HW 3

Andrew Wu

Saturday, January 27, 2024 2:26 PM

1. Groups must have

Boolean	And	OR	XOR
Closure	✓	✓	✓
Associativity	✓	✓	✓
Identity Element	✓	✓	✓
Inverse Element	X	X	✓

Set A doesn't have an element where $a \wedge b = 1$ or $a \vee b = 0$, ∴ AND & OR aren't groups

2. Set of all unsigned integers = $\{0, 1, \ldots, \infty\}$

gcd(·) operator

Closure: gcd of two unsigned ints is an unsigned int. ✓

Associativity: $gcd(a, gcd(b,c)) = gcd(gcd(a,b),c)$ ✓

Identity: $gcd(a, 0) = a$ ✓

Inverse: $gcd(a, 1) = 1$ ✓

∴ W is a group under the gcd(·) operator

3. Group operator ⟷ ring operator

Multiplication	Closure:	Still holds true since it was originally valid ✓
"	Associativity:	Multiplication is Associative ✓
"	identity element:	original ring had multiplicative identity ✓
"	inverse element:	May not have multiplicative inverse X
Addition	closure:	Still holds from original ring ✓
"	Associativity:	Should still hold from original ring ✓
"	Distributive property:	Still holds from original ring ✓

uncertainty of a multiplication inverse element

" Distributive property"

Due to the uncertainty of a multiplication inverse element being present, the group will no longer be a ring

4. You can use Bezout's Identity to find the multiplicative inverse of an integer in Z_p. You first make sure that the $\gcd(a,p)=1$, then use Bezout's Identity of $x \cdot a + y \cdot n = \gcd(a,n)$, with x equaling the multiplicative inverse

47 in Z_{97}

$\gcd(47,97) = \gcd(97,47)$
$= \gcd(47,50)$
$= \gcd(50,47)$
$= \gcd(47,3)$
$= \gcd(3,2)$
$= \gcd(2,1)$

reside 50 $= 1 \cdot 97 - 1 \cdot 47$
reside 47 $= 1 \cdot 47 + 0 \cdot 97$
reside 3 $= 1 \cdot 50 - 1 \cdot 47$
$= 1 \cdot 97 - 2 \cdot 47$
reside 2 $= 1 \cdot 47 - 15 \cdot 3$
$= 1 \cdot 47 - 15 \cdot 97 + 30 \cdot 47$
reside 1 $= 1 \cdot 3 - 1 \cdot 2$
$= 1 \cdot 97 - 2 \cdot 47 - (1 \cdot 47 - 15 \cdot 97 + 30 \cdot 47)$
$= 16 \cdot 97 - 33 \cdot 47$
x

