ECE 40400
Luke Canfield

Homework 3

1. $A = \{0,1\}$ boolean and — Must satisfy closure, associativity, identity element, inverse element

Closure: $0 \cap 0 = 0$, $0 \cap 1 = 0$, $1 \cap 0 = 0$, $1 \cap 1 = 1$ all in A so closure holds

Associativity: $(a \cap b) \cap c = a \cap (b \cap c)$ since and is associative so property holds

Identity: identity element is 1 since $a \cap 1 = a$, property holds for any element in A

Inverse: There doesn't exist an inverse element for zero as any value $0 \cap a = 0$ which $\neq i$

so boolean and does not form a group with $A = \{0,1\}$

$A = \{0,1\}$ boolean or

Closure: $0 \cup 1 = 1$, $0 \cup 0 = 0$, $1 \cup 0 = 1$, $1 \cup 1 = 1$ all in A so closure holds

Associativity: $a \cup (b \cup c) = (a \cup b) \cup c$ since or is associative so property holds

Identity: inverse element is 0 since $a \cup 0 = a$, property holds for any element in A

Inverse: there doesn't exist an inverse element for 1 as any value $1 \cup a = 1$ which $\neq i$

so boolean or doesn't form a group with $A = \{0,1\}$

$A = \{0,1\}$ boolean xor

Closure: $0 \oplus 1 = 1$, $0 \oplus 0 = 0$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$ all in A so closure holds

Associativity: $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ since xor is associative so property holds

Identity: identity element is 0 as $a \oplus 0 = a$, property holds for any element in A.

Inverse: there exists an element b, for every a in the set such that $a \oplus b = i$ so property holds

Boolean xor forms a group with $A = \{0,1\}$

2. W: set of all unsigned integers, gcd(·) operator

Closure: $\gcd(a,b)$ for two unsigned integers is ≥ 0 so property holds

Associativity: $\gcd(a, \gcd(b,c)) = \gcd(\gcd(a,b), c)$ since gcd is associative so property holds

Identity: identity element is 0 as $\gcd(a,0) = a$, property holds for any element in W

Inverse: the inverse element of every element a in W is itself such that $\gcd(a,a) = i$

The GCD(·) operator forms a group with W = set of all unsigned integers

3. If we switch the two operators, the ring wouldn't exist anymore. The addition operator would not distribute over the multiplication operator. Meaning $a + (b \cdot c) \neq (a+b) \cdot (a+c)$

Ex. $a=4$ $b=5$ $c=6$ $\quad 4 + (5 \cdot 6) = 34 \quad (4+5) \cdot (4+6) = 90 \quad 34 \neq 90$. Therefore this property doesn't hold meaning it's not a ring.

4. We can use Bezout's Identity to find the multiplicative inverse if we're given a which is relatively prime to n we have $\gcd(a,n) = 1$ which must satisfy $x \cdot a + y \cdot n = 1$ for some x and y. We then find the multiplicative inverse using the Euclid Algorithm to find $\gcd(a,n)$ but at each step we write the expression for the remainder as $a \cdot x + n \cdot y$. Once the remainder becomes 1, x will be the inverse.

ECE 40400
Luke Canfield

Homework 3 Cont.

4. Cont. Multiplicative Inverse of 47 in Z_{97}

$gcd(47,97)$ $a=47$ $n=97$ $x \cdot a + y \cdot n = 1$

$= gcd(97,47)$ | residue $47 = 1 \cdot 47 + 0 \cdot 97$

$= gcd(47,40)$ | residue $40 = -1 \cdot 47 + 1 \cdot 97$

$= gcd(7,1)$ | residue $1 = 3 - 1 \cdot 2$

$= 3 - 1(47 - 15 \cdot 3) = 3 - 47 + 15 \cdot 3 = 3 \cdot 16 - 47$

$= (97 - 47 \cdot 2) \cdot 16 - 1 \cdot 47 = 16 \cdot 97 - 33 \cdot 47$

$x = -33 + 97 = 64$ multiplicative inverse $= 64$

5. a.) $28x \equiv 34 (mod\ 37) \rightarrow 28x (mod\ 37) = 34 (mod\ 37)$ $28x + 37y = 1$

