Algoritmalar, Tamsayılar ve Matrisler

CSC-2259 Ayrık Yapılar

Fonksiyonların Büyümesi

$f : R \to R$ $\quad\quad$ $g : R \to R$

Big-Oh: $f(x)$ is $O(g(x))$

En kötü durum

Big-Omega: $f(x)$ is $\Omega(g(x))$

En iyi durum

Big-Theta: $f(x)$ is $\Theta(g(x))$

Aynı durum

Big-Oh: $f(x)$ is $O(g(x))$

(Notation abuse: $f(x) = O(g(x))$)

There are constants C, k (called witnesses) such that for all $x > k$:

$$|f(x)| \leq C \cdot |g(x)|$$

$$f(x) = x^2 \qquad g(x) = x^2 + 2x + 1$$

$$f(x) = O(g(x))$$

$$x^2 = O(x^2 + 2x + 1)$$

For $x > 0$: $x^2 \leq x^2 + 2x + 1$

$$f(x) \leq g(x)$$

Witnesses: $C = 1, \quad k = 0$

$$f(x) = x^2 \qquad g(x) = x^2 + 2x + 1$$

$$g(x) = O(f(x))$$

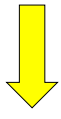
$$x^2 + 2x + 1 = O(x^2)$$

For $x > 1$: $x^2 + 2x + 1 \le x^2 + 2x^2 + x^2 = 4x^2$

$$g(x) \le 4 \cdot f(x)$$

Witnesses: $C = 4, \quad k = 1$

$f(x) = O(g(x))$ ve $g(x) = O(f(x))$



f ve g aynı derecededir

Example: x^2 ve $x^2 + 2x + 1$
aynı derecededir

$f(x) = O(g(x))$ ve $|g(x)| \leq |h(x)|$

$f(x) = O(h(x))$

Example: $x^2 + 2x + 1 = O(x^2)$, $|x^2| \leq |x^3|$ $\Rightarrow$ $x^2 + 2x + 1 = O(x^3)$

$n^2 \neq O(n)$

Suppose $n^2 = O(n)$

Then for all $n > k$: $|n^2| \leq C \cdot |n|$

$|n| \leq C$

Impossible for $n > \max(C, k)$

Theorem: If $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$

then $f(x) = O(x^n)$

Proof: for $x > 1$

$$\begin{aligned} |f(x)| &= |a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0| \\ &\le |a_n| x^n + |a_{n-1}| x^{n-1} + \cdots + |a_1| x + |a_0| \\ &\le |a_n| x^n + |a_{n-1}| x^n + \cdots + |a_1| x^n + |a_0| x^n \\ &= x^n (|a_n| + |a_{n-1}| + \cdots + |a_1| + |a_0|) \end{aligned}$$

Witnesses: $C = |a_n| + |a_{n-1}| + \cdots + |a_0|, \quad k = 1$

End of Proof

$$1 + 2 + \cdots + n = O(n^2)$$

$$1 + 2 + \cdots + n \le n + n + \cdots + n = n^2$$

Witnesses: $C = 1, \quad k = 1$

$$n! = 1 \cdot 2 \cdot \cdots \cdot n = O(n^n)$$

$$n! = 1 \cdot 2 \cdot \cdots \cdot n \leq n \cdot n \cdot \cdots \cdot n = n^n$$

Witnesses: $C = 1, \quad k = 1$

$$2^n = O(n!)$$

$$\begin{aligned} 2^n &= 2 \cdot 2^{n-1} \\ &= 2 \cdot (2 \cdot 2 \cdot \cdots \cdot 2) \\ &\leq 2 \cdot (2 \cdot 3 \cdot \cdots \cdot n) \\ &= 2 \cdot n! \end{aligned}$$

Witnesses: $C = 2, \quad k = 2$

$$\log n! = O(n \cdot \log n)$$

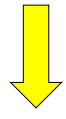
$$\log n! \leq \log n^n = n \cdot \log n$$

Witnesses: $C = 1, \quad k = 1$

$$n = O(2^n)$$

$$\log n = O(n)$$

For $n > 1$: $n < 2^n$



$$\log n < \log 2^n = n \cdot \log 2 = n$$

Witnesses: $C = 1, \quad k = 1$

$$\log_a n = O(\log n)$$

$$\log_a n = \frac{\log n}{\log a}$$

Witnesses: $C = \frac{1}{\log a}, \quad k = 1$

constant $\frac{1}{x} = O(1)$

For $x > 1$: $\frac{1}{x} \leq 1$

Witnesses: $C = 1, \quad k = 1$

Interesting functions

$$1 \quad \log n \quad n \quad n\log n \quad n^2 \quad 2^n \quad n!$$

Higher growth

Theorem: If $f_1(x) = O(g_1(x))$, $f_2(x) = O(g_2(x))$

then $(f_1 + f_2)(x) = O(\max(|g_1(x)|, |g_2(x)|))$

Proof: $x > k_1 \quad |f_1(x)| \le C_1 \cdot |g_1(x)|$

$x > k_2 \quad |f_2(x)| \le C_2 \cdot |g_2(x)|$

$x > \max(k_1, k_2)$

$$\begin{aligned} |(f_1 + f_2)(x)| &= |f_1(x) + f_2(x)| \le |f_1(x)| + |f_2(x)| \\ &\le C_1 |g_1(x)| + C_2 |g_2(x)| \\ &\le (C_1 + C_2) \cdot \max(|g_1(x)|, |g_2(x)|) \end{aligned}$$

Witnesses: $C = C_1 + C_2, \quad k = \max(k_1, k_2)$

End of Proof

Corollary: If $f_1(x) = O(g(x))$, $f_2(x) = O(g(x))$

then $(f_1 + f_2)(x) = O(g(x))$

Theorem: If $f_1(x) = O(g_1(x))$, $f_2(x) = O(g_2(x))$

then $(f_1 f_2)(x) = O(g_1(x) g_2(x))$

$$3n\log(n!) + (n^2+3)\log n = O(n^2 \log n)$$

Multiplication

$3n = O(n)$

$\log(n!) = O(n \log n)$

$3n\log(n!) = O(n \cdot n \log n) = O(n^2 \log n)$

$n^2 + 3 = O(n^2)$

$\log n = O(\log n)$

$(n^2+3)\log(n) = O(n^2 \log n)$

Addition

$3n\log(n!) + (n^2+3)\log n = O(n^2 \log n)$

Big-Omega: $f(x)$ is $\Omega(g(x))$

(Notation abuse: $f(x) = \Omega(g(x))$)

