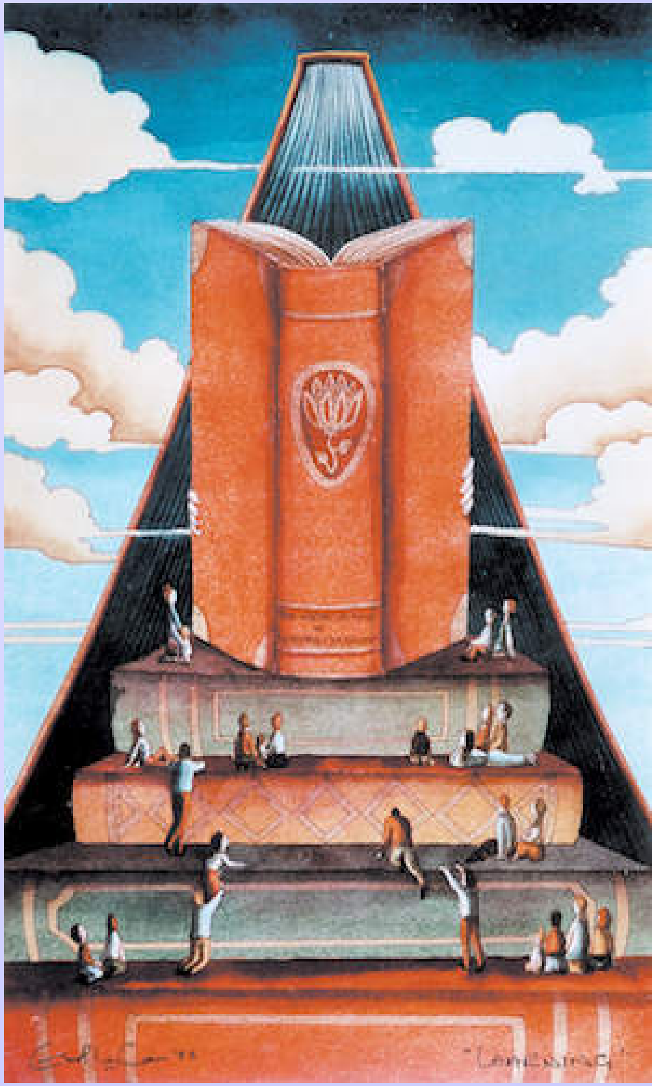
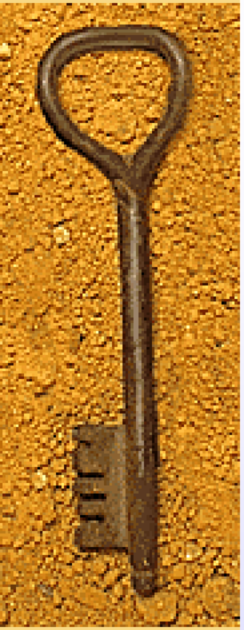
COMPUTER SECURITY (CSE 4105)

Number Theory and Finite Fields

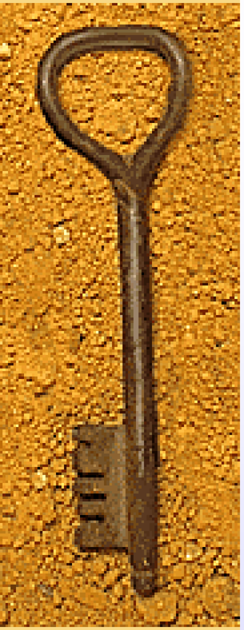


Divisibility



- We say that a nonzero b divides a if a = mb for some m, where a, b, and m are integers.
- That is, b divides a if there is no remainder on division.
- The notation is commonly used b|a to mean b divides a.
- Also, if b|a, we say that b is a divisor of a.

The positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24.
$13 \mid 182;\ -5 \mid 30;\ 17 \mid 289;\ -3 \mid 33;\ 17 \mid 0$



Divisibility

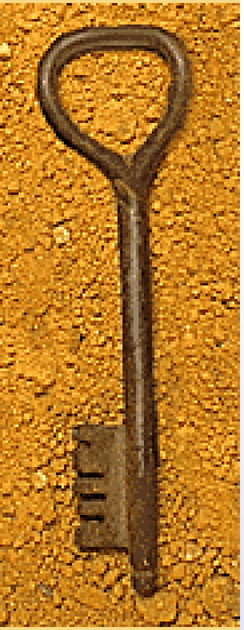
- Subsequently, we will need some simple properties of divisibility for integers, which are as follows:

  - If $a|1$, then $a = \pm 1$.
  - If $a|b$ and $b|a$, then $a = \pm b$.
  - Any $b \neq 0$ divides 0.
  - If $a|b$ and $b|c$, then $a|c$:

$$\boxed{11|66 \text{ and } 66|198 = 11|198}$$

  - If $b|g$ and $b|h$, then $b|(mg + nh)$ for arbitrary integers m and n.

Division Algorithm



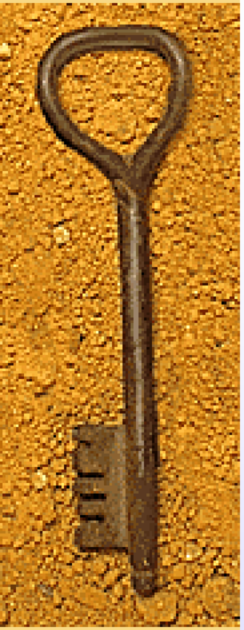
- Given any positive integer n and any nonnegative integer a, if we divide a by n, we get an integer quotient q and an integer remainder r that obey the following relationship:

$$a = qn + r$$

$$q = \lfloor a/n \rfloor$$

$$0 \le r < n$$

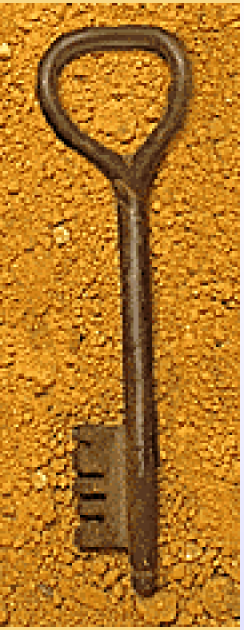
$\lfloor x \rfloor$ is the largest integer less than or equal to



Euclidean Algorithm

- Euclidean algorithm is a simple procedure for determining the greatest common divisor of two positive integers.
- Relatively Prime: Two integers are relatively prime if their only common positive integer factor is 1.
- Greatest Common Divisor: The greatest common divisor of a and b is the largest integer that divides both a and b.
  - We will use the notation gcd(a,b) to mean the greatest common divisor of a and b.
  - We also define gcd(0, 0) = 0.

Euclidean Algorithm



- More formally, the positive integer c is said to be the greatest common divisor of a and b if
  - c is a divisor of both a and b
  - Any divisor of a and b is a divisor of c
- An equivalent definition is the following:

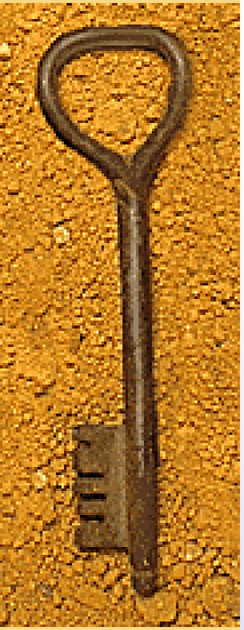
$$\gcd(a, b) = \max[k, \text{such that } k \mid a \text{ and } k \mid b]$$

- Because we require that the greatest common divisor be positive, gcd(a,-b)=gcd(-a,b)=gcd(-a,-b)
- In general, gcd(a, b) = gcd(|a|,|b|).

