + m\mathbb{Z}) = a + n\mathbb{Z}$ and $\phi(b + m\mathbb{Z}) = b + n\mathbb{Z}$, so we need to show that $a \equiv b \pmod{n}$, or in other words that $n|(a - b)$. But $m|(a - b)$, and $n|m$, so $n|(a - b)$. Note that it's important that $n|m$ here. Try an example with $n \nmid m$ and see how it fails to be well-defined.

   Next we show ϕ is a ring homomorphism. That is we show $\phi((a + b) + m\mathbb{Z}) \equiv \phi(a + m\mathbb{Z}) + \phi(b + m\mathbb{Z}) \pmod{n}$. By definition we have
   $\phi((a + b) + m\mathbb{Z}) = (a + b) + n\mathbb{Z} \equiv (a + n\mathbb{Z}) + (b + n\mathbb{Z}) \equiv \phi(a + m\mathbb{Z}) + \phi(b + m\mathbb{Z}) \pmod{n}$. Similarly for multiplication we have
   $\phi((a \cdot b) + m\mathbb{Z}) = (a \cdot b) + n\mathbb{Z} \equiv (a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) \equiv \phi(a + m\mathbb{Z}) \cdot \phi(b + m\mathbb{Z}) \pmod{n}$.

   The book doesn't mention this, but for rings with unit element it is typical to require that the unit element of one ring map to the unit element of the other ring under the ring homomorphism. Otherwise you could map everything to 0, say, which is a trivial case you'd like to not allow. Notice that ϕ does indeed map $1 + m\mathbb{Z}$ to $1 + n\mathbb{Z}$.

   Finally we show ϕ is surjective; that is for any $b + n\mathbb{Z}$ there exists some $a + m\mathbb{Z}$ such that $\phi(a + m\mathbb{Z}) = b + n\mathbb{Z}$. Just let $a = b$ and you've found it.

8. Theorem 2.6.2 states that the unit group of $\mathbb{Z}/m\mathbb{Z}$ is the set of all $a + m\mathbb{Z}$ such that $\gcd(a, m) = 1$. Example 2.4.4 shows that the zero divisors of $\mathbb{Z}/m\mathbb{Z}$ are those $a + m\mathbb{Z}$ such that $1 < \gcd(a, m) < m$. It follows the unit group of $\mathbb{Z}/16\mathbb{Z}$ is $\{1, 3, 5, 7, 9, 11, 13, 15\}$, where I've chosen representatives of the equivalence classes for brevity. The zero divisors of $\mathbb{Z}/16\mathbb{Z}$ are $\{2, 4, 6, 8, 10, 12, 14\}$. Notice that an element of $\mathbb{Z}/16\mathbb{Z}$ (and $\mathbb{Z}/m\mathbb{Z}$ in general) is either a unit, a zero-divisor or zero, and each element can only be one of the three.

   Comments: This was just a matter of understanding the definitions, so almost everyone who tried it got it right. I didn't take off any points if you just left out one element of either set.

10. If $122x \equiv 1 \bmod 343$, then there exists some y such that $122x + 343y = 1$. We use the extended Euclidean algorithm. First compute the sequence of remainders:

$$\begin{aligned} 343 &= 122 \cdot 2 + 99 \\ 122 &= 99 \cdot 1 + 23 \\ 99 &= 23 \cdot 4 + 7 \\ 23 &= 7 \cdot 3 + 2 \\ 7 &= 2 \cdot 3 + 1. \end{aligned}$$

   Now back-substitute:

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 \\ &= 7 - (23 - 7 \cdot 3) \cdot 3 \\ &= 7 \cdot 10 - 23 \cdot 3 \\ &= (99 - 23 \cdot 4) \cdot 10 - 23 \cdot 3 \\ &= 99 \cdot 10 - 23 \cdot 43 \\ &= 99 \cdot 10 - (122 - 99) \cdot 43 \\ &= 99 \cdot 53 - 122 \cdot 43 \\ &= (343 - 122 \cdot 2) \cdot 53 - 122 \cdot 43 \\ &= 343 \cdot 53 - 122 \cdot 149 \end{aligned}$$

   It follows $122 \cdot (-149) \equiv 1 \pmod{343}$, and so $-149 \equiv 194 \pmod{343}$ satisfies $122x \equiv 1 \bmod 343$. Note that this means 194 is the multiplicative inverse of 122 mod 343.

12. If $d_1 d_2 \ldots d_k$ is the decimal expansion of d, then $d = \sum_{i=1}^{k} d_i 10^{k-i}$. Let $e = \sum_{i=1}^{k} d_i (-1)^{k-i}$. We will show something stronger than was asked for, namely that $d \equiv e \pmod{11}$. It follows immediately that d is divisible by 11 if and only if e is divisible by 11.

    The simplest way to do this is to note that $10 \equiv (-1) \pmod{11}$, and so we can replace 10 by -1 in any polynomial expression and get the same result mod 11. I believe this was proved in class. Let $f(x) = \sum_{i=1}^{k} d_i x^{k-i}$; this is a polynomial in x. Then $d = f(10)$ and $e = f(-1)$, so it follows $d \equiv e \pmod{11}$.

    Comments: Very few people even attempted this, and even fewer got it right. Almost everyone who got points for this problem used the answer above, but I only gave full credit if you included enough detail to convince me that you really understood what you were doing.