6.5 Greatest common divisor and Euclid's algorithm

6.6 Number representation

6.7 Fast exponentiation

Greatest Common Divisor (GCD)

[**Def**]
Let $a, b \in \mathbf{Z}$, $a,b \neq 0$. The largest $d \in \mathbf{Z}$ such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b

denotation: $gcd(a,b)$

Greatest Common Divisor (GCD)

[**Def**]
Let $a, b \in \mathbf{Z}$, $a,b \neq 0$. The largest $d \in \mathbf{Z}$ such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b

denotation: $gcd(a,b)$

How to find GCD

1. find prime factorization of both a, and b
2. take the prime factors present in both factorization with their smallest powers (present in those factorization)
3. multiply

Greatest Common Divisor (GCD)

[**Def**]
Let $a, b \in \mathbf{Z}$, $a,b \neq 0$. The largest $d \in \mathbf{Z}$ such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b

denotation: $gcd(a,b)$

How to find GCD

1. find prime factorization of both a, and b
2. take the prime factors present in both factorization with their smallest powers (present in those factorization)
3. multiply

Example 6:
Find $gcd(28,72)$.

Greatest Common Divisor (GCD)

[**Def**]
Let $a, b \in \mathbf{Z}$, $a,b \neq 0$. The largest $d \in \mathbf{Z}$ such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b

denotation: $gcd(a,b)$

How to find GCD

1. find prime factorization of both a, and b
2. take the prime factors present in both factorization with their smallest powers (present in those factorization)
3. multiply

Example 6:
Find $gcd(28,72)$.

Solution:
1st method:
$28 = 2^2 \cdot 7$, $72 = 2^3 \cdot 3^2$
$gcd(28,36) = 2^2 = 4$.

Greatest Common Divisor (GCD)

[**Def**]
Let $a, b \in \mathbf{Z}$, $a,b \neq 0$. The largest $d \in \mathbf{Z}$ such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b

denotation: $gcd(a,b)$

How to find GCD

1. find prime factorization of both a, and b
2. take the prime factors present in both factorization with their smallest powers (present in those factorization)
3. multiply

Example 6:
Find $gcd(28,72)$.

Solution:
1st method:
$28 = 2^2 \cdot 7,\ 72 = 2^3 \cdot 3^2$
$gcd(28,36) = 2^2 = 4$.

2nd method:

Greatest Common Divisor (GCD)

[**Def**]
Let $a, b \in \mathbf{Z}$, $a,b \neq 0$. The largest $d \in \mathbf{Z}$ such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b

denotation: $gcd(a,b)$

How to find GCD

1. find prime factorization of both a, and b
2. take the prime factors present in both factorization with their smallest powers (present in those factorization)
3. multiply

Example 6:
Find $gcd(28,72)$.

Solution:
1st method:
$28 = 2^2 \cdot 7$, $72 = 2^3 \cdot 3^2$
$gcd(28,36) = 2^2 = 4$.

2nd method:

[**Def**]
Let $a, b \in \mathbf{Z}$, $a,b \neq 0$. The largest $d \in \mathbf{Z}$ such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b

denotation: $gcd(a,b)$

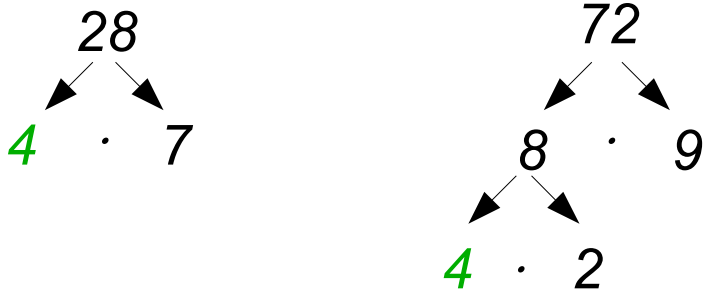
How to find GCD

1. find prime factorization of both a, and b
2. take the prime factors present in both factorization with their smallest powers (present in those factorization)
3. multiply

Example 6:
Find $gcd(28,72)$.

Solution:
1st method:
$28 = 2^2 \cdot 7$, $72 = 2^3 \cdot 3^2$
$gcd(28,36) = 2^2 = 4$.

2nd method:

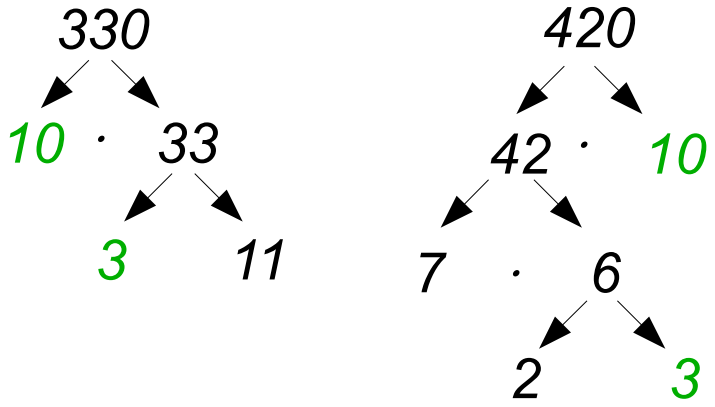


Example 7:
Find *gcd(330,420)*.

Example 7:
Find *gcd(330,420)*.

Solution:

2nd method:



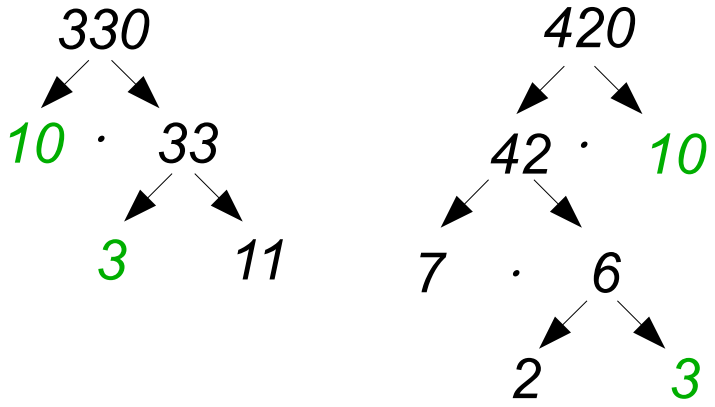
gcd(330,420) = 10 · 3 = 30

Example 7:
Find *gcd(330,420)*.

Solution:
1st method:
$330 = 2 \cdot 3 \cdot 5 \cdot 11,$
$420 = 2^2 \cdot 3 \cdot 5 \cdot 7$

$gcd(330,420) = 2 \cdot 3 \cdot 5 = 30$.

2nd method:



$gcd(330,420) = 10 \cdot 3 = 30$

The methods described above are quite inefficient.

Euclidean Algorithm gives a more efficient way of finding GCD.
It is named after Greek mathematician Euclid.

The Euclidean Algorithm

The methods described above are quite inefficient.

Euclidean Algorithm gives a more efficient way of finding GCD.
It is named after Greek mathematician Euclid.