There are constants C, k (called witnesses) such that for all $x > k$:

$$| f(x) | \geq C \cdot | g(x) |$$

$$8x^3 + 5x^2 + 7 = \Omega(x^3)$$

$x > 1$ $\qquad$ $8x^3 + 5x^2 + 7 \geq 8x^3$

Witnesses: $C = 8, \quad k = 1$

Same order

Big-Theta: $f(x)$ is $\Theta(g(x))$

(Notation abuse: $f(x) = \Theta(g(x))$)

$$f(x) = O(g(x)) \text{ and } f(x) = \Omega(g(x))$$

Alternative definition:

$$f(x) = O(g(x)) \text{ and } g(x) = O(f(x))$$

$$3x^2 + 8x \log x = \Theta(x^2)$$

$$3x^2 + 8x \log x \leq 3x^2 + 8x^2 = 11x^2$$

$3x^2 + 8x \log x = O(x^2)$ Witnesses: $C = 11, \quad k = 1$

$$3x^2 + 8x \log x \geq 3x^2$$

$3x^2 + 8x \log x = \Omega(x^2)$ Witnesses: $C = 3, \quad k = 1$

Theorem: If $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$

then $f(x) = \Theta(x^n)$

Proof: We have shown: $f(x) = O(x^n)$

We only need to show $f(x) = \Omega(x^n)$

Take $x > 1$ and examine two cases

Case 1: $a_n > 0$

Case 2: $a_n < 0$

Case 1: $a_n > 0 \qquad (x > 1)$

$$b = \max(|a_{n-1}|, |a_{n-2}|, \ldots, |a_0|)$$

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \\ &\geq a_n x^n - nbx^{n-1} \\ &\geq a' x^n \end{aligned}$$

For $0 < a' < a_n$ and $x \geq \dfrac{nb}{(a_n - a')}$

Case 2 is similar

End of Proof

Complexity of Algorithms

Time complexity

Number of operations performed

Space complexity

Size of memory used

Linear search algorithm

```
ardsil(int Dizi[], int N, int aranan)
{
      int k;
      for (k=0; k<N; k++) {
           if  (Dizi[k]==aranan)
                return k;
       }
       return -1;
}
```

Time complexity

Comparisons

Item not found in list: $2(n+1)+1$

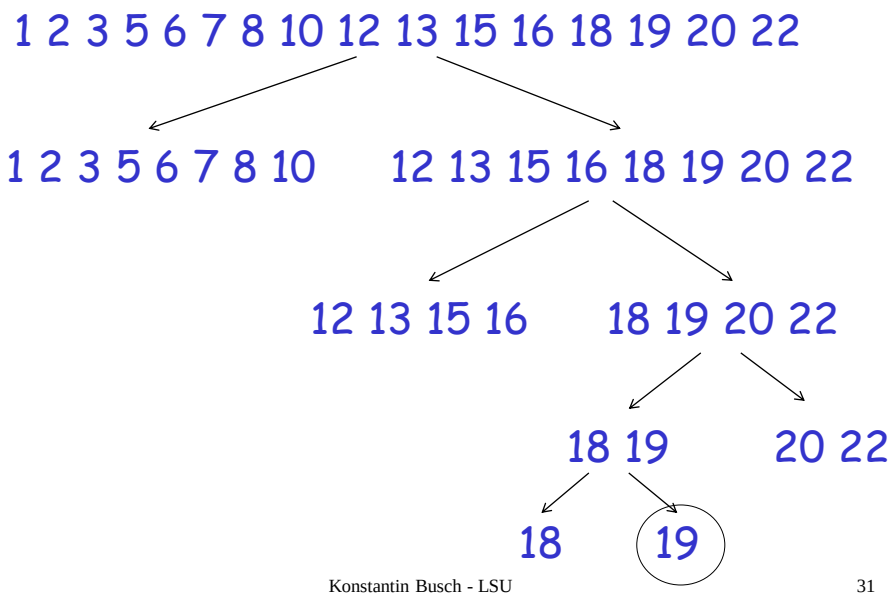
Item found in position i: $2i+1$

Worst case performance: $2(n+1)+1 = O(n)$

Binary search algorithm

```
Binary-Search( x,  a_1, a_2, ..., a_n ) {
  i ← 1        //left endpoint of search area
  j ← n        //right endpoint of search area
  while(i < j ) {
     m ← ⌊(i + j) / 2⌋
     if (x > a_m) i ← m+1   //item is in right half
     else j ← m             //item is in left half
  }
  if (x = a_i ) return i     //item found
  else return 0              //item not found
}
```

Search 19



Time complexity

Size of search list at iteration 1: $\frac{n}{2^0}$

Size of search list at iteration 2: $\frac{n}{2^1}$

$\vdots$

Size of search list at iteration k: $\frac{n}{2^{k-1}}$

Size of search list at iteration k: $\frac{n}{2^{k-1}}$

Smallest list size: 1

in last iteration m: $\frac{n}{2^{m-1}} = 1$

$$m = 1 + \log n$$

Total comparisons:

$$(1 + \log n) \cdot 2 + 1 = \Theta(\log n)$$

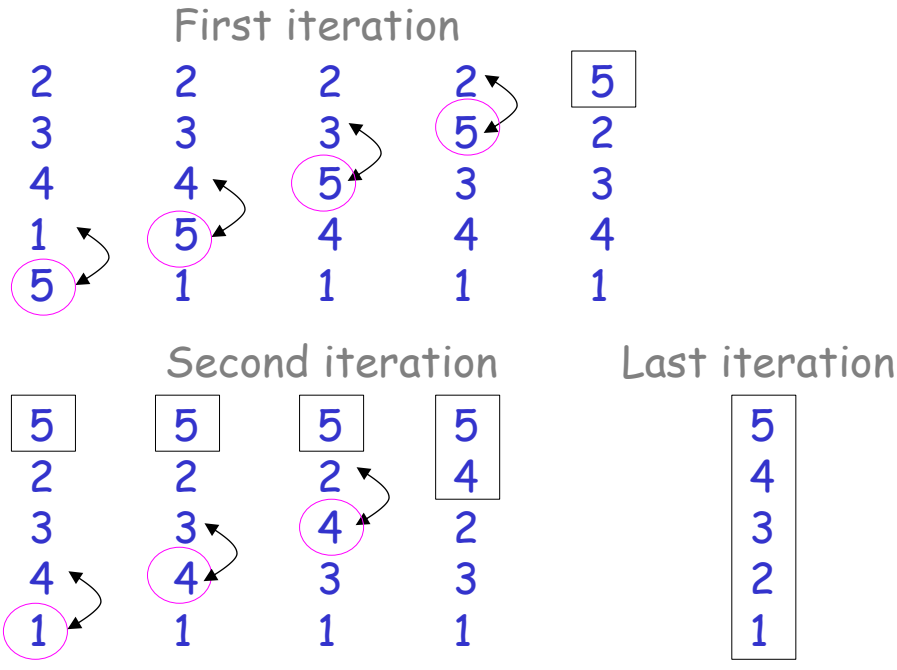
#iterations

Comparisons per iteration

Last comparison

Bubble sort algorithm

```
Bubble-Sort( a_1, a_2, ..., a_n ) {
  for (i ← 1 to n − 1) {
     for (j ← 1 to n − i )
        if (a_j > a_{j+1})
           swap a_j, a_{j+1}
}
```

Time complexity

Comparisons in iteration 1: $n-1$

Comparisons in iteration 2: $n-2$

$\vdots$

Comparisons in iteration $n-1$: 1

Total: $1+2+\cdots+(n-1)=\frac{(n-1)n}{2}=\Theta(n^2)$

Hassas problemler

Class P:

Problems with algorithms whose time complexity is polynomial $O(n^b)$

Examples: Search, Sorting, Shortest path

Intractable problems

Class NP :

Solution can be verified in polynomial time
but no polynomial time algorithm is known

Examples: Satisfiability,
TSP (gezgin satıcı problemi), Vertex coloring

Important computer science question

$$P = NP\,?$$

Unsolvable problems

There exist unsolvable problems which
do not have any algorithm

Example: Halting problem in Turing Machines
Turing makinasından kararsızlık problemleri

Integers and Algorithms

Base b expansion of integer n:

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b^1 + a_0$$

$$(a_k a_{k-1} \cdots a_1 a_0)_b$$

Integers: $k \geq 0 \qquad 0 \leq a_i < b$

Example: $(276)_{10} = 2 \cdot 10^2 + 7 \cdot 10 + 6$

Binary expansion

Digits: 0,1

$$(1\,01011111)_2$$
$$= 1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5$$
$$+ 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$
$$= 351$$

Hexadecimal expansion

Digits: $0,1,2,\ldots,9,A,B,C,D,E,F$

$$(2AE0B)_{16}$$
$$= 2\cdot 16^4 + 10\cdot 16^3 + 14\cdot 16^2 + 0\cdot 16 + 11$$
$$= 175627$$

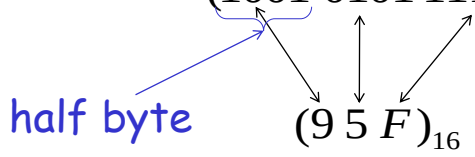
Octal expansion

Digits: $0,1,2,\ldots,7$

$$(245)_8$$
$$= 2\cdot 8^2 + 4\cdot 8 + 5$$
$$= 165$$

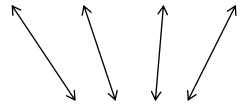
Conversion between binary and hexadecimal

$$(1001\ 0101\ 1111)_2$$



Conversion between binary and octal

$$(100\ 101\ 011\ 111)_2$$



$$(4\ 5\ 3\ 7)_8$$

Binary expansion of $241 = (11110001)_2$

$$\begin{array}{rcrcll}
241 & = & 2\cdot 120 & + & 1 & a_0 \\
120 & = & 2\cdot 60 & + & 0 & a_1 \\
60 & = & 2\cdot 30 & + & 0 & a_2 \\
30 & = & 2\cdot 15 & + & 0 & \\
15 & = & 2\cdot 7 & + & 1 & \vdots \\
7 & = & 2\cdot 3 & + & 1 & \\
3 & = & 2\cdot 1 & + & 1 & \\
1 & = & 2\cdot 0 & + & 1 & a_7
\end{array}$$

Octal expansion of $12345 = (30071)_8$

$$
\begin{array}{rcrcll}
12345 & = & 8 \cdot 1543 & + & 1 & a_0 \\
1543 & = & 8 \cdot 192 & + & 7 & a_1 \\
192 & = & 8 \cdot 24 & + & 0 & a_2 \\
24 & = & 8 \cdot 3 & + & 0 & a_3 \\
3 & = & 8 \cdot 0 & + & 3 & a_4
\end{array}
$$

Base b expansion(n) {
  $q \leftarrow n$
  $k \leftarrow 0$
  While ($q \neq 0$) {
    $a_k \leftarrow q \bmod b$
    $q \leftarrow \lfloor q / b \rfloor$
    $k \leftarrow k + 1$
  }
  return $(a_{k-1} a_{k-2} \cdots a_1 a_0)_b$
}

Carry bit: 1 1 1

$$\begin{array}{rl} 1110 & a \\ +1011 & b \\ \hline 11001 & \end{array}$$

Time complexity of binary addition: $O(n)$

(counting bit additions) $O(\log a)$


```
Binary_addition(a, b) {
    a = (a_{n-1} a_{n-2} ... a_1 a_0)_2
    b = (b_{n-1} b_{n-2} ... b_1 b_0)_2
    c ← 0                    //carry bit
    for j ← 0 to n-1 {
        d ← ⌊(a_j + b_j + c)/2⌋ //auxilliary
        s_j ← a_j + b_j + c - 2d  //j sum bit
        c ← d                //carry bit
    }
    s_n ← c                  //last sum bit
    return (s_n s_{n-1} ... s_1 s_0)_2
}
```

$$
\begin{array}{rrrrrl}
 & & 1 & 1 & 0 & a \\
 & \times & 1 & 0 & 1 & b \\
\hline
 & & 1 & 1 & 0 & c_0 \\
 & 0 & 0 & 0 & & c_1 \\
+ & 1 & 1 & 0 & & c_2 \\
\hline
 & 1 & 1 & 1 & 1 & 0
\end{array}
$$