$$\boxed{\gcd(60, 24) = \gcd(60, -24) = 12}$$

- Thus, a and b are relatively prime if gcd(a, b) = 1

Euclid's Algorithm for gcd



- EUCLID(a,b)
  1. Compute r = a mod b
  2. While $r \neq 0$

     a = b

     b = r

     r = a mod b
  3. Return b

Euclid's Algorithm for gcd

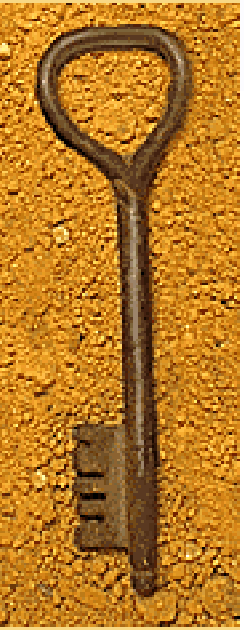
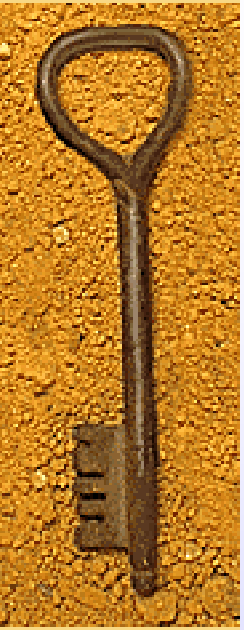


Table 4.1 Euclidean Algorithm Example

Dividend	Divisor	Quotient	Remainder
a = 1160718174	b = 316258250	q_1 = 3	r_1 = 211943424
b = 316258250	r_1 = 211943434	q_2 = 1	r_2 = 104314826
r_1 = 211943424	r_2 = 104314826	q_3 = 2	r_3 = 3313772
r_2 = 104314826	r_3 = 3313772	q_4 = 31	r_4 = 1587894
r_3 = 3313772	r_4 = 1587894	q_5 = 2	r_5 = 137984
r_4 = 1587894	r_5 = 137984	q_6 = 11	r_6 = 70070
r_5 = 137984	r_6 = 70070	q_7 = 1	r_7 = 67914
r_6 = 70070	r_7 = 67914	q_8 = 1	r_8 = 2156
r_7 = 67914	r_8 = 2156	q_9 = 31	r_9 = 1078
r_8 = 2156	r_9 = 1078	q_{10} = 2	r_{10} = 0

Modular Arithmetic



- If a is an integer and n is a positive integer, we define a mod n to be the remainder when a is divided by n.
- The integer n is called the modulus. Thus,

$$a = qn + r \qquad 0 \leq r < n;\ q = \lfloor a/n \rfloor$$

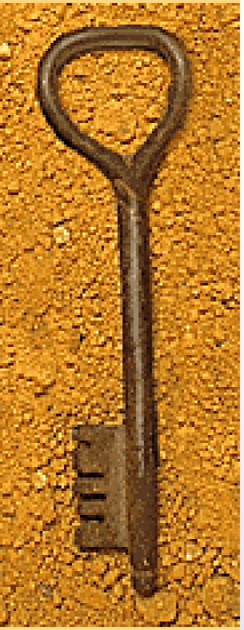
$$a = \lfloor a/n \rfloor \times n + (a \bmod n)$$

$$11 \bmod 7 = 4; \qquad -11 \bmod 7 = 3$$

- Two integers a and b are said to be congruent modulo n, if (a mod n) = (b mod n).
- This is written as a ≡ b mod n or b ≡ a mod n.

$$73 \equiv 4 \pmod{23}; \qquad 21 \equiv -9 \pmod{10}$$

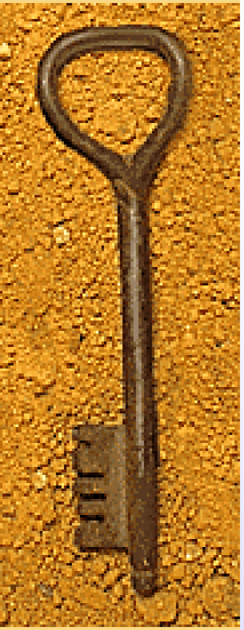
Properties of Modulo operator



- $a \equiv b \bmod n$ if $n \mid (a-b)$
  - If $n \mid (a-b)$ then $a-b = kn$ for some k.
  - So we can write $a = b + kn$
  - Now, $a \bmod n = (b + kn) \bmod n$
    $= b \bmod n$
  - $a \equiv b \bmod n$
- $a \equiv b \bmod n$ implies $b \equiv a \bmod n$
- $a \equiv b \bmod n$ and $b \equiv c \bmod n$ implies $a \equiv c \bmod n$

$$
\begin{aligned}
23 &\equiv 8 \pmod{5} && \text{because} && 23 - 8 = 15 = 5 \times 3 \\
-11 &\equiv 5 \pmod{8} && \text{because} && -11 - 5 = -16 = 8 \times (-2) \\
81 &\equiv 0 \pmod{27} && \text{because} && 81 - 0 = 81 = 27 \times 3
\end{aligned}
$$