Input: two positive integers, x and y.
Output: gcd(x, y).

```
If ( y < x )
       Swap x and y
r = y mod x

While ( r ≠ 0 )
       y := x
       x := r
       r := y mod x
End-while

Return( x )
```

This algorithm uses the following lemma (see proof as ZyBooks):

[Lemma 1]
Let $a=bq+r$, where a,b,q, and r are integers. Then $gcd(a,b) = gcd(b,r)$

The Euclidean Algorithm

x y

Example: find gcd(1331,1001)

```
If ( y < x )
       Swap x and y.
r = y mod x

While ( r ≠ 0 )
       y := x
       x := r
       r := y mod x
End-while

Return( x )
```

The Euclidean Algorithm

Example: find gcd(1331,1001)

x y

Solution: gcd(1331,1001) = gcd(1001,1331)

x y x y

– we prefer to take smaller value as divisor and larger as dividend.

```
If ( y < x )
       Swap x and y.
r = y mod x

While ( r ≠ 0 )
       y := x
       x := r
       r := y mod x
End-while

Return( x )
```

The Euclidean Algorithm

x y

Example: find gcd(1331,1001)

x y x y

Solution: gcd(1331,1001) = gcd(1001,1331)

– we prefer to take smaller value as divisor and larger as dividend.

$$\frac{1331}{1001} = 1\,R\,330$$

```
If ( y < x )
       Swap x and y.
r = y mod x

While ( r ≠ 0 )
       y := x
       x := r
       r := y mod x
End-while

Return( x )
```

The Euclidean Algorithm

x y

Example: find gcd(1331,1001)

x y x y

Solution: gcd(1331,1001) = gcd(1001,1331)

– we prefer to take smaller value as divisor and larger as dividend.

$$\frac{1331}{1001} = 1\,R\,330$$

Thus gcd(1331,1001) = gcd(330,1001)

```
If ( y < x )
        Swap x and y.
r = y mod x

While ( r ≠ 0 )
        y := x
        x := r
        r := y mod x
End-while

Return( x )
```

The Euclidean Algorithm

x y

Example: find gcd(1331,1001)

x y x y

Solution: gcd(1331,1001) = gcd(1001,1331)

– we prefer to take smaller value as divisor and larger as dividend.

$$\frac{1331}{1001} = 1\ R\ 330$$

Thus gcd(1331,1001) = gcd(330,1001) =

$$\frac{1001}{330} = 3\ R\ 11$$

```
If ( y < x )
        Swap x and y.
r = y mod x

While ( r ≠ 0 )
        y := x
        x := r
        r := y mod x
End-while

Return( x )
```

The Euclidean Algorithm

Example: find gcd(1331,1001)

Solution: gcd(1331,1001) = gcd(1001,1331)
– we prefer to take smaller value as divisor and larger as dividend.

$$\frac{1331}{1001} = 1\,R\,330$$

Thus gcd(1331,1001) = gcd(330,1001) = gcd(11,330)

$$\frac{1001}{330} = 3\,R\,11$$

```
If ( y < x )
        Swap x and y.
r = y mod x

While ( r ≠ 0 )
        y := x
        x := r
        r := y mod x
End-while

Return( x )
```

The Euclidean Algorithm

x y

Example: find gcd(1331,1001)

x y x y

Solution: gcd(1331,1001) = gcd(1001,1331)

– we prefer to take smaller value as divisor and larger as dividend.

$$\frac{1331}{1001} = 1\,R\,330$$

Thus gcd(1331,1001) = gcd(330,1001) = gcd(11,330) =

$$\frac{1001}{330} = 3\,R\,11 \qquad \frac{330}{11} = 30\,R\,0$$

```
If ( y < x )
        Swap x and y.
r = y mod x

While ( r ≠ 0 )
        y := x
        x := r
        r := y mod x
End-while

Return( x )
```

The Euclidean Algorithm

x y

Example: find gcd(1331,1001)

x y x y

Solution: gcd(1331,1001) = gcd(1001,1331)

– we prefer to take smaller value as divisor and larger as dividend.

$$\frac{1331}{1001} = 1\,R\,330$$

Thus gcd(1331,1001) = gcd(330,1001) = gcd(11,330) = 11

$$\frac{1001}{330} = 3\,R\,11$$

$$\frac{330}{11} = 30\,R\,0$$

STOP

```
If ( y < x )
        Swap x and y.
r = y mod x

While ( r ≠ 0 )
        y := x
        x := r
        r := y mod x
End-while

Return( x )
```

The Euclidean Algorithm

x y

Example: find gcd(1331,1001)

x y x y

Solution: gcd(1331,1001) = gcd(1001,1331)

– we prefer to take smaller value as divisor and larger as dividend.

$$\frac{1331}{1001} = 1\,R\,330$$

Thus gcd(1331,1001) = gcd(330,1001) = gcd(11,330) = 11

$$\frac{1001}{330} = 3\,R\,11$$

$$\frac{330}{11} = 30\,R\,0$$

STOP

Answer: gcd(1331,1001) = 11

```
If ( y < x )
        Swap x and y.
r = y mod x

While ( r ≠ 0 )
        y := x
        x := r
        r := y mod x
End-while

Return( x )
```

The extended Euclidean algorithm

The gcd(x,y) can be expressed as a linear combination of x and y:

Let x,y $\in$ Z, then there are integers s and t such that
gcd(x, y) = sx + ty

```
If ( y < x )
       Swap x and y.
r := 1

While ( r ≠ 0 )
       d := y div x
       r := y - dx
       y := x
       x := r
End-while

Return( y )
```

or

```
If ( y < x )
       Swap x and y.
r := 1

While ( r ≠ 0 )
       r := y - (y div x)x
       y := x
       x := r
End-while

Return( y )
```

The extended Euclidean algorithm

The gcd(x,y) can be expressed as a linear combination of x and y:

> Let x,y $\in$ Z, then there are integers s and t such that
> gcd(x, y) = sx + ty

Example: find gcd(1331,1001)

```
If ( y < x )
   Swap x and y
r := 1

While ( r ≠ 0 )
   d := y div x
   r := y - dx
   y := x
   x := r
End-while

Return( y )
```

The extended Euclidean algorithm

The gcd(x,y) can be expressed as a linear combination of x and y:

> Let x,y $\in$ Z, then there are integers s and t such that
> gcd(x, y) = sx + ty

Example: find gcd(1331,1001)

Solution: gcd(1331,1001) = gcd(1001,1331)
– we prefer to take smaller value as divisor and larger as dividend.

r = 1

```
If ( y < x )
   Swap x and y
r := 1

While ( r ≠ 0 )
   d := y div x
   r := y - dx
   y := x
   x := r
End-while

Return( y )
```

The extended Euclidean algorithm

The gcd(x,y) can be expressed as a linear combination of x and y:

> Let x,y ∈ Z, then there are integers s and t such that
> gcd(x, y) = sx + ty

Example: find gcd(1331,1001)

Solution: gcd(1331,1001) = gcd(1001,1331)
– we prefer to take smaller value as divisor and larger as dividend.

d = 1331 div 1001 = 1
r = 1331 – 1 * 1001 = 330
y = 1001
x = 330

```
If ( y < x )
    Swap x and y
r := 1

While ( r ≠ 0 )
    d := y div x
    r := y - dx
    y := x
    x := r
End-while

Return( y )
```

The extended Euclidean algorithm

The gcd(x,y) can be expressed as a linear combination of x and y:

> Let x,y ∈ Z, then there are integers s and t such that
> gcd(x, y) = sx + ty

Example: find gcd(1331,1001)

Solution: gcd(1331,1001) = gcd(1001,1331)
– we prefer to take smaller value as divisor and larger as dividend.

d = 1331 div 1001 = 1
r = 1331 – 1 * 1001 = 330
y = 1001
x = 330

d = 1001 div 330 = 3
r = 1001 – 3 * 330 = 11
y = 330
x = 11

```
If ( y < x )
    Swap x and y
r := 1

While ( r ≠ 0 )
    d := y div x
    r := y - dx
    y := x
    x := r
End-while

Return( y )
```