Time complexity of multiplication: $O(n)$

(counting shifts and bit additions) $O(\log^2 a)$

Binary_multiplication(a,b) {

$a = (a_{n-1}a_{n-2}\cdots a_1 a_0)_2$

$b = (b_{n-1}b_{n-2}\cdots b_1 b_0)_2$

for $j \leftarrow 0$ to $n-1$ {

if $(b_j = 1)$

$c_j \leftarrow a_j \cdot 2^j$ //a shifted j positions

else

$c_j \leftarrow 0$

}

$p \leftarrow c_0 + c_1 + \cdots + c_{n-1}$

return binary expansion of p

}

Tam sayılar ve böler

Tam sayılar $a, b \quad (a \neq 0)$

a böler : b $\quad a \mid b \quad$ $\exists c, \; b = a \cdot c$

faktör

Örnekler: $3 \mid 12 \quad 12 = 3 \cdot 4$

$3 \nmid 7$

a, b, c Tam sayı

if $a \mid b$ then $a \mid bc$

$a \mid b \Rightarrow \exists s \quad b = a \cdot s \Rightarrow bc = a \cdot (sc)$

a, b, c Tam sayı

if $a \mid b$ and $a \mid c$ then $a \mid (b+c)$

$$\left.\begin{array}{ll} a \mid b \Rightarrow \exists s & b = a \cdot s \\ a \mid c \Rightarrow \exists t & c = a \cdot t \end{array}\right\} \; b + c = a \cdot (s+t)$$

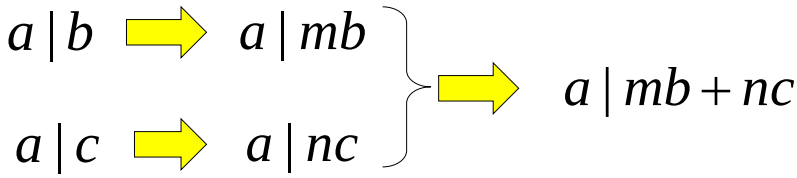
a, b, c integers

if $a \mid b$ and $b \mid c$ then $a \mid c$

$$\left.\begin{array}{ll} a \mid b \Rightarrow \exists s & b = a \cdot s \\ b \mid c \Rightarrow \exists t & c = b \cdot t \end{array}\right\} \; c = a \cdot st$$

a, b, c, m, n integers

if $a \mid b$ and $a \mid c$ then $a \mid mb + nc$



The division "algorithm"

$a \in Z \qquad d \in Z^+$

There are unique $q, r \in Z$ such that:

$$a = d \cdot q + r$$

bölen — d

bölüm — q

kalan — r

$$0 \leq r < d$$

$$a = d \cdot q + r$$

$$q = a \text{ div } d \qquad r = a \text{ mod } d$$

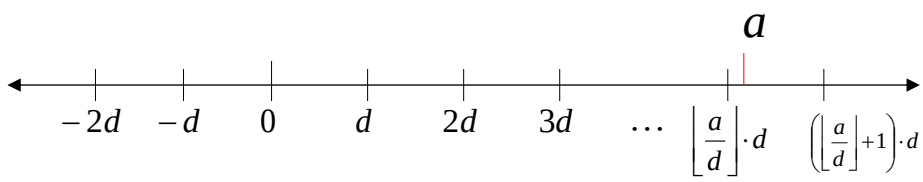
$$q = \left\lfloor \frac{a}{d} \right\rfloor \qquad r = \left| a - \left\lfloor \frac{a}{d} \right\rfloor d \right|$$

Examples: $101 = 11 \cdot 9 + 2$

$9 = 101 \text{ div } 11 \qquad 2 = 101 \text{ mod } 11$

$-11 = 3(-4) + 1$

$-4 = -11 \text{ div } 3 \qquad 1 = -11 \text{ mod } 3$



Number of positive integers divisible by d and not exceeding a:

$$\left\lfloor \frac{a}{d} \right\rfloor$$

```
Division_algorithm(a, d ) {
    q ← 0     r ←| a |
     while ( r ≥ d ) {
        r ← r − d
        q ← q + 1
     }
     if (a < 0 and r > 0) {   //a is negative
        r ← d − r             //adjust r
        q ← −(q + 1)          //adjust q
     }
     else if ( a < 0 ) { q ← −q }
     return  q (a div d) , r (a mod d)
}
```


$a = 15$

$d = 4$

r	q
15	0
$15 - 4 = 11$	1
$11 - 4 = 7$	2
$7 - 4 = 3$	3

$r = 15 \bmod 4 = 3 \qquad q = 15 \text{ div } 4 = 3$

Time complexity of division alg.: $O(q \log a)$

There is a better algorithm: $O(\log a \cdot \log d)$

(based on binary search)

Modular Arithmetic

$$a, b \in Z \qquad m \in Z^+$$

$$a \equiv b \pmod{m}$$

"a is congruent to b modulo m"