Properties of Modular Arithmetic



- $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$

  Let $a \bmod n = r_a$

  and $b \bmod n = r_b$

  Now, $a = r_a + jn$ for some integer j

  $b = r_b + kn$ for some integer k

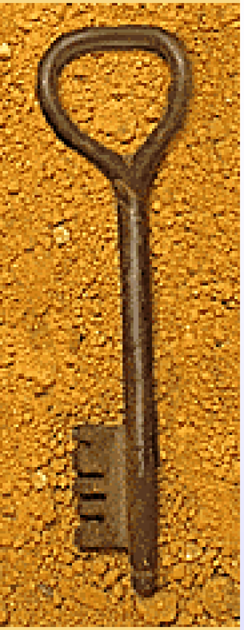
  $(a + b) \bmod n = (r_a + jn + r_b + kn) \bmod n$

  $= [(r_a + r_b) + n(j+k)] \bmod n$

  $= (r_a + r_b) \bmod n$

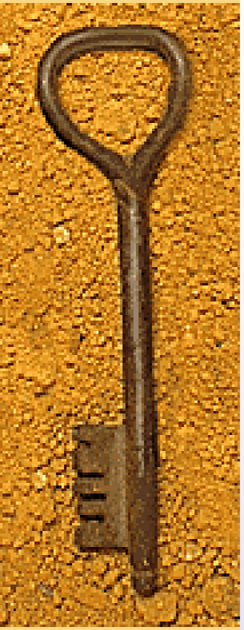
  $= [(a \bmod n) + (b \bmod n)] \bmod n$

Properties of Modular Arithmetic



- $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
- $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

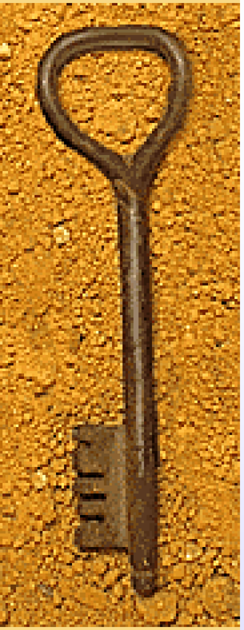
$$11 \bmod 8 = 3;\ 15 \bmod 8 = 7$$
$$[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$$
$$(11 + 15) \bmod 8 = 26 \bmod 8 = 2$$
$$[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 = -4 \bmod 8 = 4$$
$$(11 - 15) \bmod 8 = -4 \bmod 8 = 4$$
$$[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8 = 21 \bmod 8 = 5$$
$$(11 \times 15) \bmod 8 = 165 \bmod 8 = 5$$



Monoid

- Set with an operation i.e. (M,*) is a monoid if it follows the following rules:
  - **Closure**: if a and b belong to M then a*b is also in M
  - **Associative**: a*b*c = a*(b*c) = (a*b)*c
  - **Identity element**: there is an identity element e in M such that a*e = e*a = a for all a in M

Group and Abelian group

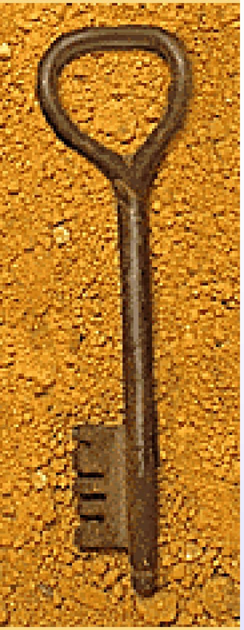


- When monoid follows the rule of inverse element, it is called **group**.
  - Inverse element: for each a in M there is an element a^{-1} in M such that

$$a*a^{-1} = a^{-1}*a = e$$

- A group is said to be **Abelian** if it satisfy the following condition:
  - Communicative: $a*b = b*a$

Ring and Field



- $(R, +, x)$ is a **Ring** if R is an Abelian group under + and R is a monoid under x and R follows distributive law.
  - Distributive: $ax(b+c) = axb + axc$

    $(a+b)xc = axc + bxc$

- $(F, +, x)$ is a **Field** if F is a communicative ring and for all non-zero elements, it holds $axa^{-1} = e$

Thanks for your Attention