The extended Euclidean algorithm

The gcd(x,y) can be expressed as a linear combination of x and y:

> Let x,y ∈ Z, then there are integers s and t such that
> gcd(x, y) = sx + ty

Example: find gcd(1331,1001)

Solution: gcd(1331,1001) = gcd(1001,1331)
– we prefer to take smaller value as divisor and larger as dividend.

d = 1331 div 1001 = 1
r = 1331 – 1 * 1001 = 330
y = 1001
x = 330

d = 1001 div 330 = 3
r = 1001 – 3 * 330 = 11
y = 330
x = 11

d = 330 div 11 = 30
r = 330 – 30 * 11 = 0
y = 11
x = 0

```
If ( y < x )
   Swap x and y
r := 1

While ( r ≠ 0 )
   d := y div x
   r := y - dx
   y := x
   x := r
End-while

Return( y )
```

The extended Euclidean algorithm

The gcd(x,y) can be expressed as a linear combination of x and y:

> Let x,y ∈ Z, then there are integers s and t such that
> gcd(x, y) = sx + ty

Example: find gcd(1331,1001)

Solution: gcd(1331,1001) = gcd(1001,1331)
– we prefer to take smaller value as divisor and larger as dividend.

d = 1331 div 1001 = 1
r = 1331 – 1 * 1001 = 330
y = 1001
x = 330

d = 1001 div 330 = 3
r = 1001 – 3 * 330 = 11
y = 330
x = 11

d = 330 div 11 = 30
r = 330 – 30 * 11 = 0
y = 11
x = 0

Return(11)

```
If ( y < x )
   Swap x and y
r := 1

While ( r ≠ 0 )
   d := y div x
   r := y - dx
   y := x
   x := r
End-while

Return( y )
```

The extended Euclidean algorithm

The gcd(x,y) can be expressed as a linear combination of x and y:

> Let x,y ∈ Z, then there are integers s and t such that
> gcd(x, y) = sx + ty

Example: find gcd(1331,1001)

Solution: gcd(1331,1001) = gcd(1001,1331)
– we prefer to take smaller value as divisor and larger as dividend.

d = 1331 div 1001 = 1
r = 1331 – 1 * 1001 = 330
y = 1001
x = 330

d = 1001 div 330 = 3
r = 1001 – 3 * 330 = 11
y = 330
x = 11

d = 330 div 11 = 30
r = 330 – 30 * 11 = 0
y = 11
x = 0

How to find s and t?

```
If ( y < x )
   Swap x and y
r := 1

While ( r ≠ 0 )
   d := y div x
   r := y - dx
   y := x
   x := r
End-while

Return( y )
```

Return(11)

The extended Euclidean algorithm

The gcd(x,y) can be expressed as a linear combination of x and y:

> Let x,y ∈ Z, then there are integers s and t such that
> gcd(x, y) = sx + ty

Example: find gcd(1331,1001)

x y

Solution: gcd(1331,1001) = gcd(1001,1331)
– we prefer to take smaller value as divisor and larger as dividend.

d = 1331 div 1001 = 1
r = 1331 – 1 * 1001 = 330
y = 1001
x = 330

d = 1001 div 330 = 3
r = 1001 – 3 * 330 = 11
y = 330
x = 11

d = 330 div 11 = 30
r = 330 – 30 * 11 = 0
y = 11
x = 0

How to find s and t?

The extended Euclidean algorithm

The gcd(x,y) can be expressed as a linear combination of x and y:

> Let x,y ∈ Z, then there are integers s and t such that
> gcd(x, y) = sx + ty

Example: find gcd(1331,1001)

x y

Solution: gcd(1331,1001) = gcd(1001,1331)
– we prefer to take smaller value as divisor and larger as dividend.

d = 1331 div 1001 = 1
r = 1331 – 1 * 1001 = 330
y = 1001
x = 330

d = 1001 div 330 = 3
r = 1001 – 3 * 330 = 11
y = 330
x = 11

d = 330 div 11 = 30
r = 330 – 30 * 11 = 0
y = 11
x = 0

How to find s and t?

1001 – 3 * 330 = 11
11 = 1001 – 3 * 330
11 = 1001 – 3 (1331-1*1001)
11 = 1001 – 3*1331 + 3*1001
11 = 4*1001 – 3*1331
s = 4, t = -3

Greatest Common Divisor (GCD)

[**Def**]
Two integers are relatively prime if their *GCD* is *1*. - was given in 6.3

Greatest Common Divisor (GCD)

[**Def**]
Two integers are relatively prime if their *GCD* is *1*.

Example: Determine if each of these pairs are relatively prime
a) *11, 15*
b) *15, 21*

Greatest Common Divisor (GCD)

[**Def**]
Two integers are relatively prime if their *GCD* is *1*.

Example: Determine if each of these pairs are relatively prime

a) *11, 15* *gcd(11,15) = 1* Yes

b) *15, 21*

Greatest Common Divisor (GCD)

[**Def**]
Two integers are relatively prime if their *GCD* is *1*.

Example: Determine if each of these pairs are relatively prime

a) *11, 15* *gcd(11,15) = 1* Yes

b) *15, 21* *gcd(15,21) = 3* No

Greatest Common Divisor (GCD)

[**Def**]
Two integers are relatively prime if their *GCD* is *1*.

Example: Determine if each of these pairs are relatively prime

a) *11, 15* *gcd(11,15) = 1* Yes
b) *15, 21* *gcd(15,21) = 3* No

[Def]
A multiplicative inverse **mod** n (or just inverse **mod** n) of an integer *x*, is an integer $s \in \{1, 2, \ldots, n-1\}$ such that $s \cdot x \bmod n = 1$.

Greatest Common Divisor (GCD)

[**Def**]
Two integers are relatively prime if their *GCD* is *1*.

Example: Determine if each of these pairs are relatively prime

a) *11, 15* *gcd(11,15) = 1* Yes
b) *15, 21* *gcd(15,21) = 3* No

[Def]
A multiplicative inverse **mod** n (or just inverse **mod** n) of an integer *x*, is an integer $s \in \{1, 2, \ldots, n\text{-}1\}$ such that $s \cdot x \bmod n = 1$.

Example: 2 is a multiplicative inverse of 3 mod 5 because
$2 \cdot 3 \bmod 5 = 6 \bmod 5 = 1$

Greatest Common Divisor (GCD)

[**Def**]
Two integers are relatively prime if their *GCD* is *1*.

Example: Determine if each of these pairs are relatively prime

a) *11, 15* *gcd(11,15) = 1* Yes
b) *15, 21* *gcd(15,21) = 3* No

[Def]
A multiplicative inverse **mod** n (or just inverse **mod** n) of an integer *x*, is an integer $s \in \{1, 2, \ldots, n\text{-}1\}$ such that $s \cdot x$ **mod** n = 1.

Example: 2 is a multiplicative inverse of 3 mod 5 because
$2 \cdot 3 \bmod 5 = 6 \bmod 5 = 1$

Not every number has an inverse mod n.

x has an inverse mod n **if and only if** *x* and *n* are relatively prime.

Finding the inverse of a number **mod** *n* is a key step in the RSA cryptosystem.

Greatest Common Divisor (GCD)

The *Extended Euclidean Algorithm* can be used to find the multiplicative inverse of x mod n when it exists.

- if gcd(x, n) ≠ 1, then x does not have a multiplicative inverse **mod** n

- if x and n are relatively prime, then the *Extended Euclidean Algorithm* finds integers s and t such that $1 = s \cdot x + t \cdot n$

- (s **mod** n) is the unique multiplicative inverse of x in {0, 1, …, n **-** 1}.