$gcd(28,37) = 1$ $37 = 28 \cdot 1 + 9 \rightarrow 9 = 37 \cdot 1 - 28$ $28 = 9 \cdot 3 + 1 \rightarrow 1 = 28 - 3 \cdot 9$

$1 = 28 - 3 \cdot 9 = 28 - 3 \cdot (37 - 28) = 28 - 3 \cdot 37 + 3 \cdot 28$ $1 = 4 \cdot 28 - 3 \cdot 37$ $MI = 4$

$x \equiv 34 \cdot 4 (mod\ 37) \rightarrow x \equiv 136 (mod\ 37) \rightarrow x \equiv 25 (mod\ 37) \rightarrow \boxed{x = 25}$

b.) $19x \equiv (42 mod\ 43)$ $19x + 43y = 1$

$gcd(19,43) = 1$ $43 = 2 \cdot 19 + 5 \rightarrow 5 = 43 - 2 \cdot 19$ $19 = 3 \cdot 5 + 4 \rightarrow 4 = 19 - 5 \cdot 3$ $5 = 1 \cdot 4 + 1 \rightarrow 1 = 5 - 1 \cdot 4$

$1 = 5 - 1 \cdot (19 - 5 \cdot 3) = 5 - 1 \cdot 19 + 5 \cdot 3 = 4 \cdot 5 - 1 \cdot 19 = 4 \cdot (43 - 2 \cdot 19) - 1 \cdot 19 = 4 \cdot 43 - 9 \cdot 19$

$MI = -9 = 34$ $x \equiv 42 \cdot 34 (mod\ 37) \rightarrow x \equiv 9 (mod\ 37) \rightarrow \boxed{x = 9}$

c.) $54x \equiv 69 (mod\ 79)$ $gcd(54,79) = 1$ $54x + 79y = 1$

$79 = 54 \cdot 1 + 25$ $54 = 25 \cdot 2 + 4$ $25 = 6 \cdot 4 + 1 \rightarrow 1 = 25 - 6 \cdot 4$

$1 = 25 - 6 \cdot (54 - 25 \cdot 2) \rightarrow 1 = 13 \cdot 25 - 6 \cdot 54 \rightarrow 1 = 13 \cdot (79 - 54) - 6 \cdot 54 \rightarrow 1 = 13 \cdot 79 - 19 \cdot 54$ $MI = -19 + 79 = 60$

$x \equiv 69 \cdot 60 (mod\ 79) \rightarrow x \equiv 4140 (mod\ 79) \rightarrow x \equiv 32 (mod\ 79) \rightarrow \boxed{x = 32}$

d.) $153x \equiv 182 (mod\ 271)$ $gcd(153,271) = 1$ $153x + 271y = 1$

$271 = 1 \cdot 153 + 118$ $153 = 118 \cdot 1 + 35$ $118 = 3 \cdot 35 + 13$ $35 = 2 \cdot 13 + 9$ $13 = 1 \cdot 9 + 4$ $9 = 2 \cdot 4 + 1$ $1 = 9 - 2 \cdot 4$

$1 = 9 - 2 \cdot (13 - 1 \cdot 9) \rightarrow 1 = 3 \cdot 9 - 2 \cdot 13 \rightarrow 1 = 3(35 - 2 \cdot 13) - 2 \cdot 13 \rightarrow 1 = 3 \cdot 35 - 8 \cdot 13 \rightarrow 1 = 3 \cdot 35 - 8(118 - 3 \cdot 35) \rightarrow 1 = 27 \cdot 35 - 8 \cdot 118$

$\rightarrow 1 = 27(153 - 118) - 8 \cdot 118 \rightarrow 27(153) - 35 \cdot 118 \rightarrow 1 = 27(153) - 35(271 - 153) \rightarrow 1 = 62(153) - 35(271)$