$$a \bmod m = b \bmod m$$

Examples: $1 \equiv 13 \pmod{12}$ $\qquad 0 \equiv m \pmod{m}$

$11 \equiv 5 \pmod{6}$ $\qquad k \cdot m \equiv 0 \pmod{m}$

Equivalent definitions

$$a \equiv b \pmod{m}$$

$$\Updownarrow$$

$$a \bmod m = b \bmod m$$

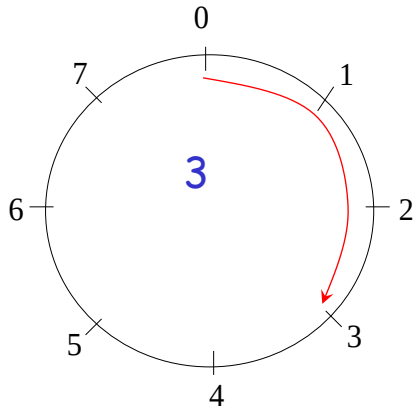
$$\Updownarrow$$

$$m \mid a - b$$

$$\Updownarrow$$

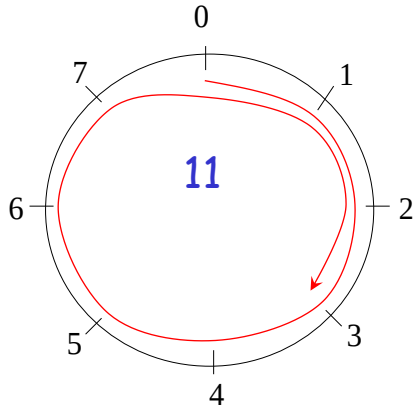
$$\exists k \in Z, \quad a = b + km$$

$$3 \bmod 8 = 3$$



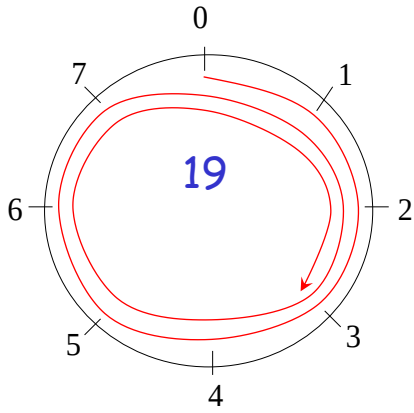
Length of line represents number

$$11 \bmod 8 = 3$$



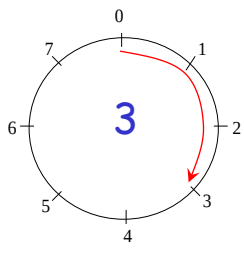
Length of helix line represents number

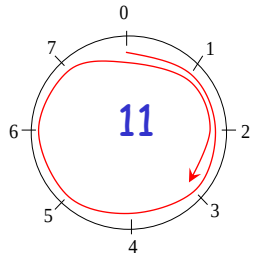
$$19 \bmod 8 = 3$$

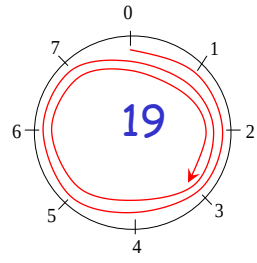


Length of helix line represents number

$$3 \equiv 11 \equiv 19 (\bmod 8)$$







Helix lines terminate in same number

Congruence class of a modulo m :

$$S_a = \{b \mid a \equiv b \pmod{m}\}$$

There are m congruence classes:

$$S_0, S_1, \ldots, S_{m-1}$$

$$\left.\begin{array}{l} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{array}\right\} \Rightarrow a + c \equiv b + d \pmod{m}$$

$$\left.\begin{array}{l} a \equiv b \pmod{m} \Rightarrow a = b + sm \\ c \equiv d \pmod{m} \Rightarrow c = d + tm \end{array}\right\} a + c = d + b + (s+t)m$$

$$\left.\begin{array}{l} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{array}\right\} \Rightarrow a \cdot c \equiv b \cdot d \pmod{m}$$

$$\left.\begin{array}{l} a \equiv b \pmod{m} \Rightarrow a = b + sm \\ c \equiv d \pmod{m} \Rightarrow c = d + tm \end{array}\right\} \begin{array}{l} a \cdot c = (b + sm)(d + tm) \\ \quad = \mathrm{bd} + m(bt + ds + stm) \end{array}$$

$$7 \equiv 2 \pmod{5}$$

$$11 \equiv 1 \pmod{5}$$

$$18 = 7 + 11 \equiv (2 + 1) \pmod{5} = 3 \pmod{5}$$

$$77 = 7 \cdot 11 \equiv (2 \cdot 1) \pmod{5} = 2 \pmod{5}$$

$$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

$$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$$

Follows from previous results by using:

$$a \bmod m = (a \bmod m) \bmod m$$

$$b \bmod m = (b \bmod m) \bmod m$$

Modular exponentiation

Compute $b^n \bmod m$ efficiently using small numbers

Binary expansion of n

$$b^n = b^{a_{k-1}2^{k-1}+\cdots+a_1 2+a_0} = b^{a_{k-1}2^{k-1}} \cdots b^{a_1 2} b^{a_0}$$

$$b^n \bmod m$$
$$= b^{a_{k-1}2^{k-1}} \cdots b^{a_1 2} b^{a_0} \bmod m$$
$$= ((b^{a_{k-1}2^{k-1}} \bmod m) \cdot \cdots \cdot (b^{a_1 2} \bmod m) \cdot (b^{a_0} \bmod m)) \bmod m$$

Example: $3^{644} \bmod 645 = 36$

$$644 = 1010000100 = 2^9 + 2^7 + 2^2$$

$$3^{644} = 3^{2^9+2^7+2^2} = 3^{2^9} 3^{2^7} 3^{2^2}$$

$$3^{644} \bmod 645$$
$$= (3^{2^9} 3^{2^7} 3^{2^2}) \bmod 645$$
$$= ((3^{2^9} \bmod 645)(3^{2^7} \bmod 645)(3^{2^2} \bmod 645) \bmod 645)$$

Compute all the powers of 3 efficiently

$3^2 \bmod 645 = 9 \bmod 645 = 9$

$3^{2^2} \bmod 645 = \left(3^2\right)^2 \bmod 645 = ((3^2 \bmod 645)(3^2 \bmod 645)) \bmod 645 = (9 \cdot 9 \bmod 645) = 81$

$3^{2^3} \bmod 645 = \left(3^{2^2}\right)^2 \bmod 645 = ((3^{2^2} \bmod 645)(3^{2^2} \bmod 645)) \bmod 645 = 81 \cdot 81 \bmod 645 = 111$

$\vdots$

$3^{2^9} \bmod 645 = \left(3^{2^8}\right)^2 \bmod 645 = ((3^{2^8} \bmod 645)(3^{2^8} \bmod 645)) \bmod 645 = 111$