Greatest Common Divisor (GCD)

The *Extended Euclidean Algorithm* can be used to find the multiplicative inverse of x mod n when it exists.

• if gcd(x, n) ≠ 1, then x does not have a multiplicative inverse **mod** n

• if x and n are relatively prime, then the *Extended Euclidean Algorithm* finds integers s and t such that $1 = s \cdot x + t \cdot n$

• (s **mod** n) is the unique multiplicative inverse of x in {0, 1, …, n **-** 1}.

Example: gcd(12,35) = 1,
and the extended euclidean algorithm will return:

gcd(12,35) = 1 = 3 * 12 – 1 * 35

Greatest Common Divisor (GCD)

The *Extended Euclidean Algorithm* can be used to find the multiplicative inverse of x mod n when it exists.

• if gcd(*x*, *n*) ≠ 1, then *x* does not have a multiplicative inverse **mod** *n*

• if *x* and *n* are relatively prime, then the *Extended Euclidean Algorithm* finds integers *s* and *t* such that $1 = s \cdot x + t \cdot n$

• (*s* **mod** *n*) is the unique multiplicative inverse of *x* in {0, 1, …, n **-** 1}.

Example: gcd(12,35) = 1,
and the extended euclidean algorithm will return:
gcd(12,35) = 1 = 3 * 12 – 1*35

The multiplicative inverse of 12 **mod** 34 is 3 **mod** 35 = 3
checking: (12*3) **mod** 35 = 1

The multiplicative inverse of 35 **mod** 12 is (-1) **mod** 12 = 11
checking: (35*11) **mod** 35 = 385 **mod** 12 = 1

Representation of Integers

In our everyday life we use decimal notation to express integers

Note: decimal notation and decimal numbers are two different terms.

The other ones you probably have heard of are: binary, HEX (hexadecimal), and maybe octal.

Representation of Integers

In our everyday life we use decimal notation to express integers

Note: decimal notation and decimal numbers are two different terms.

The other ones you probably have heard of are: binary, HEX (hexadecimal), and maybe octal.

[**Theorem**]
Let $b \in \mathbf{Z}^+$ and $b > 1$. Then if n is a positive integer, it can be expressed uniquely in the form $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where k is a nonnegative integer, $a_0, a_1, \ldots, a_k$ are nonnegative integers less than b, and $a_k \neq 0$.

A proof of this theorem can be constructed using mathematical induction (not presented here)

$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$ is called base b expansion of n

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 10 gives decimal notation.

Example: 567 stands for 5 hundreds + 6 tens + 7 ones

$567 = 5 * 10^2 + 6 * 10^1 + 7 * 10^0 =$
$= 500 + 60 + 7$

digits: 0,1,2,3,4,5,6,7,8,9

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

digits: $0, 1$

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

digits: *0, 1*
binary expansions are used by computers to represent integers and do arithmetic with them.

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

digits: *0, 1*
binary expansions are used by computers to represent integers and do arithmetic with them.

Example: What is the decimal form (expansion) of the integer that has $(10\ 1101\ 1001)_2$ as its binary expansion?

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

digits: $0, 1$
binary expansions are used by computers to represent integers and do arithmetic with them.

Example: What is the decimal form (expansion) of the integer that has $(10\ 1101\ 1001)_2$ as its binary expansion?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

digits: *0, 1*
binary expansions are used by computers to represent integers and do arithmetic with them.

Example: What is the decimal form (expansion) of the integer that has $(10\ 1101\ 1001)_2$ as its binary expansion?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(10\ 1101\ 1001)_2$ =

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

digits: $0, 1$
binary expansions are used by computers to represent integers and do arithmetic with them.

Example: What is the decimal form (expansion) of the integer that has $(10\ 1101\ 1001)_2$ as its binary expansion?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(10\ 1101\ 1001)_2 = 1 +$

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

digits: $0, 1$
binary expansions are used by computers to represent integers and do arithmetic with them.

Example: What is the decimal form (expansion) of the integer that has $(10\ 1101\ 1001)_2$ as its binary expansion?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(10\ 1101\ 1001)_2 = 1 + 0 \cdot 2$

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

digits: $0, 1$
binary expansions are used by computers to represent integers and do arithmetic with them.

Example: What is the decimal form (expansion) of the integer that has $(10\ 1101\ 1001)_2$ as its binary expansion?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(10\ 1101\ 1001)_2 = 1 + 0 \cdot 2 + 0 \cdot 2^2 +$

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

digits: $0, 1$
binary expansions are used by computers to represent integers and do arithmetic with them.

Example: What is the decimal form (expansion) of the integer that has $(10\ 1101\ 1001)_2$ as its binary expansion?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(10\ 1101\ 1001)_2 = 1 + 0 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 +$

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

digits: $0, 1$
binary expansions are used by computers to represent integers and do arithmetic with them.

Example: What is the decimal form (expansion) of the integer that has $(10\ 1101\ 1001)_2$ as its binary expansion?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(10\ 1101\ 1001)_2 = 1 + 0 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 + 0 \cdot 2^5 + 1 \cdot 2^6 + 1 \cdot 2^7 + 0 \cdot 2^8 + 1 \cdot 2^9 =$

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

digits: $0, 1$
binary expansions are used by computers to represent integers and do arithmetic with them.

Example: What is the decimal form (expansion) of the integer that has $(10\ 1101\ 1001)_2$ as its binary expansion?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(10\ 1101\ 1001)_2 = 1 + 0 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 + 0 \cdot 2^5 + 1 \cdot 2^6 + 1 \cdot 2^7 + 0 \cdot 2^8 + 1 \cdot 2^9 = 1 + 8 + 16 + 64 + 128 + 512$

Binary Expansion

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 2 gives binary expansions of integers.

digits: $0, 1$
binary expansions are used by computers to represent integers and do arithmetic with them.

Example: What is the decimal form (expansion) of the integer that has $(10\ 1101\ 1001)_2$ as its binary expansion?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(10\ 1101\ 1001)_2 = 1 + 0 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + 1 \cdot 2^4 + 0 \cdot 2^5 + 1 \cdot 2^6 + 1 \cdot 2^7 + 0 \cdot 2^8 + 1 \cdot 2^9 = 1 + 8 + 16 + 64 + 128 + 512 = 729_{10}$

Answer: $(10\ 1101\ 1001)_2 = 729_{10}$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the decimal expansion of the hexadecimal expansion of $(3DF0B)_{16}$?

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the decimal expansion of the hexadecimal expansion of $(3DF0B)_{16}$?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the decimal expansion of the hexadecimal expansion of $(3DF0B)_{16}$?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(3DF0B)_{16}$ =

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the decimal expansion of the hexadecimal expansion of $(3DF0B)_{16}$?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(3DF0B)_{16} = 11 +$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the decimal expansion of the hexadecimal expansion of $(3DF0B)_{16}$?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(3DF0B)_{16} = 11 + 0 \cdot 16 +$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the decimal expansion of the hexadecimal expansion of $(3DF0B)_{16}$?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(3DF0B)_{16} = 11 + 0 \cdot 16 + 15 \cdot 16^2 + 13 \cdot 16^3 + 3 \cdot 16^4 =$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the decimal expansion of the hexadecimal expansion of $(3DF0B)_{16}$?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(3DF0B)_{16} = 11 + 0 \cdot 16 + 15 \cdot 16^2 + 13 \cdot 16^3 + 3 \cdot 16^4 = 11 + 3840 + 53248 + 196608$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the decimal expansion of the hexadecimal expansion of $(3DF0B)_{16}$?

