# Math 223
# Assignment 2 Episode 2: The Algebraic Systems, Groups, Rings, and Fields Strikes Back

Quinn Neumiiller

October 6, 2013

**Question 1.** Divisibility Rules. Suppose that $a \in \mathbb{N}$ is written as $a = a_n a_{n-1} ... a_1 a_0$ in base 10 notation, where each $a_i$ is a digit among the numbers 0 to 9.

**Question 1a.** Prove that $a \equiv (\sum_{i=0}^{n} a_i) \bmod 9$.

*Proof.* Each $a_i$ can be represented as $a_i * 10^i$

We know that $9 \equiv 10 - 1$ and that $10^i \equiv 1 \bmod 9$

Therefore,

$a_i * 10^i \equiv a_i$

$a_n * 10^n + a_{n-1} * 10^{n-1} + ... + a_1 * 10^1 + a_0 * 10^0$

$\equiv a_n + a_{n-1} + ... + a_1 + a_0 \bmod 9$

$\equiv (\sum_{i=0}^{n} a_i) \bmod 9$

□

**Question 1b.** Prove that $a \equiv (\sum_{i=0}^{n} a_i) \bmod 3$.

*Proof.* Each $a_i$ can be represented as $a_i * 10^i$

We know that $9 \equiv 10 - 1$, $3 \equiv 9$ and that $10^i \equiv 1 \bmod 3$

Therefore,

$a_i * 10^i \equiv a_i$

$a_n * 10^n + a_{n-1} * 10^{n-1} + ... + a_1 * 10^1 + a_0 * 10^0$

$\equiv a_n + a_{n-1} + ... + a_1 + a_0 \bmod 3$

$\equiv (\sum_{i=0}^{n} a_i) \bmod 3$

□

**Question 1c.** Prove that $a \equiv a_0 \bmod 5$.

*Proof.* Each $a_i$ can be represented as $a_i * 10^i$

We know that $5 \equiv 10$ and that $10^i \equiv 0 \bmod 5$

Therefore,

$a_i * 10^i \equiv a_i$

$a_n * 10^n + a_{n-1} * 10^{n-1} + ... + a_1 * 10^1 + a_0 * 10^0$

$\equiv a_n * 0 + a_{n-1} * 0 + ... + a_1 * 0 + a_0 * 1$

$\equiv 0 + 0 + ... + 0 + a_0 \bmod 5$

$\equiv a_0 \bmod 5$

□

**Question 1d.** Prove that $a \equiv (\sum_{i=0}^{n} (-1)^i a_i) \bmod 11$.

*Proof.* Each $a_i$ can be represented as $a_i * 10^i$

We know that $10^k \equiv -1^k \bmod 11$

Therefore,

$a_n * 10^n + a_{n-1} * 10^{n-1} + ... + a_1 * 10^1 + a_0 * 10^0$

$\equiv a_n * -1^n + a_{n-1} * -1^{n-1} + ... + a_1 * -1^1 + a_0 * -1^0$

$\equiv (\sum_{i=0}^{n} (-1)^i a_i) \bmod 11$.

□

**Question 1e.** Prove that modulo 7, $a \equiv (a_0 + 3a_1 + 2a_2) - (a_3 + 3a_4 + 2a_5) + (a_6 + 3a_7 + 2a_8) - (a_9 + 3a_{10} + 2a_{11})$+...

*Proof.* $10^0 \equiv 3^0 \bmod 7 \equiv 1 \bmod 7$
$10^1 \equiv 3^1 \bmod 7 \equiv 3 \bmod 7$
$10^2 \equiv 3^2 \bmod 7 \equiv 2 \bmod 7$

$10^3 \equiv 3^3 \bmod 7 \equiv -1 \bmod 7$
$10^4 \equiv 3^4 \bmod 7 \equiv -3 \bmod 7$
$10^5 \equiv 3^5 \bmod 7 \equiv -2 \bmod 7$

$10^6 = 10^{\phi(7)} \equiv 1 \bmod 7$
$10^7 = 10^{6+1} = 10^6 * 10^1 = 10^{\phi(7)} * 10^1 \equiv 1 * 10 \equiv 3 \bmod 7$
$10^8 = 10^{6+2} = 10^6 * 10^2 = 10^{\phi(7)} * 10^2 \equiv 1 * 100 \equiv 2 \bmod 7$

We can see that a pattern forms for any power of 10, $k$, where $k > 6$, such that $10^k \equiv 10^{k \bmod \phi(7)}$ □