Use the powers of 3 to get result efficiently

3^{644}

$= (3^{2^9} 3^{2^7} 3^{2^2} \bmod 645)$

$= (3^{2^9} 3^{2^7} (3^{2^2} \bmod 645) \bmod 645) = (3^{2^9} 3^{2^7} 81 \bmod 645)$

$= (3^{2^9} (((3^{2^7} \bmod 645) 81) \bmod 645) \bmod 645) = (3^{2^9} ((396 \cdot 81) \bmod 645) \bmod 645) = (3^{2^9} \cdot 471 \bmod 645)$

$= (((3^{2^9} \bmod 645) \cdot 471) \bmod 645) = 111 \cdot 471 \bmod 645 = 36$

Modular_Exponentiation(b, n, m) {

$n = (a_{n-1}a_{n-2}\cdots a_1 a_0)_2$

$x \leftarrow 1$

$power \leftarrow b \bmod m$

for $i = 0$ to $k-1$ {

if ($a_i = 1$) $x \leftarrow (x \cdot power) \bmod m$

$power \leftarrow (power \cdot power) \bmod m$

}

return $x \quad (b^n \bmod m)$

}

Time complexity: $O(\log^2 m \cdot \log n)$

bit operations

Congruent application: Hashing functions

$$h(k) = k \bmod m$$

Example: $h(k) = k \bmod 111$

Employer id Folder#

$h(064212848) = 064212848 \bmod 111 = 14$

$h(037149212) = 037149212 \bmod 111 = 65$

$h(107405723) = 107405723 \bmod 111 = 14$ collision

Application: Pseudorandom numbers

Sequence of pseudorandom numbers

$$x_0, x_1, x_2, \ldots$$

Linear congruential method: $x_{n+1} = (ax_n + c) \bmod m$

$2 \le a < m$

$0 \le c < m$

seed $0 \le x_0 < m$

Example: $x_{n+1} = (7x_n + 4) \bmod 9$ seed $x_0 = 3$

3,7,8,6,1,2,0,4,5,3,7,8,6,1,2,0,4,5,3…

Application: Cryptology

"MEET YOU IN THE PARK"

encryption $f(x) = (x+3) \bmod m$

decryption $f^{-1}(x) = (x-3) \bmod m$

"PHHW BRX LQ WKH SDUN"

Shift cipher: $f(x) = (x+2) \bmod m$

Affine transformation: $f(x) = (ax+b) \bmod m$

Asal ve En Büyük Ortak Bölen

Asal : p Positive integer greater than 1, only positive factors are $1, p$

Asal olmayanlar = composite (bileşik)

Asallar: 2,3,5,7,11,13,17,19,23,29,31,37,41,...

Aritmetiğin temel teoremi

Her pozitif tamsayı, ya asaldır ya da asal sayıların sonucudur.

Asal çarpanlarına ayırma:

$$m = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_l^{k_l}$$

asal

Örnekler: $100 = 2^2 \cdot 5^2$ $999 = 3^3 \cdot 37$

$$7007 = 7^2 \cdot 11 \cdot 13$$

Theorem: If n is composite then it has prime divisor $p \leq \sqrt{n}$

Proof:

n is composite $\Rightarrow$ $\exists a, \exists b, 1 < a, b < n, n = ab$

$c = \min(a, b) \leq \sqrt{n}$ since otherwise

$ab > \sqrt{n}\sqrt{n} = n$

From fundamental theorem of arithmetic
c is either prime or has a prime divisor

End of Proof


```
Prime_factorization( n ) {
    p ← 2    //first prime
    n' ← n
    while ( n'>1 and p ≤ √n') {
        if ( p divides n') {
            p is a factor of n
            n' ← n' / p
        }
        else
            p ← next prime after p
    }
    return all prime factors found
}
```

$n = 7007$

$p = 2,3,5$ do not divide 7007

$p = 7$ $\quad 7007 = 7 \cdot 1001$ $\quad n'$

$p = 7$ $\quad 1001 = 7 \cdot 143$

$p = 7$ does not divide 143

$p = 11$ $\quad 143 = 11 \cdot 13$

$p = 11$ $\quad 13$ $\quad (11 > \sqrt{13})$

$n = 7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$

Theorem: Sonsuz sayıda asal sayı vardır

Proof: Sonlu sayıda asal sayı olduğunu varsayalım

$p_1, p_2, \ldots, p_k$

Let $q = p_1 p_2 \cdots p_k + 1$

If some prime $p_i \mid q$

Since $p_i \mid -p_1 p_2 \cdots p_k$

$\Rightarrow p_i \mid q - p_1 p_2 \cdots p_k = 1$

impossible

No prime divides q $\Rightarrow$ q is prime

(From fundamental theorem of arithmetic)

Contradiction!

End of Proof

Bilinen en büyük asal (as of 2006)

$$2^{30.402.457} - 1$$

Mersenne asal sayılarının gösterimi:

$$2^k - 1$$

$2^2 - 1 = 3$ $2^3 - 1 = 7$ $2^5 - 1 = 31$

Asal sayı teoremi

The number of primes less or equal to n approaches to:

$$\frac{n}{\ln n}$$

$\log_e n$

Goldbach'nın varsayımı:

Her tam sayı iki asal sayının toplamıdır

$4 = 2 + 2 \quad 6 = 3 + 3 \quad 8 = 5 + 3 \quad 10 = 7 + 3$

Ardışık ikili asal sayılar varsayımı:

Sonsuz sayıda ardışık ikili asal sayı vardır.