Solution: using the highlighted formula and starting from the right, i.e.
$n = a_0 + a_1 b^1 + + a_2 b^2 + \ldots + a_{k-1} b^{k-1} + a_k b^k$

$(3DF0B)_{16} = 11 + 0 \cdot 16 + 15 \cdot 16^2 + 13 \cdot 16^3 + 3 \cdot 16^4 = 11 + 3840 + 53248 + 196608 = 253707_{10}$

Answer: $(3DF0B)_{16} = 253707_{10}$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 16 gives hexadecimal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the hexadecimal expansion of the decimal number 4678?

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be *16* gives hexadecimal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the hexadecimal expansion of the decimal number 4678?

Solution: *divide by 16, set aside the remainder; the quotient of division divide by 16 and set aside the remainder, and so on, till the quotient is 1 (or 0).*

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be *16* gives hexadecimal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the hexadecimal expansion of the decimal number 4678?

Solution: *divide by 16, set aside the remainder; the quotient of division divide by 16 and set aside the remainder, and so on, till the quotient is 1 (or 0).*

4678 ÷ 16 = 292 R 6

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be *16* gives hexadecimal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the hexadecimal expansion of the decimal number 4678?

Solution: *divide by 16, set aside the remainder; the quotient of division divide by 16 and set aside the remainder, and so on, till the quotient is 1 (or 0).*

4678 ÷ 16 = 292 R 6
292 ÷ 16 = 18 R 4

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base *b* to be *16* gives hexadecimal expansions of integers.

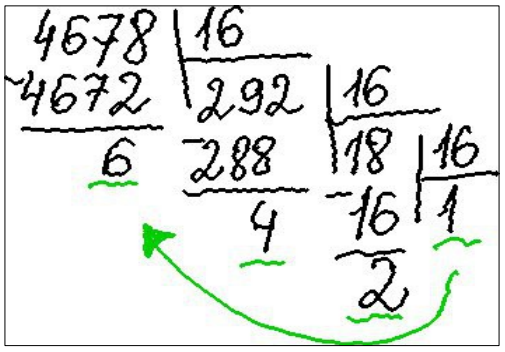
digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the hexadecimal expansion of the decimal number 4678?

Solution: *divide by 16, set aside the remainder; the quotient of division divide by 16 and set aside the remainder, and so on, till the quotient is 1 (or 0).*

4678 ÷ 16 = 292 R 6
292 ÷ 16 = 18 R 4
18 ÷ 16 = 1 R 2

or



Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base *b* to be *16* gives hexadecimal expansions of integers.

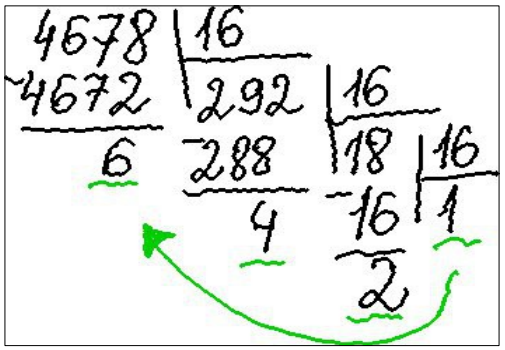
digits: *0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F*
10 11 12 13 14 15

Example: What is the hexadecimal expansion of the decimal number 4678?

Solution: *divide by 16, set aside the remainder; the quotient of division divide by 16 and set aside the remainder, and so on, till the quotient is 1 (or 0).*

4678 ÷ 16 = 292 R 6
292 ÷ 16 = 18 R 4
18 ÷ 16 = 1 R 2

or



Now, starting from the end (from the last quotient): $(1\ 2\ 4\ 6)_{16}$

Answer: $(4678)_{10} = (1246)_{16}$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 8 gives octal expansions of integers.

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 8 gives octal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7*

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 8 gives octal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7*

Example: Find the decimal expansion of $(1347)_8$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$, where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 8 gives octal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7*

Example: Find the decimal expansion of $(1347)_8$

Solution:

$(1347)_8 = 7 + 4 \cdot 8 + 3 \cdot 8^2 + 1 \cdot 8^3 =$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$,
where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 8 gives octal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7*

Example: Find the decimal expansion of $(1347)_8$

Solution:

$(1347)_8 = 7 + 4 \cdot 8 + 3 \cdot 8^2 + 1 \cdot 8^3 = 7 + 32 + 192 + 512$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$, where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 8 gives octal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7*

Example: Find the decimal expansion of $(1347)_8$

Solution:

$(1347)_8 = 7 + 4 \cdot 8 + 3 \cdot 8^2 + 1 \cdot 8^3 = 7 + 32 + 192 + 512 = 743$

Answer: $(1347)_8 = 743$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$, where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 8 gives octal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7*

Example: Find the decimal expansion of $(1347)_8$

Solution:

$(1347)_8 = 7 + 4 \cdot 8 + 3 \cdot 8^2 + 1 \cdot 8^3 = 7 + 32 + 192 + 512 = 743$

Answer: $(1347)_8 = 743$

Example: Find the octal expansion of $(47)_{10}$

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$, where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 8 gives octal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7*

Example: Find the decimal expansion of $(1347)_8$

Solution:

$(1347)_8 = 7 + 4 \cdot 8 + 3 \cdot 8^2 + 1 \cdot 8^3 = 7 + 32 + 192 + 512 = 743$

Answer: $(1347)_8 = 743$

Example: Find the octal expansion of $(47)_{10}$

Solution:

$47 \div 8 = 5$ R 7

Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$, where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 8 gives octal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7*

Example: Find the decimal expansion of $(1347)_8$

Solution:

$(1347)_8 = 7 + 4 \cdot 8 + 3 \cdot 8^2 + 1 \cdot 8^3 = 7 + 32 + 192 + 512 = 743$

Answer: $(1347)_8 = 743$

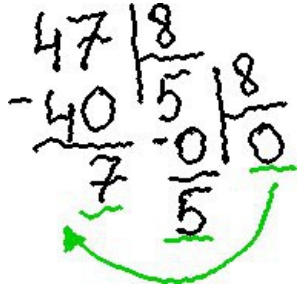
Example: Find the octal expansion of $(47)_{10}$

Solution:

$47 \div 8 = 5$ R 7

$5 \div 8 = 0$ R 5

or



Hexadecimal Expansion (HEX)

Let $b \in \mathbf{Z}^+$ and $b > 1$; $n \in \mathbf{Z}^+$, $n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b^1 + a_0$, where $k \in \mathbf{Z}^+$ and $k \geq 0$; $0 \leq a_i < b$, $i = 0,\ldots,k$, and $a_k \neq 0$.

Choosing the base b to be 8 gives octal expansions of integers.

digits: *0, 1, 2, 3, 4, 5, 6, 7*

Example: Find the decimal expansion of $(1347)_8$

Solution:

$(1347)_8 = 7 + 4 \cdot 8 + 3 \cdot 8^2 + 1 \cdot 8^3 = 7 + 32 + 192 + 512 = 743$

Answer: $(1347)_8 = 743$

Example: Find the octal expansion of $(47)_{10}$

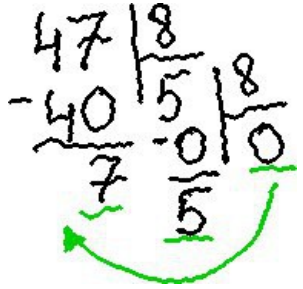
Solution:

$47 \div 8 = 5$ R 7

$5 \div 8 = 0$ R 5

Answer: $(057)_8 = (57)_8$

or



Hexadecimal Expansion (HEX)

There is a nice table that allows to speed up the process of “conversions”, but be very careful when using it. There are lots of nuances.