-33 in mod $97 = 64$

64 is the multiplicative inverse of 47 in Z_{97}

5. a) $28x \equiv 34 \pmod{37}$

$\gcd(37,28) = 1$

$37 = 28 \cdot 1 + 9$
$28 = 9 \cdot 3 + 1$
$9 = 1 \cdot 9 + 0$

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

$28 \cdot 4 \; x \equiv 34 \cdot 4 \pmod{37}$

$28 \cdot 4 \quad x \equiv 34 \cdot 4 \pmod{37}$

$x \equiv 136 \pmod{37} = \boxed{25}$

b) $19x \equiv 42 \pmod{43}$

$\gcd(43, 19) = 1$

$43 = 19 \cdot 2 + 5$

$19 = 5 \cdot 3 + 4$

$5 = 4 \cdot 1 + 1$

$4 = 1 \cdot 4 + 0$

$1 = 5 - 4 \cdot 1$

$= 5 - (19 - 5 \cdot 3) \cdot 1$

$= 5 \cdot 4 - 19$

$= (43 - 19 \cdot 2)4 - 19$

$= 43 \cdot 4 - 19 \cdot 9$

$19 \cdot -9 \quad x \equiv 42 \cdot -9 \pmod{43}$

$x \equiv -378 \pmod{43} = \boxed{9}$

c) $54x \equiv 69 \pmod{79}$

$\gcd(79, 54) = 1$

$79 = 54 \cdot 1 + 25$

$54 = 25 \cdot 2 + 4$

$25 = 4 \cdot 6 + 1$

$4 = 1 \cdot 4 + 0$

$1 = 25 - 4 \cdot 6$

$= 25 - (54 - 25 \cdot 2) \cdot 6$

$= 25 \cdot 13 - 54 \cdot 6$

$= 79 \cdot 13 - 54 \cdot 19$

$54 \cdot -19 \quad x \equiv 69 \cdot -19 \pmod{79}$

$x \equiv -1311 \pmod{79} = \boxed{32}$

d) $153x \equiv 182 \pmod{271}$

$\gcd(271, 153) = 1$

$271 = 153 \cdot 1 + 118$

$153 = 118 \cdot 1 + 35$

$118 = 35 \cdot 3 + 13$

$35 = 13 \cdot 2 + 9$

$13 = 9 \cdot 1 + 4$

$9 = 4 \cdot 2 + 1$

$4 = 1 \cdot 4 + 0$

$1 = 9 - 4 \cdot 2$

$= 9 - (13 - 9) \cdot 2$

$= 9 \cdot 3 - 13 \cdot 2$

$= (35 - 13 \cdot 2) \cdot 3 - 13 \cdot 2$

$= 35 \cdot 3 - 13 \cdot 8$

$= 35 \cdot 3 - 118 \cdot 8 + 35 \cdot 24$

$= (153 - 118) \cdot 27 - 118 \cdot 8$

$= 153 \cdot 27 - (271 - 153) \cdot 35$

$= 153 \cdot 62 - 271 \cdot 35$

$153 \cdot 62 \quad x \equiv 182 \cdot 62 \pmod{271}$

$x \equiv 11284 \pmod{271} = 173$

$153 \cdot 62 \quad x \equiv 182 \cdot 62 \pmod{271}$

$x \equiv 11284 \pmod{271} = \boxed{173}$

e) $672x \equiv 836 \pmod{997}$

$\gcd(997, 672) = 1$

$997 = 672 \cdot 1 + 325$

$672 = 325 \cdot 2 + 22$

$325 = 22 \cdot 14 + 17$

$22 = 17 \cdot 1 + 5$

$17 = 5 \cdot 3 + 2$

$5 = 2 \cdot 2 + 1$

$2 = 1 \cdot 2 + 0$

$1 = 5 - 2 \cdot 2$

$= 5 - (17 - 5 \cdot 3) \cdot 2$

$= 5 \cdot 7 - 17 \cdot 2$

$= (22 - 17) \cdot 7 - 17 \cdot 2$

$= 22 \cdot 7 - 17 \cdot 9$

$= 22 \cdot 7 - (325 - 22 \cdot 14) \cdot 9$

$= 22 \cdot 133 - 325 \cdot 9$

$= (672 - 325 \cdot 2) \cdot 133 - 325 \cdot 9$

$= 672 \cdot 133 - 325 \cdot 275$

$= 672 \cdot 133 - (997 - 672) \cdot 275$

$= 672 \cdot 408 - 997 \cdot 275$

$672 \cdot 408 \, x \equiv 836 \cdot 408 \pmod{997}$

$x \equiv 341088 \pmod{997} = \boxed{114}$

6. $(54x^{10} - 62x^9 - 84x^8 + 70x^7 - 75x^6 + x^5 - 50x^3 + 84x^2 + 65x + 78)$

$+ (-67x^9 + 44x^8 - 26x^7 - 32x^6 + 61x^5 + 68x^4 + 22x^3 + 74x^2 + 87x + 38)$ GF(89)

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

$= \boxed{54x^{10} + 49x^9 + 49x^8 + 44x^7 + 66x^6 + 62x^5 + 68x^4 + 61x^3 + 69x^2 + 63x + 27}$

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

$24x^6 + 18x^5 + 24x^4 + 3x^3 + 72x^5 + 54x^4 + 72x^3 + 9x^2$

$+ 56x^4 + 42x^3 + 56x^2 + 7x + 40x^3 + 30x^2 + 40x + 5$

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

8. $GF(2^3) \quad \text{mod } (x^3 + x + 1)$

a) $(x^2+x+1)\times(x^2+x)$

$x^4 + x^3+x^2 + x^3+x^2+x$

x^4+x

$x + \frac{x^2}{x^3+x+1}$

$x^3+x+1 \overline{)\,x^4+x}$ $\quad x$

x^4+x^2+x

$-x^2$

b) ~~x^2~~ $-(x^2+x+1)$

$-x-1 \longrightarrow \boxed{x+1}$

c) $\frac{x^2+x+1}{x^2+1}$

$1 + \frac{x}{x^2+1}$

$x^2+1 \overline{)\,x^2+x+1}$ $\quad 1$

x^2+1

x