İki farklı ikili asal sayı vardır:

$3,5 \quad 5,7 \quad 11,13 \quad 17,19$

En büyük ortak bölen

$\gcd(a,b) =$ largest integer d such that $d \mid a$ and $d \mid b$

$a, b \in Z$

$|a| + |b| \neq 0$

Examples: $\gcd(24,36) = 12$

Common divisors of 24, 36: 1, 2, 3, 4, 6, 12

$\gcd(17,22) = 1$

Common divisors of 17, 22: 1

Önemsiz durumlar:

$$\gcd(m, 1) = 1$$

$$m \neq 0 \Rightarrow \gcd(m, 0) = m$$

Theorem: If $a = b \cdot q + r$ (a/b) $0 \leq r < b$
then $\gcd(a,b) = \gcd(b,r)$

Proof:

$$d \mid a \\ d \mid b$$ ⇒ $$a = ds \\ b = dt$$ ⇒ $$r = d(s - tq) \\ b = dt$$ ⇒ $$d \mid r \\ d \mid b$$

Thus, (a,b) and (b,r) have
the same set of common divisors

End of proof

divisions	$a = r_0$		$b = r_1$	remainder
r_0 / r_1	r_0	$=$	$r_1 q_1 + r_2$	$0 < r_2 < r_1$
r_1 / r_2	r_1	$=$	$r_2 q_2 + r_3$	$0 < r_3 < r_2$
$\vdots$	$\vdots$		$\vdots$	$\vdots$
r_{n-2} / r_{n-1}	r_{n-2}	$=$	$r_{n-1} q_{n-1} + r_n$	$0 < r_n < r_{n-1}$
r_{n-1} / r_n	r_{n-1}	$=$	$r_n q_n + 0$	

first zero

result

$$\gcd(a,b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \cdots$$
$$= \gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$$

$a = 662 \quad b = 414$

662	$=$	$414 \cdot 1 + 248$	$r_2 = 248 < 414 = r_1$
414	$=$	$248 \cdot 1 + 166$	$r_3 = 166 < 248 = r_2$
248	$=$	$166 \cdot 1 + 82$	$r_4 = 82 < 166 = r_3$
166	$=$	$82 \cdot 2 + 2$	$r_5 = 2 < r_4 = 82$
82	$=$	$2 \cdot 41 + 0$	

result

$$\gcd(662,414) = \gcd(414,248) = \gcd(248,166)$$
$$= \gcd(166,82) = \gcd(82,2) = \gcd(2,0) = 2$$

$a \quad b$

$r_0 \quad r_1 \quad r_2 \quad r_3 \quad r_4 \quad \cdots \quad r_{n-1} \quad r_n \quad 0$

$r_0 \bmod r_1 = r_2$

$r_1 \bmod r_2 = r_3$

$r_2 \bmod r_3 = r_4$

$r_{n-2} \bmod r_{n-1} = r_n$

$r_{n-1} \bmod r_n = 0$

$$\gcd(a,b) = r_n$$

$a \quad b \quad \quad \quad \quad \quad r_n$

$662 \quad 414 \quad 248 \quad 166 \quad 82 \quad 2 \quad 0$

$662 \bmod 414 = 248$

$414 \bmod 248 = 166$

$248 \bmod 166 = 82$

$166 \bmod 82 = 2$

$82 \bmod 2 = 0$

$$\gcd(a,b) = r_n = 2$$

Azalan sıralama

$a \quad b$

$$r_0 > r_1 > \quad \cdots \quad > r_i > r_{i+1} > r_{i+2} > \quad \cdots \quad > r_n > 0$$

$$r_i \bmod r_{i+1} = r_{i+2}$$

Özellik: $\frac{r_i}{2} > r_{i+2}$

Durum 1: $\frac{r_i}{2} \geq r_{i+1} \Rightarrow \frac{r_i}{2} \geq r_{i+1} > r_{i+2}$

Azalan sıralama

$a \quad b$

$$r_0 > r_1 > \quad \cdots \quad > r_i > r_{i+1} > r_{i+2} > \quad \cdots \quad > r_n > 0$$

$$r_i \bmod r_{i+1} = r_{i+2}$$

Özellik: $\frac{r_i}{2} > r_{i+2}$

Durum 2: $\frac{r_i}{2} < r_{i+1} \Rightarrow r_i - r_{i+1} = r_{i+2} < \frac{r_i}{2}$

Azalan sıralama

$a \quad b$

$$r_0 > r_1 > \quad \cdots \quad > r_i > r_{i+1} > r_{i+2} > \quad \cdots \quad > r_n > 0$$

$$r_i \bmod r_{i+1} = r_{i+2}$$

Özellik: $\frac{r_i}{2} > r_{i+2}$ ⇒ $n \leq 2 \log a$

Euclidian Algorithm

```
gcd(a,b) {
    x ← a
    y ← b
    while (y ≠ 0) {
        r ← x mod y
        x ← y
        y ← r
    }
    return x
}
```

Time complexity: $O(\log a)$ divisions

Aralarında asal sayılar:

If $\gcd(a,b)=1$ then a,b are relatively prime

a and b have no common factors in their prime factorization

Örnek: 21, 22 aralarında asal sayılardır

$$\gcd(21,22)=1$$

$$21=3\cdot 7 \qquad 22=2\cdot 11$$

En küçük ortak kat

$$\operatorname{lcm}(a,b) = \text{smallest positive integer } d \text{ such that } a \mid d \text{ and } b \mid d$$

$$a,b \in Z^+$$

Examples: $\operatorname{lcm}(3,4)=12$

$\operatorname{lcm}(5,10)=10$

Sayılar teorisinin uygulamaları

Doğrusal kombinasyon:

if $a, b \in Z^+$ then there are $s, t \in Z$ such that

$$\gcd(a,b) = sa + tb$$

Örnek: $\gcd(6,14) = 2 = (-2)\cdot 6 + 1\cdot 14$

Doğrusal kombinasyon, Öklid algoritmasının adımlarını tersine çevirerek bulunabilir.

$$\gcd(252,198) = 18 = 4\cdot 252 - 5\cdot 198$$

$$\begin{aligned} 252 &= 1\cdot 198 + 54 \\ 198 &= 3\cdot 54 + 36 \\ 54 &= 1\cdot 36 + 18 \\ 36 &= 2\cdot 18 + 0 \end{aligned}$$

$$\begin{aligned} &\gcd(252,198) = 18 \\ &= 54 - 1\cdot 36 = 54 - 1\cdot(198 - 3\cdot 54) \\ &= 4\cdot 54 - 1\cdot 198 = 4\cdot(252 - 1\cdot 198) - 1\cdot 198 \\ &= 4\cdot 252 - 5\cdot 198 \end{aligned}$$