Example:
to convert $(11\ 1010\ 1001\ 1111)_2$ into hexadecimal notation we group the binary digits into groups of four (from the right), and add initial zeros at the start (if needed), use the table, write the hexadecimal notation:

11 1010 1001 1111
3 A 9 F

therefore,
$(11\ 1010\ 1001\ 1111)_2 = (3A9F)_{16}$

Hexadecimal Expansion (HEX)

There is a nice table that allows to speed up the process of “conversions”, but be very careful when using it. There are lots of nuances.

TABLE 1 Hexadecimal, Octal, and Binary Representation of the Integers 0 through 15.

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

Example 5:
to convert $(11\ 1010\ 1001\ 1111)_2$ into hexadecimal notation we group the binary digits into groups of four (from the right), and add initial zeros at the start (if needed),

Hexadecimal Expansion (HEX)

There is a nice table that allows to speed up the process of “conversions”, but be very careful when using it. There are lots of nuances.

TABLE 1 Hexadecimal, Octal, and Binary Representation of the Integers 0 through 15.

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

Example 5:
to convert $(11\ 1010\ 1001\ 1111)_2$ into hexadecimal notation we group the binary digits into groups of four (from the right), and add initial zeros at the start (if needed), use the table, write the hexadecimal notation:

11 1010 1001 1111

Hexadecimal Expansion (HEX)

There is a nice table that allows to speed up the process of “conversions”, but be very careful when using it. There are lots of nuances.

TABLE 1 Hexadecimal, Octal, and Binary Representation of the Integers 0 through 15.

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

Example 5:
to convert $(11\ 1010\ 1001\ 1111)_2$ into hexadecimal notation we group the binary digits into groups of four (from the right), and add initial zeros at the start (if needed), use the table, write the hexadecimal notation:

11 1010 1001 1111
3

Hexadecimal Expansion (HEX)

There is a nice table that allows to speed up the process of “conversions”, but be very careful when using it. There are lots of nuances.

TABLE 1 Hexadecimal, Octal, and Binary Representation of the Integers 0 through 15.

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

Example 5:
to convert $(11\ 1010\ 1001\ 1111)_2$ into hexadecimal notation we group the binary digits into groups of four (from the right), and add initial zeros at the start (if needed), use the table, write the hexadecimal notation:

11 1010 1001 1111
3 A

Hexadecimal Expansion (HEX)

There is a nice table allows to speed up the process of “conversions”, but be very careful when using it. There are lots of nuances.

TABLE 1 Hexadecimal, Octal, and Binary Representation of the Integers 0 through 15.

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

Example 5:
to convert $(11\ 1010\ 1001\ 1111)_2$ into hexadecimal notation we group the binary digits into groups of four (from the right), and add initial zeros at the start (if needed), use the table, write the hexadecimal notation:

11 1010 1001 1111
3 A 9

Hexadecimal Expansion (HEX)

There is a nice table that allows to speed up the process of “conversions”, but be very careful when using it. There are lots of nuances.

TABLE 1 Hexadecimal, Octal, and Binary Representation of the Integers 0 through 15.

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

Example 5:
to convert $(11\ 1010\ 1001\ 1111)_2$ into hexadecimal notation we group the binary digits into groups of four (from the right), and add initial zeros at the start (if needed), use the table, write the hexadecimal notation:

11 1010 1001 1111
3 A 9 F

therefore,
$(11\ 1010\ 1001\ 1111)_2 = (3A9F)_{16}$

In cryptography it is important to be able to find b^n efficiently, where b, n are large integers.

We can use an algorithm that employs the binary expansion of the exponent n. To compute b^n, the algorithm computes b, b^2, $(b^2)^2$,$(b^4)^2$, ... till some point, and then multiplies all of them.

Input: Positive integers x and y.
Output: x^y

```
procedure fastExponentiation(x,y)
p := 1     // p holds the partial result.
s := x     // s holds the current (x^2)^j
r := y     // r is used for binary expansion of y

While ( r > 0 )
      If ( r mod 2 = 1 ), p := p·s
      s := s·s
      r := r div 2
End-while
Return(p)
```

Example: Find 7^{16}

p = 1, s = 7, r = 16

```
p := 1
s := x
r := y

While ( r > 0 )
    If ( r mod 2 = 1 )
       p := p·s
    s := s·s
    r := r div 2
End-while
Return(p)
```

Modular Exponentiation

Example: Find 7^{16}

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49 7^2
r = 16 div 2 = 8

```
p := 1
s := x
r := y

While ( r > 0 )
    If ( r mod 2 = 1 )
       p := p·s
    s := s·s
    r := r div 2
End-while
Return(p)
```

Modular Exponentiation

Example: Find 7^{16}

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49 7^2
r = 16 div 2 = 8

p = 1, s = 49, r = 8

```
p := 1
s := x
r := y

While ( r > 0 )
    If ( r mod 2 = 1 )
       p := p·s
    s := s·s
    r := r div 2
End-while
Return(p)
```

Modular Exponentiation

Example: Find 7^{16}

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49 7^2
r = 16 div 2 = 8

p = 1, s = 49, r = 8

8 mod 2 = 0
s = 49*49 = 2401 $(7^2)^2$
r = 8 div 2 = 4

```
p := 1
s := x
r := y

While ( r > 0 )
    If ( r mod 2 = 1 )
       p := p·s
    s := s·s
    r := r div 2
End-while
Return(p)
```

Modular Exponentiation

Example: Find 7^{16}

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49
r = 16 div 2 = 8

p = 1, s = 49, r = 8

8 mod 2 = 0
s = 49*49 = 2401 7^4
r = 8 div 2 = 4

p = 1, s = 2 401, r = 4

```
p := 1
s := x
r := y

While ( r > 0 )
    If ( r mod 2 = 1 )
       p := p·s
    s := s·s
    r := r div 2
End-while
Return(p)
```

Modular Exponentiation

Example: Find 7^{16}

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49
r = 16 div 2 = 8

p = 1, s = 49, r = 8

8 mod 2 = 0
s = 49*49 = 2401 7^4
r = 8 div 2 = 4

p = 1, s = 2 401, r = 4

4 mod 2 = 0
s = 2 401*2 401 = 5 764 801 $(7^4)^2$
r = 4 div 2 = 2

```
p := 1
s := x
r := y

While ( r > 0 )
    If ( r mod 2 = 1 )
       p := p·s
    s := s·s
    r := r div 2
End-while
Return(p)
```

Modular Exponentiation

Example: Find 7^{16}

p = 1, s = 5 764 801, r = 2

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49
r = 16 div 2 = 8

p = 1, s = 49, r = 8

8 mod 2 = 0
s = 49*49 = 2401
r = 8 div 2 = 4

p = 1, s = 2 401, r = 4

4 mod 2 = 0
s = 2 401*2 401 = 5 764 801
r = 4 div 2 = 2

7^8

```
p := 1
s := x
r := y

While ( r > 0 )
    If ( r mod 2 = 1 )
       p := p·s
    s := s·s
    r := r div 2
End-while
Return(p)
```