**Question 2.** Find all solutions, if any, for the following euqations in $\mathbb{Z}_n$

**Question 2a.** $2x = 5 \bmod 15$

1. Determine gcd(a,z)

gcd(2,15)

$$\begin{aligned} 15 =& 2(7) + 1 \\ =& 1 \end{aligned}$$

2. Back substitute

$$1 = 15 - 2(7)$$

3. Finding inverse

$$1 = 15 + 2(-7)$$

Inverse is -7
4. Solving for x

$$\begin{aligned} 2x(-7) &= 5(-7) \text{ in } \mathbb{Z}_{15} \\ (-14)x &= -35 \text{ in } \mathbb{Z}_{15} \\ x &= -35 \text{ in } \mathbb{Z}_{15} \\ x &= -35 \text{ in } \mathbb{Z}_{15} \\ x &= 10 \text{ in } \mathbb{Z}_{15} \end{aligned}$$

**Question 2b.** $23x = 1$ in $\mathbb{Z}_{41}$
1. Determine gcd(a,z)
gcd(23,41)

$$\begin{aligned} 41 =& 23(1) + 18 \\ 23 =& 18(1) + 5 \\ 18 =& 5(3) + 3 \\ 5 =& 3(1) + 2 \\ 3 =& 2(1) + 1 \\ =& 1 \end{aligned}$$

There is one unique solution for x.
2. Back substitute

$$\begin{aligned}1 =& 3 - 2(1)\\ =& 3 - (5 - 3) = 3(2) - 5\\ =& (18 - 5(3))(2) - 5 = 18(2) - 5(7)\\ =& 18(2) - (23 - 18)(7) = 18(9) - 23(7)\\ =& (41 - 23)(9) - 23(7) = 41(9) - 23(16)\\ =& 41(9) - 23(16)\end{aligned}$$

3. Finding inverse

$$1 = 41(9) + 23x(-16)$$

Inverse is -16

4. Solving for x

$$\begin{aligned}23x(-16) =& 1(-16) \text{ in } \mathbb{Z}_{41}\\ 1x =& -16 \text{ in } \mathbb{Z}_{41}\\ x =& -16 \text{ in } \mathbb{Z}_{41}\end{aligned}$$

**Question 2c.** $1426x = 597$ in $\mathbb{Z}_{2000}$

1. Determine gcd(a,z)

gcd(1426,2000)

$$\begin{aligned}2000 =& 1426(1) + 574\\ 1426 =& 574(2) + 278\\ 574 =& 278(2) + 18\\ 278 =& 18(15) + 8\\ 18 =& 8(2) + 2\\ 8 =& 2(4) + 0\end{aligned}$$

gcd(1426,2000) = 2

Is 597|2? No. There is no solution.

**Question 2d.** $1731x = 871$ in $\mathbb{Z}_{2000}$

1. Determine gcd(a,z)

gcd(1731,2000)

$$\begin{aligned}2000 =& 1731(1) + 269\\1731 =& 269(6) + 117\\269 =& 117(2) + 35\\117 =& 35(3) + 12\\35 =& 12(2) + 11\\12 =& 11(1) + 1\end{aligned}$$

gcd(1731,2000) = 1
2. Back substitute

$$\begin{aligned}1 =& 12 - 11\\1 =& 12(3) - 35\\1 =& 117(3) - 35(10)\\1 =& 117(23) - 269(10)\\1 =& 1731(23) - 269(148)\\1 =& 1731(171) - 2000(148)\end{aligned}$$

3. Finding inverse

$$1 = 1731x(171) + 2000(148)$$

Inverse is 171.
4. Solving for x

$$\begin{aligned}1731x(171) =& 871(171) \text{ in } \mathbb{Z}_{2000}\\1731x(171) =& 1(171) \text{ in } \mathbb{Z}_{2000}\\296001x =& 148941 \text{ in } \mathbb{Z}_{2000}\\x =& 941 \text{ in } \mathbb{Z}_{2000}\end{aligned}$$

**Question 2e.** The system $\begin{matrix}8x + 3y = 9\\6x + 5y = 2\end{matrix}$ in $\mathbb{Z}_{12}$.

1. Determine gcd(a,z)
det = $10x \equiv 1$ mod 12 gcd(10, 12) = 2
There is no solution because $2 \nmid 1$

**Question 2f.** $x^4 + 3x^2 + 10 = 0$ in $\mathbb{Z}_{11}$

| | $x^4 + 3x^2 + 10 = 0$ in $\mathbb{Z}_{11}$ |
|---|---|
| 0 | 16 |
| 1 | 16 |
| 2 | 20 |
| 3 | 28 |
| 4 | 24 |
| 5 | 24 |
| 6 | 28 |
| 7 | 36 |
| 8 | 48 |
| 9 | 48 |

No solution.

