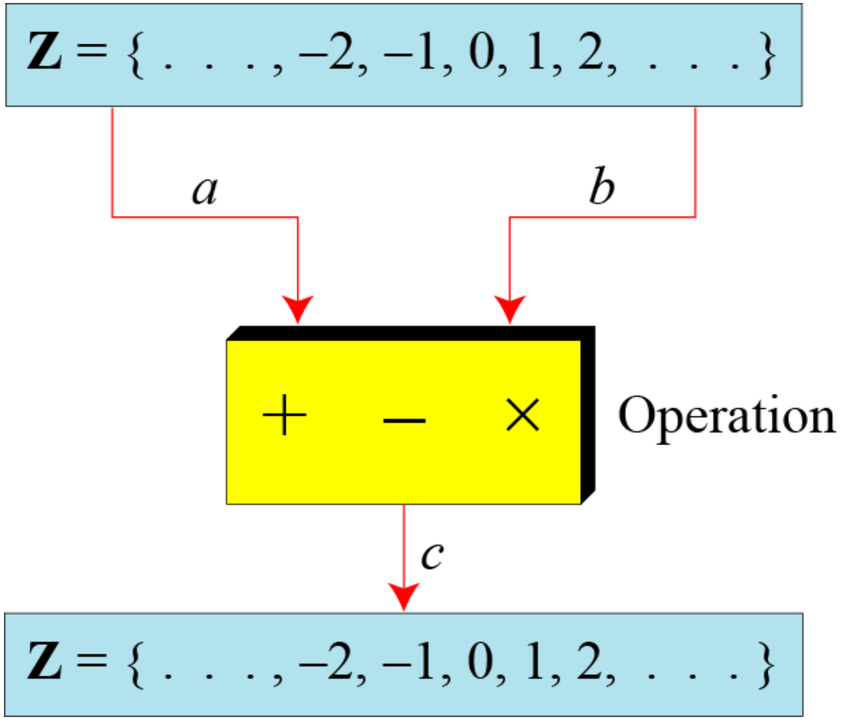
Network Security
Mathematics of Crypto

Amir Rezapour
Institute of Information Security,
National Tsing Hua University

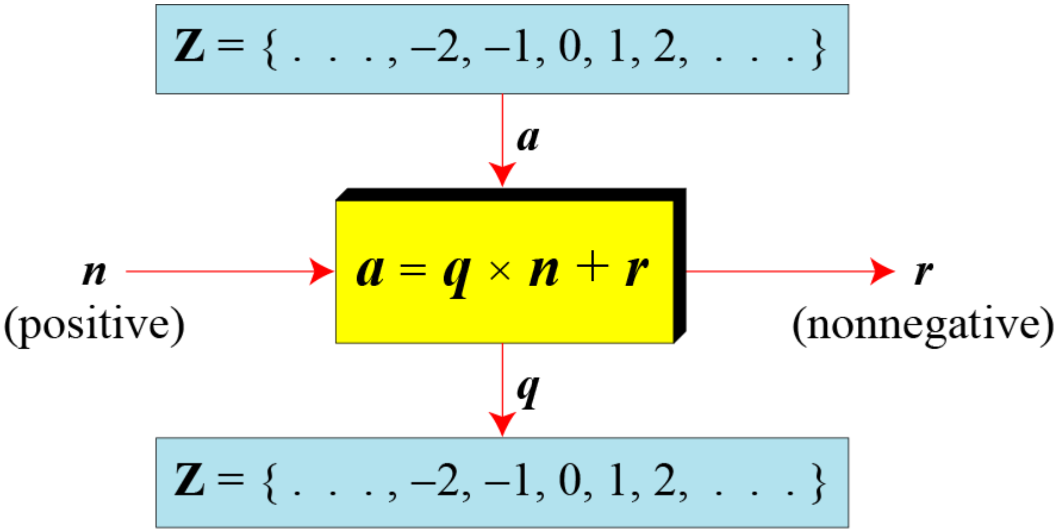
Set of Integers

- The set of integers, denoted by Z, contains all integral numbers.
- $+, -, \times$ applies to Z