Modular Exponentiation

Example: Find 7^{16}

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49
r = 16 div 2 = 8

p = 1, s = 49, r = 8

8 mod 2 = 0
s = 49*49 = 2401
r = 8 div 2 = 4

p = 1, s = 2 401, r = 4

4 mod 2 = 0
s = 2 401*2 401 = 5 764 801 7^8
r = 4 div 2 = 2

p = 1, s = 5 764 801, r = 2

4 mod 2 = 0
s = $5\ 764\ 801^2 = 33\ 232\ 930\ 569\ 601$ $(7^8)^2$
r = 2 div 2 = 1

```
p := 1
s := x
r := y

While ( r > 0 )
    If ( r mod 2 = 1 )
       p := p·s
    s := s·s
    r := r div 2
End-while
Return(p)
```

Modular Exponentiation

Example: Find 7^{16}

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49
r = 16 div 2 = 8

p = 1, s = 49, r = 8

8 mod 2 = 0
s = 49*49 = 2401
r = 8 div 2 = 4

p = 1, s = 2 401, r = 4

4 mod 2 = 0
s = 2 401*2 401 = 5 764 801
r = 4 div 2 = 2

p = 1, s = 5 764 801, r = 2

4 mod 2 = 0
s = 5 764 801^2 = 33 232 930 569 601 7^{16}
r = 2 div 2 = 1

p = 1, s = 33 232 930 569 601, r = 1

```
p := 1
s := x
r := y

While ( r > 0 )
    If ( r mod 2 = 1 )
       p := p·s
    s := s·s
    r := r div 2
End-while
Return(p)
```

Modular Exponentiation

Example: Find 7^{16}

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49
r = 16 div 2 = 8

p = 1, s = 49, r = 8

8 mod 2 = 0
s = 49*49 = 2401
r = 8 div 2 = 4

p = 1, s = 2 401, r = 4

4 mod 2 = 0
s = 2 401*2 401 = 5 764 801
r = 4 div 2 = 2

p = 1, s = 5 764 801, r = 2

4 mod 2 = 0
s = 5 764 801^2 = 33 232 930 569 601 7^{16}
r = 2 div 2 = 1

p = 1, s = 33 232 930 569 601, r = 1

1 mod 2 = 1
p = 1 * 33 232 930 569 601
s = 33 232 930 569 601^2 = ...
r = 1 div 2 = 0

```
p := 1
s := x
r := y

While ( r > 0 )
    If ( r mod 2 = 1 )
       p := p·s
    s := s·s
    r := r div 2
End-while
Return(p)
```

Modular Exponentiation

Example: Find 7^{16}

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49
r = 16 div 2 = 8

p = 1, s = 49, r = 8

8 mod 2 = 0
s = 49*49 = 2401
r = 8 div 2 = 4

p = 1, s = 2 401, r = 4

4 mod 2 = 0
s = 2 401*2 401 = 5 764 801
r = 4 div 2 = 2

p = 1, s = 5 764 801, r = 2

4 mod 2 = 0
s = 5 764 801^2 = 33 232 930 569 601 7^{16}
r = 2 div 2 = 1

p = 1, s = 33 232 930 569 601, r = 1

1 mod 2 = 1
p = 1 * 33 232 930 569 601 7^{16}
s = 33 232 930 569 601^2 = ...
r = 1 div 2 = 0

```
p := 1
s := x
r := y

While ( r > 0 )
    If ( r mod 2 = 1 )
       p := p·s
    s := s·s
    r := r div 2
End-while
Return(p)
```

Modular Exponentiation

Example: Find 7^{16}

p = 1, s = 7, r = 16

16 mod 2 = 0
s = 7*7 = 49
r = 16 div 2 = 8

p = 1, s = 49, r = 8

8 mod 2 = 0
s = 49*49 = 2401
r = 8 div 2 = 4

p = 1, s = 2 401, r = 4

4 mod 2 = 0
s = 2 401*2 401 = 5 764 801
r = 4 div 2 = 2

p = 1, s = 5 764 801, r = 2

4 mod 2 = 0
s = 5 764 801^2 = 33 232 930 569 601
r = 2 div 2 = 1

p = 1, s = 33 232 930 569 601, r = 1

1 mod 2 = 1
p = 1 * 33 232 930 569 601
s = 33 232 930 569 601^2 = ...
r = 1 div 2 = 0

7^{16}

```
p := 1
s := x
r := y

While ( r > 0 )
    If ( r mod 2 = 1 )
       p := p·s
    s := s·s
    r := r div 2
End-while
Return(p)
```

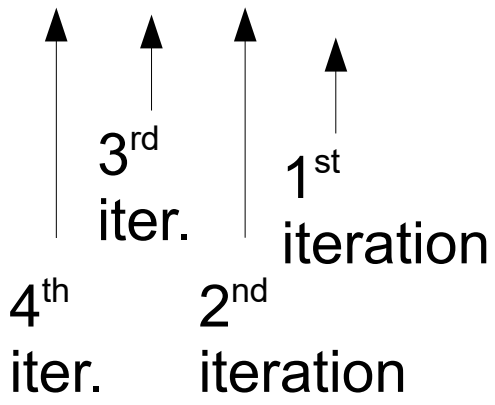
Return(33 232 930 569 601)

Example: Find 7^{16}

What does the algorithm do?

$16 = (1\ 0000)_2 = 1 * 2^4 + 0 * 2^3 + 0 * 2^2 + 0 * 2^1 + 0 * 2^0$

Therefore $7^{16} = 7^{1*2^4+0*2^3+0*2^2+0*2^1+0*2^0} = 7^{2^4} * 7^0 * 7^0 * 7^0 * 7^0$



In cryptography it is important to be able to find b^n ***mod*** m efficiently, where b, n, and m are large integers.

As we have discussed, it is impractical to first compute b^n and then find its remainder when divided by m, because b^n will be a huge number.

Modular Exponentiation

In cryptography it is important to be able to find b^n ***mod*** m efficiently, where b, n, and m are large integers.

As we have discussed, it is impractical to first compute b^n and then find its remainder when divided by m, because b^n will be a huge number.

```
Input: Positive integers x and y.
Output: x^y mod n

p := 1    //p holds the partial result.
s := x    //s holds the current (x^2)^j
r := y    //r is used to compute the binary expansion of y

While ( r > 0 )
      If ( r mod 2 = 1 )
            p := p·s mod n
      s := s·s mod n
      r := r div 2
End-while

Return(p)
```

modifications from fast exponentiation are shown in pink

Example: Find 7^{644} ***mod*** *645*

644=(10 1000 0100)$_2$

p = 1, s = 7, r = 644

```
p := 1, s := x
r := y

While ( r > 0 )
  If ( r mod 2 = 1 )
     p := p·s mod n
  s := s·s mod n
  r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 1, s = 7, r = 644

644 mod 2 != 1, *hence p is not updated*
s = 7 * 7 mod 645 = 49 mod 645 = 49
r = 644 div 2 = 322

```
p := 1, s := x
r := y

While ( r > 0 )
   If ( r mod 2 = 1 )
      p := p·s mod n
   s := s·s mod n
   r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 1, s = 7, r = 644

644 mod 2 != 1, *hence p is not updated*
s = 7 * 7 mod 645 = 49 mod 645 = 49
r = 644 div 2 = 322

p = 1, s = 49, r = 322

```
p := 1, s := x
r := y

While ( r > 0 )
   If ( r mod 2 = 1 )
      p := p·s mod n
   s := s·s mod n
   r := r div 2
End-while

Return(p)
```