$MI = 62$ $x \equiv 182(62)(mod\ 271) \rightarrow x \equiv 173 (mod\ 271) \rightarrow \boxed{x = 173}$

e.) $672x \equiv 836 (mod\ 997)$ $gcd(672,997) = 1$ $672x + 997y = 1$

$997 = 672 + 325$ $672 = 325 \cdot 2 + 22$ $325 = 14 \cdot 22 + 17$ $22 = 17 + 5$ $17 = 5 \cdot 3 + 2$ $5 = 2 \cdot 2 + 1$ $1 = 5 - 2 \cdot 2$

$1 = 5 - 2(17 - 5 \cdot 3) \rightarrow 1 = -2(17) + 7(5) \rightarrow 1 = -2(17) + 7(22 - 17) \rightarrow 1 = -9(17) + 7(22) \rightarrow 1 = -9(325 - 14 \cdot 22) + 7(22) \rightarrow$

$1 = 133(22) - 9(325) \rightarrow 1 = 133(672 - 325 \cdot 2) - 9(325) \rightarrow 1 = 133(672) - 275(325) \rightarrow 1 = 133(672) - 275(997 - 672)$

$1 = 408(672) - 275(997)$ $MI = 408$

$x \equiv 836(408)(mod\ 997) \rightarrow x \equiv 114 (mod\ 997)$ $\boxed{x = 114}$

6. $(54x^{10} - 62x^9 - 84x^8 + 70x^7 - 75x^6 + x^5 - 50x^3 + 84x^2 + 65x + 78) + (-67x^9 + 44x^8 - 26x^7 - 37x^6 + 61x^5 + 68x^4 + 22x^3 + 74x^2 + 87x + 38$

$= 54x^{10} - 129x^9 - 40x^8 + 44x^7 - 112x^6 + 62x^5 + 68x^4 - 28x^3 + 158x^2 + 152x + 116$

$= 54x^{10} + 49x^9 - 40x^8 + 44x^7 + 66x^6 + 62x^5 + 68x^4 + 61x^3 + 69x^2 + 63x + 27$ (mod 89)

ECE 40400
Luke Canfield

Homework 3 Cont.

7. $(8x^3+6x^2+8x+1)\cdot(3x^3+9x^2+7x+5)$ in $GF(11)$

$24x^6+72x^5+56x^4+40x^3+18x^5+54x^4+42x^3+30x^2+24x^4+72x^3+56x^2+40x+3x^3+9x^2+7x+5$

$= 24x^6+90x^5+134x^4+157x^3+95x^2+47x+5$

$= 2x^6+2x^5+2x^4+3x^3+7x^2+3x+5 \pmod{11}$

8. $GF(2^3)$ $\bmod(x^3+x+1)$

a.) $(x^2+x+1)\cdot(x^2+x) = (x^4+x^3+x^2)+(x^3+x^2+x) = (x^4+x)\bmod(x^3+x+1)$ $\quad x^2+x+1$

$$\begin{array}{r l}
 & x \\
x^3+x+1 & \overline{\big)\, x^4+x} \\
- & x^4+x^2+x \\
\hline
 & -x^2
\end{array}
\qquad = x - \frac{x^2}{x^3+x+1} \pmod{x^3+x+1}$$

b.) $x^2-(x^2+x+1) = -x-1 = x+1$ $\quad x^3+x+1\,\overline{\big)\,x+1}$ $\quad = x+1 \pmod{x^3+x+1}$

c.) $\dfrac{x^2+x+1}{x^2+1}$

$$\begin{array}{r l}
 & 1 \\
x^2+1 & \overline{\big)\, x^2+x+1} \\
- & x^2+1 \\
\hline
 & x
\end{array}
\qquad = 1+\frac{x}{x^2+1} \qquad 1+\frac{x}{x^2+1} \pmod{x^3+x+1}$$