Integer Division

- In integer arithmetic, if we divide a by n, we can get q and r.
- $-255 = (-\mathbf{23} \times 11) + (-2) \leftrightarrow -255 = (-\mathbf{24} \times 11) + 9$



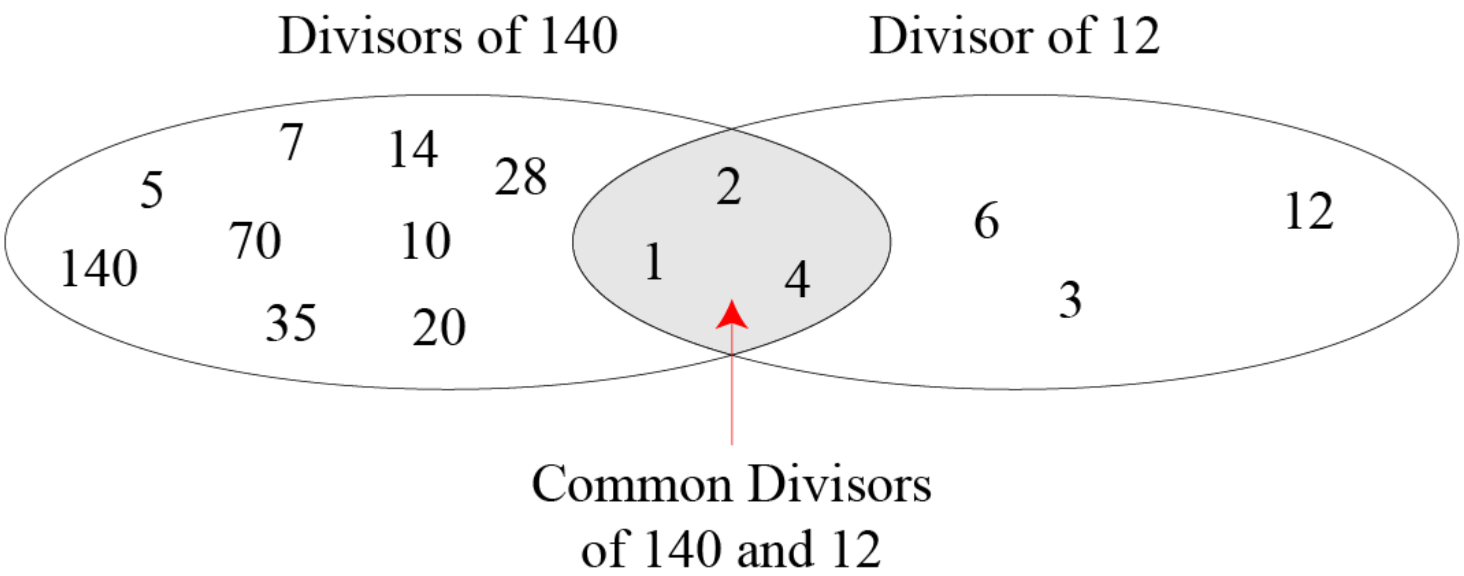
Divisibility

- If a is not zero and in the division relation, $a = q \times n + r$
  - If the remainder is zero, $n|a$
    - $32 = 8 \times 4$, $8|32$
  - If the remainder is *not* zero, $n \nmid a$
    - $42 = 5 \times 8 + 2$, $8 \nmid 42$

- *Fact 1*: The integer 1 has only one divisor, itself.
- *Fact 2*: Any positive integer has at least two divisors, 1 and itself (but it can have more).