Modular Exponentiation

Example: Find 7^{644} ***mod*** *645*

644=(10 1000 0100)$_2$

p = 1, s = 7, r = 644

644 mod 2 != 1, *hence p is not updated*
s = 7 * 7 mod 645 = 49 mod 645 = 49
r = 644 div 2 = 322

p = 1, s = 49, r = 322

322 mod 2 != 1, *hence p is not updated*
r = 49^2 mod 645 = 2401 mod 645 = 466
r = 322 div 2 = 161

```
p := 1, s := x
r := y

While ( r > 0 )
   If ( r mod 2 = 1 )
      p := p·s mod n
   s := s·s mod n
   r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 1, s = 7, r = 644

644 mod 2 != 1, *hence p is not updated*
s = 7 * 7 mod 645 = 49 mod 645 = 49
r = 644 div 2 = 322

p = 1, s = 49, r = 322

322 mod 2 != 1, *hence p is not updated*
r = 49^2 mod 645 = 2401 mod 645 = 466
r = 322 div 2 = 161

p = 1, s = 466, r = 161

```
p := 1, s := x
r := y

While ( r > 0 )
   If ( r mod 2 = 1 )
      p := p·s mod n
   s := s·s mod n
   r := r div 2
End-while

Return(p)
```

Modular Exponentiation

Example: Find 7^{644} ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 1, s = 7, r = 644

644 mod 2 != 1, *hence p is not updated*
s = 7 * 7 mod 645 = 49 mod 645 = 49
r = 644 div 2 = 322

p = 1, s = 49, r = 322

322 mod 2 != 1, *hence p is not updated*
r = 49^2 mod 645 = 2401 mod 645 = 466
r = 322 div 2 = 161

p = 1, s = 466, r = 161

161 mod 2 = 1, *hence p is updated*
p = 1 * 466 mod 645 = 466
s = 466^2 mod 645 = 436
r = 161 div 2 = 80

```
p := 1, s := x
r := y

While ( r > 0 )
   If ( r mod 2 = 1 )
      p := p·s mod n
   s := s·s mod n
   r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

644=(10 1000 0100)$_2$

p = 1, s = 7, r = 644

644 mod 2 != 1, *hence p is not updated*
s = 7 * 7 mod 645 = 49 mod 645 = 49
r = 644 div 2 = 322

p = 1, s = 49, r = 322

322 mod 2 != 1, *hence p is not updated*
r = 49^2 mod 645 = 2401 mod 645 = 466
r = 322 div 2 = 161

p = 1, s = 466, r = 161

161 mod 2 = 1, *hence p is updated*
p = 1 * 466 mod 645 = 466
s = 466^2 mod 645 = 436
r = 161 div 2 = 80

p = 466, s = 436, r = 80

```
p := 1, s := x
r := y

While ( r > 0 )
   If ( r mod 2 = 1 )
      p := p·s mod n
   s := s·s mod n
   r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

644=(10 1000 0100)$_2$

p = 466, s = 436, r = 80

```
p := 1, s := x
r := y

While ( r > 0 )
   If ( r mod 2 = 1 )
      p := p·s mod n
   s := s·s mod n
   r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 466, s = 436, r = 80

80 mod 2 != 1, *hence p is not updated*
$s = 436^2 \bmod 645 = 466$
r = 80 div 2 = 40

```
p := 1, s := x
r := y

While ( r > 0 )
   If ( r mod 2 = 1 )
      p := p·s mod n
   s := s·s mod n
   r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

644=(10 1000 0100)$_2$

p = 466, s = 436, r = 80

80 mod 2 != 1, *hence p is not updated*
s = 436^2 mod 645 = 466
r = 80 div 2 = 40

p = 466, s = 466, r = 40

```
p := 1, s := x
r := y

While ( r > 0 )
   If ( r mod 2 = 1 )
      p := p·s mod n
   s := s·s mod n
   r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

644=(10 1000 0100)$_2$

p = 466, s = 436, r = 80

80 mod 2 != 1, *hence p is not updated*
s = 436^2 mod 645 = 466
r = 80 div 2 = 40

p = 466, s = 466, r = 40

40 mod 2 != 1, *hence p is not updated*
s = 466^2 mod 645 = 436
R = 40 div 2 = 20

```
p := 1, s := x
r := y

While ( r > 0 )
   If ( r mod 2 = 1 )
      p := p·s mod n
   s := s·s mod n
   r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

644=(10 1000 0100)$_2$

p = 466, s = 436, r = 80

80 mod 2 != 1, *hence p is not updated*
s = 436^2 mod 645 = 466
r = 80 div 2 = 40

p = 466, s = 466, r = 40

40 mod 2 != 1, *hence p is not updated*
s = 466^2 mod 645 = 436
R = 40 div 2 = 20

p = 466, s = 436, r = 20

```
p := 1, s := x
r := y

While ( r > 0 )
   If ( r mod 2 = 1 )
      p := p·s mod n
   s := s·s mod n
   r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 466, s = 436, r = 80

80 mod 2 != 1, *hence p is not updated*
$s = 436^2 \bmod 645 = 466$
r = 80 div 2 = 40

p = 466, s = 466, r = 40

40 mod 2 != 1, *hence p is not updated*
$s = 466^2 \bmod 645 = 436$
R = 40 div 2 = 20

p = 466, s = 436, r = 20

20 mod 2 != 1, *hence p is not updated*
$s = 436^2 \bmod 645 = 466$
r = 20 div 2 = 10

```
p := 1, s := x
r := y

While ( r > 0 )
   If ( r mod 2 = 1 )
      p := p·s mod n
   s := s·s mod n
   r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

644=(10 1000 0100)$_2$

p = 466, s = 436, r = 80

80 mod 2 != 1, *hence p is not updated*
s = 436^2 mod 645 = 466
r = 80 div 2 = 40

p = 466, s = 466, r = 40

40 mod 2 != 1, *hence p is not updated*
s = 466^2 mod 645 = 436
R = 40 div 2 = 20

p = 466, s = 436, r = 20

20 mod 2 != 1, *hence p is not updated*
s = 436^2 mod 645 = 466
r = 20 div 2 = 10

p = 466, s = 466, r = 10

```
p := 1, s := x
r := y

While ( r > 0 )
   If ( r mod 2 = 1 )
      p := p·s mod n
   s := s·s mod n
   r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

644=(10 1000 0100)$_2$

p = 466, s = 466, r = 10

10 mod 2 != 1, *hence p is not updated*
s = 466^2 mod 645 = 436
r = 10 div 2 = 5

p = 466, s = 436, r = 5

5 mod 2 = 1, *hence p is updated*
p = 466 * 436 mod 645 = 1
s = 436^2 mod 645 = 466
r = 5 div 2 = 2

p = 1 , s = 466, r = 2

2 mod 2 != 1, *hence p is not updated*
s = 466^2 mod 645 = 436
r = 2 div 2 = 1

p = 1, s = 436, r=1

```
p := 1, s := x
r := y

While ( r > 0 )
   If ( r mod 2 = 1 )
      p := p·s mod n
   s := s·s mod n
   r := r div 2
End-while

Return(p)
```

Example: Find 7^{644} ***mod*** *645*

$644=(10\ 1000\ 0100)_2$

p = 1, s = 436, r=1

1 mod 2 = 1, hence p is updated
p = 1 * 436 mod 645 = 436
s = 436^2 mod 645 = 466
r = 1 div 2 = 0

p = 436, s = 466, r = 0

STOP

Return(436)

7^{644} ***mod*** *645 = 436*

```
p := 1, s := x
r := y

While ( r > 0 )
  If ( r mod 2 = 1 )
     p := p·s mod n
  s := s·s mod n
  r := r div 2
End-while

Return(p)
```