Modular Arithmetic Examples

19CSE311 Computer Security
Jevitha KP
Department of CSE

GCD(12343642, 2343)

a	b	q	r
12343642	2343	5268	718
2343	718	3	189
718	189	3	151
189	151	1	38
151	38	3	37
38	37	1	1
37	1	37	0

Addition Modulo 11 Example

- Z11 = { 0,1,2,3,4,5,6,7,8,9,10}

0	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
0	0	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10	0
2	2	3	4	5	6	7	8	9	10	0	1
3	3	4	5	6	7	8	9	10	0	1	2
4	4	5	6	7	8	9	10	0	1	2	3
5	5	6	7	8	9	10	0	1	2	3	4
6	6	7	8	9	10	0	1	2	3	4	5
7	7	8	9	10	0	1	2	3	4	5	6
8	8	9	10	0	1	2	3	4	5	6	7
9	9	10	0	1	2	3	4	5	6	7	8
10	10	0	1	2	3	4	5	6	7	8	9

Multiplication Modulo 11 Example

- Z11 = { 0,1,2,3,4,5,6,7,8,9,10}

0	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Additive Inverse Z11

- Z11 = { 0,1,2,3,4,5,6,7,8,9,10}
- Additive Inverse mod 11= {0,10,9,8,7,6,5,4,3,2,1 }

Multiplicative Inverse Z11

- Z11 = { 1,2,3,4,5,6,7,8,9,10}
- Multiplicative Inverse mod 11= {1,6,4,3,9,2,8,7,5,10 }

Modular Arithmetic

- Perform the following operations (the inputs come from Zn):
  - a. Add 7 to 14 in Z15.
  - b. Subtract 11 from 7 in Z13.
  - c. Multiply 11 by 7 in Z20.
- Perform the following operations (the inputs come from either Z or Zn):
  - a. Add 17 to 27 in Z14.
  - b. Subtract 43 from 12 in Z13.
  - c. Multiply 123 by −10 in Z19.

Modular Arithmetic

» a. Add 7 to 14 in Z15.

= 7+14

= 21 mod 15

= 6 mod 15

Modular Arithmetic

» b. Subtract 11 from 7 in Z13.

= 7-11 mod 13

= -4 mod 13

= (-4+13) mod 13

= 9 mod 13

Modular Arithmetic

» c. Multiply 11 by 7 in Z20.

= 7 * 11 mod 20

= 77 mod 20

= 17 mod 20

Modular Arithmetic

» Perform the following operations (the inputs come from either Z or Zn):

» a. Add 17 to 27 in Z14.

1st approach

= 17 mod 14 + 27 mod 14

= 3 mod 14 + 13 mod 14

= 16 mod 14 = 2 mod 14.

2nd approach

= 17+27 mod 14

= 44 mod 14 = 2 mod 14

Modular Arithmetic

» b. Subtract 43 from 12 in Z13. - 8

= 12 - 43 mod 13

= -31 mod 13

= -31+13 mod 13 = -18 mod 13

= -18 + 13 mod 13 = -5 mod 13

= -5 +13 mod 13

= 8 mod 13

Modular Arithmetic

» c. Multiply 123 by −10 in Z19.

= 123 * -10 mod 19

= -1230 mod 19

= -14 mod 19

= -14 + 19 mod 19

= 5 mod 19