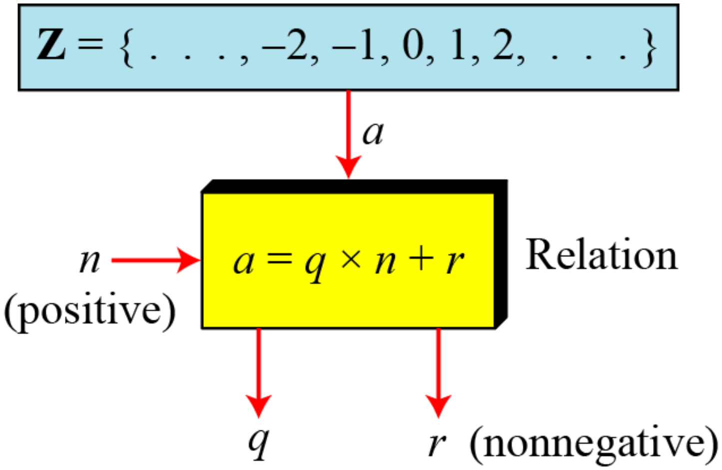
Common divisors of two integers

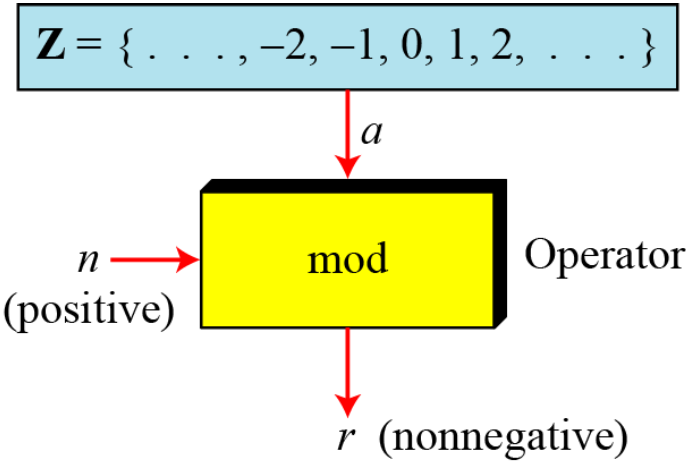
- The greatest common divisor of two positive integers $\gcd(a, b)$ is the largest integer that can divide both integers.



Modulo Operator

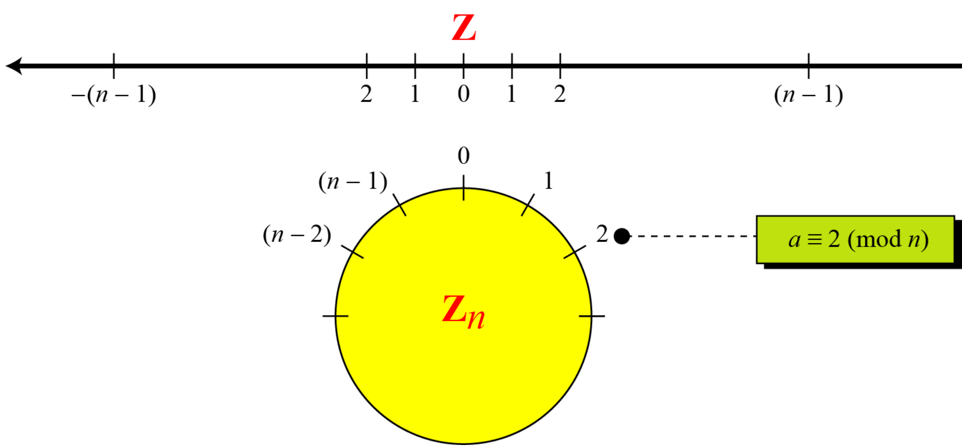
- The modulo operator is shown as **mod (n)**. The second input (n) is called the modulus. The output r is called the residue.
  - $27 = 2\ mod\ 5$, $-18 = 10\ mod\ 14$





Set of Residues

- The modulo operation creates a set, which in modular arithmetic is referred to as the set of least residues modulo n, or Z_n.