**Question 2g.** $x^2 \equiv 17$ in $\mathbb{Z}_{24}$

| | $x^2 \equiv 17$ in $\mathbb{Z}_{24}$ |
|---|---|
| 0 | 0 |
| 1 | 1 |
| 2 | 4 |
| 3 | 9 |
| 4 | 16 |
| 5 | $25 \equiv 1$ |
| 6 | $36 \equiv 12$ |
| 7 | $49 \equiv 1$ |
| 8 | $64 \equiv 16$ |
| 9 | $81 \equiv 9$ |
| 10 | $100 \equiv 4$ |
| 11 | $121 \equiv 1$ |
| 12 | $144 \equiv 0$ |
| 13 | $169 \equiv 1$ |
| 14 | $196 \equiv 4$ |
| 15 | $225 \equiv 9$ |
| 16 | $256 \equiv 16$ |
| 17 | $289 \equiv 1$ |
| 18 | $324 \equiv 12$ |
| 19 | $361 \equiv 1$ |
| 20 | $400 \equiv 16$ |
| 21 | $441 \equiv 9$ |
| 22 | $484 \equiv 4$ |
| 23 | $529 \equiv 1$ |

**Question 3.** Find all solutions for $x$, up to congruence. If there is more than one equation, then find all simultaneous solutions up to congruence.

**Question 3a.** $x \equiv 1 \bmod 4$ and $x \equiv 7 \bmod 13$.

1. Setting equations to equal each other

$$
\begin{aligned}
x =& 4k + 1 = 13l + 7 \\
=& 4k - 13l = 6
\end{aligned}
$$

2. EA

$$
\begin{aligned}
13 =& 4(3) + 1 \\
4 =& 1(4) + 0
\end{aligned}
$$

3. Back substitution

$$
\begin{aligned}
1 =& 13 - 4(3) \\
1 =& (-1) - 13 + 4(-3) \\
(6)1 =& 6(4(-3) - 13(-1)) \\
6 =& 4(-18) - 13(-6)
\end{aligned}
$$

4. Verification.

$$
\begin{aligned}
4(-18) + 1 =& -72 + 1 \\
=& -71
\end{aligned}
$$

$$
\begin{aligned}
13(-6) + 7 =& -78 + 7 \\
=& -71
\end{aligned}
$$

**Question 3b.** $x \equiv 11 \mod 142$ and $x \equiv 25 \mod 86$.

1. Setting equations to equal each other

$$
\begin{aligned}
x =& 142k + 11 = 86l + 25 \\
=& 142k - 86l = 14
\end{aligned}
$$

2. EA

$$
\begin{aligned}
142 &= 86(1) + 56 \\
86 &= 56(1) + 30 \\
56 &= 30(1) + 26 \\
30 &= 26(1) + 4 \\
26 &= 4(6) + 2 \\
4 &= 2(2) + 0
\end{aligned}
$$

3. Back substitution

$$
\begin{aligned}
2 =& 26 - 4(6) \\
2 =& 26 - (30 - 26)(6) \\
2 =& 26(7) - 30(6) \\
2 =& (56 - 30)(7) - 30(6) \\
2 =& 56(7) - 30(7) - 30(6) \\
2 =& 56(7) - 30(13) \\
2 =& 56(7) - (86 - 56)(13) \\
2 =& 56(7) - 86(13) + 56(13) \\
2 =& 56(20) - 86(13) \\
2 =& (142 - 86)(20) - 86(13) \\
2 =& 142(20) - 86(20) - 86(13) \\
2 =& 142(20) - 86(33) \\
7(2) =& 7(142(20) - 86(33)) \\
14 =& 142(140) - 86(231)
\end{aligned}
$$

4. Verification

$$
\begin{aligned}
142k + 11 =& 142(140) + 11 \\
=& 19880 + 11 \\
=& 19891
\end{aligned}
$$

$$
\begin{aligned}
86l + 25 =& 86(231) + 25 \\
=& 19891
\end{aligned}
$$

**Question 3c.** $x \equiv 2^{63} \bmod 61$.
gcd(2, 61) = 1
$\phi(61) = 60$ Due to 61 being prime.

$$\begin{aligned} 2^6 3 =& 2^{(60+3)} \\ =& 2^{60} * 2^3 \\ =& 1 * 8 \\ =& 8 \end{aligned}$$

**Question 3d.** $x \equiv 7^{78} \bmod 79$.
gcd(7, 78) = 1
$\phi(79) = 78$ Due to 79 being prime.

$$7^7 8 = 1$$

**Question 3e.** $x^2 + 3x \equiv 3 \bmod 8$.

| | $x^2 + 3x \equiv 3$ in $\mathbb{Z}_8$ |
|---|---|
| 0 | 0 |
| 1 | 4 |
| 2 | $10 \equiv 2$ |
| 3 | $18 \equiv 2$ |
| 4 | $28 \equiv 4$ |
| 5 | $40 \equiv 0$ |
| 6 | $54 \equiv 6$ |
| 7 | $70 \equiv 6$ |

No solution.

**Question 4.** Suppose $p$ is a positive prime integer. Prove that $\forall x, y \in \mathbb{Z}, (x+y)^p \equiv x^p + y^p \bmod p$

*Proof.* Since p is a positive prime integer and we know $\phi(p) \equiv 1$, $\phi(p) = p - 1$.

$$\begin{aligned} (x+y)^p \bmod p \equiv& (x+y)^{(p-1+1)} \bmod p \\ \equiv& (x+y)(x+y)^{(p-1)} \\ \equiv& (x+y)(1) \\ \equiv& x + y \\ \equiv& x(1) + y(1) \\ \equiv& x(x^{\phi(p)}) + y(y^{\phi(p)}) \\ \equiv& x(x^{p-1}) + y(y^{p-1}) \\ \equiv& x^p + y^p \end{aligned}$$

□

**Question 5.** Let $\varphi : \mathbb{Z}+ \to \mathbb{Z}^+$ be the Euler-phi function

**Question 5a.**

$$\begin{aligned}\phi(p^4q^2) =& \phi(p^4)\phi(q^2) \\ =& (p^{4-1}(p-1))(q^{2-1}(q-1)) \\ =& (p^3(p-1))(q(q-1))\end{aligned}$$

**Question 5b.**

$$\begin{aligned}\phi(343000) =& \phi(343)\phi(1000) \\ =& \phi(7^3)\phi(2^3)\phi(5^3) \\ =& 7^2(7-1))(2^2(2-1))(5^2(5-1) \\ =& 7^2(6)) * (2^2) * (5^2(4) \\ =& 49(6)) * 4 * (25(4) \\ =& 294 * 4 * 100 \\ =& 117,600\end{aligned}$$

**Question 5c.**

$$\begin{aligned}\phi(n) =& n^{1-1}(n-1) \\ =& n^0(n-1) \\ =& (n-1)\end{aligned}$$

$\phi(101) = 100$

**Question 5d.**

$$\begin{aligned}\phi(2m) =& \phi(2)\phi(m) \\ =& 2^{1-1}(2-1)\phi(m) \\ =& (2-1)\phi(m) \\ =& 1\phi(m) \\ =& \phi(m)\end{aligned}$$

**Question 6a.** Give the multiplication table for the group $U_{12}$.

1. Find the number of units

$$\begin{aligned}\phi(12) =& \phi(2^2) * \phi(3) \\ =& 2 * 2 \\ =& 2 * 2\end{aligned}$$

2. Find the 4 units

| | gcd(x, 12) |
|---|---|
| 0 | gcd(0, 12) $= 12 \equiv 0$ |
| 1 | gcd(1, 12) $= 1$ |
| 2 | gcd(2, 12) $= 2$ |
| 3 | gcd(3, 12) $= 3$ |
| 4 | gcd(4, 12) $= 4$ |
| 5 | gcd(5, 12) $= 1$ |
| 6 | gcd(6, 12) $= 6$ |
| 7 | gcd(7, 12) $= 1$ |
| 8 | gcd(8, 12) $= 4$ |
| 9 | gcd(9, 12) $= 3$ |
| 10 | gcd(10, 12) $= 2$ |
| 11 | gcd(11, 12) $= 1$ |

$U_{12} = \{1, 5, 7, 11\}$

| | 1 | 5 | 7 | 11 |
|---|---|---|---|---|
| 1 | 1 | 5 | 7 | 11 |
| 5 | 5 | $25 \equiv 1$ | $35 \equiv 11$ | $55 \equiv 7$ |
| 7 | 7 | $35 \equiv 11$ | $49 \equiv 1$ | $77 \equiv 5$ |
| 11 | 11 | $55 \equiv 7$ | $77 \equiv 5$ | $121 \equiv 1$ |

**Question 6b.** Compute the inverse of 43 in $U_{63}$

1. Find the number of units

$$\begin{aligned}\phi(63) =& \phi(3^2) * \phi(7)\\ =& 3(2) * 6\\ =& 6 * 6\\ =& 36\end{aligned}$$

gcd(43,63) = 1

$$\begin{aligned}63 =& 43(1) + 20\\ 43 =& 20(2) + 3\\ 20 =& 3(6) + 2\\ 3 =& 2(1) + 1\end{aligned}$$

$$
\begin{aligned}
1 =& 3 - 2 \\
1 =& 3 - (20 - 3(6)) \\
1 =& 3 - 20 + 3(6) \\
1 =& 3(7) - 20 \\
1 =& (43 - 20(2))(7) - 20 \\
1 =& 43(7) - 20(15) \\
1 =& 43(7) - (63 - 43)(15) \\
1 =& 43(7) - 63(15) + 43(15) \\
1 =& 43(22) - 63(15)
\end{aligned}
$$

Inverse is 22.