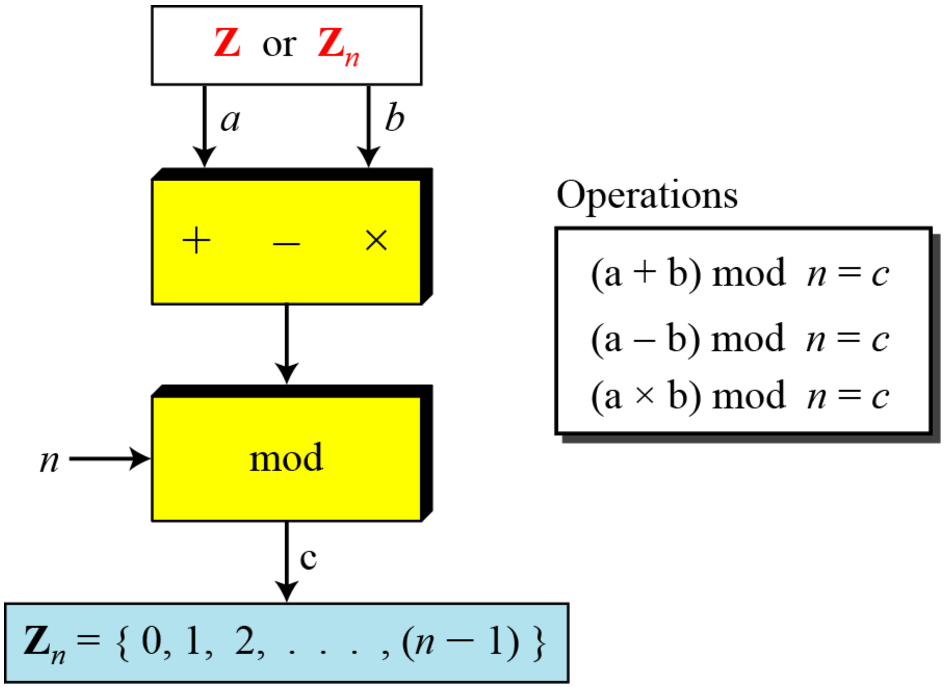


$$\mathbf{Z}_n = \{\, 0, 1, 2, 3, \ . \ . \ . \ , (n-1) \,\}$$

$\mathbf{Z}_2 = \{\, 0, 1 \,\}$ $\mathbf{Z}_6 = \{\, 0, 1, 2, 3, 4, 5 \,\}$ $\mathbf{Z}_{11} = \{\, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \,\}$

Operation in Z_n

- $+, -, \times$ for the set Z can also be defined for the set Z_n. The result may need to be mapped to Z_n using the mod operator.
  - $14 + 7 = 6 \; mod \; 15$
  - $7 - 11 = 11 \; mod \; 15$
  - $7 \times 11 = 2 \; mod \; 15$



Inverses

- In Z_n, two numbers a and b are additive inverses of each other if $a + b = 0 \; mod \; n$
  - $Z_{10} = \{0,1,2,3,4,5,6,7,8,9\}$.
  - The six pairs of additive inverses are (0, 0), (1, 9), (2, 8), (3, 7), (4, 6), and (5, 5).
- In Z_n, two numbers a and b are multiplicative inverses of each other if $a \times b = 1 \; mod \; n$
  - There are only three pairs: (1, 1), (3, 7) and (9, 9).
  - The numbers 0, 2, 4, 5, 6, and 8 do not have a multiplicative inverse. Because $\gcd(8{,}10) \neq 1$.
  - In Z_{11}, we have seven pairs: (1, 1), (2, 6), (3, 4), (5, 9), (7, 8), (9, 5), and (10, 10).

Addition and Multiplication Tables

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

Addition Table in $\mathbf{Z}_{10}$

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

Multiplication Table in $\mathbf{Z}_{10}$

Addition and Multiplication sets

- Cryptography often uses two more sets: Z_p and Z_p^*. The modulus in these two sets is a prime number.

$$Z_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$
$$Z_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

$$\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$
$$\mathbf{Z}_6^* = \{1, 5\}$$

$$\mathbf{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$$
$$\mathbf{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$$

$$\mathbf{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$
$$\mathbf{Z}_{10}^* = \{1, 3, 7, 9\}$$

Fast Computation for $x^d \ (mod\ n)$

- Let t be the number of bits for integer d,
  - e.g., If $d = 5 = 101_2$, then $t = 3$

Let d be the binary representation

```
y=1;
while (d != 0) {
    if ((d%2) == 1) { y=(y*x)%n; }
     d>>1;
     x=(x*x)%n;     /*  x^(2^k)  */
}
```