Doğrusal uygunluk

We want to solve the equation for x

$$a \cdot x \equiv b \pmod{m}$$

$$\Downarrow$$

$$x \equiv ? \pmod{m}$$

Inverse of a: $\bar{a}a \equiv 1 \pmod{m}$

$$\left.\begin{array}{l} a \cdot x \equiv b \pmod{m} \\ \bar{a} \equiv \bar{a} \bmod m \end{array}\right\} \Rightarrow \bar{a}a \cdot x \equiv \bar{a}b \pmod{m}$$

$$\left.\begin{array}{l} \bar{a}a \equiv 1 \pmod{m} \\ x \equiv x \pmod{m} \end{array}\right\} \Rightarrow \bar{a}a \cdot x \equiv 1 \cdot x \pmod{m}$$

$$\Downarrow$$

$$x \equiv \bar{a}b \pmod{m}$$

Theorem: If a and m are relatively prime then the inverse $\bar{a}$ modulo m exists

Proof: $\gcd(a,m) = 1 = sa + tm$

$$\Downarrow$$

$$sa \equiv 1 (\mathrm{mod}\, m)$$

$$\Downarrow$$

$$\bar{a} = s$$

End of proof

Example: solve equation $3x \equiv 4 (\mathrm{mod}\, 7)$

$a = 3, b = 4, m = 7$

3'ün tersi: $\bar{a} = -2$

$\gcd(3,7) = 1 = -2 \cdot 3 + 1 \cdot 7 \Rightarrow -2 \cdot 3 \equiv 1 (\mathrm{mod}\, m)$

$x \equiv \bar{a} b (\mathrm{mod}\, m)$

$x \equiv -2 \cdot 4 (\mathrm{mod}\, 7) \equiv -8 (\mathrm{mod}\, 7) \equiv 6 \,\mathrm{mod}\, 7$

Chinese remainder problem

$m_1, m_2, \ldots, m_n$:pairwise relatively prime

$$x \equiv a_1 (\mathrm{mod}\, m_1)$$
$$x \equiv a_2 (\mathrm{mod}\, m_2)$$
$$\vdots$$
$$x \equiv a_n (\mathrm{mod}\, m_n)$$

Has unique solution for x modulo: $m = m_1, m_2, \ldots, m_n$

$$x (\mathrm{mod}\, m)$$

Unique solution modulo $m = m_1, m_2, \ldots, m_n$:

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$$

$$M_k = \frac{m}{m_k}$$

y_k :inverse of M_k modulo m_k

Explanation: y_k :inverse of M_k modulo m_k

$$M_k = \frac{m}{m_k} \qquad M_k y_k \equiv 1 \bmod m_k$$

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$$

($0 \pmod{m_1}$ for every term except the first)

$$x \equiv a_1 M_1 y_1 \pmod{m_1} \qquad M_{k \neq 1} \equiv 0 \pmod{m_1}$$

$$x \equiv a_1 \pmod{m_1}$$

Similar for any m_j

Example:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

$m = 3 \cdot 5 \cdot 7 = 105$

$M_1 = m/3 = 105/3 = 35 \qquad y_1 = 2$

$M_2 = m/5 = 105/5 = 21 \qquad y_2 = 1$

$M_3 = m/7 = 105/7 = 15 \qquad y_3 = 1$

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$$
$$= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1$$
$$= 233 \equiv 23 (\bmod 3 \cdot 5 \cdot 7) \equiv 23 (\bmod 105)$$

An Application of Chinese remainder problem

Perform arithmetic with large numbers using arithmetic modulo small numbers

Example: relatively prime numbers

$$m_1 = 99, \quad m_2 = 98, \quad m_3 = 97, \quad m_4 = 95$$

$$m = 99 \cdot 98 \cdot 97 \cdot 95 = 89{,}403{,}930$$

$$123{,}684 = (33, 8, 9, 89)$$

$$123{,}684 \bmod 99 = 33$$
$$123{,}684 \bmod 98 = 8$$
$$123{,}684 \bmod 97 = 9$$
$$123{,}684 \bmod 95 = 89$$

Any number smaller than m has unique representation

$$123{,}684 = (33, 8, 9, 89)$$

$$+ \quad 413{,}456 = (32, 92, 42, 16)$$

$$(65 \bmod 99, 100 \bmod 98, 51 \bmod 97, 105 \bmod 95)$$

$$537{,}140 = (65, 2, 51, 10)$$

We obtain this by using the Chinese remainder problem solution

Fermat's little theorem:

For any prime p and integer a not divisible by p ($\gcd(a, p) = 1$):

$$a^{p-1} \equiv 1 (\text{mod } p)$$

Example: $2^{340} \equiv 1(\text{mod})341$

$a = 2 \quad p = 341$

Proof:

Property 1:

p does not divide any of:

$$1a, 2a, 3a, \ldots, (p-1)a$$

Explanation:

Suppose p divides ka, $1 \le k \le p-1$

$$\exists s \in Z: \quad ka = sp$$

$\gcd(a, p) = 1$
$1 \le k \le p-1$

Does not have p as prime factor

has p as prime factor

Contradicts fundamental theorem of arithmetic

Property 2:

any pair below is not congruent modulo p:

$$1a, 2a, 3a, \ldots, (p-1)a$$

Explanation:

Suppose $xa \equiv ya \pmod{p}$, $1 \le x < y \le p-1$

$\exists s \in Z : \quad ya = xa + sp$

$(y-x)a = sp$

p divides $(y-x)a$ $\quad 1 \le y-x \le p-1$

Contradicts Property 1

Property 3:

$1a, 2a, 3a, \ldots, (p-1)a \equiv 1,2,3, \ldots, (p-1). (mod p)$

Explanation:

From Property 2

$$1a \equiv x_1 \pmod{p}, \quad 1 \le x_1 \le p-1$$
$$2a \equiv x_2 \pmod{p}, \quad 1 \le x_2 \le p-1$$
$$\vdots$$
$$(p-1)a \equiv x_{p-1} \pmod{p}, \quad 1 \le x_{p-1} \le p-1$$

$$x_i \neq x_j \qquad 1 \le i < j \le p-1$$

$$\Downarrow$$

$$x_1 \cdot x_2 \cdot x_3 \cdots x_{p-1} = 1 \cdot 2 \cdot 3 \cdots (p-1)$$

$$\Downarrow$$

$$1a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$

Property 4:

$$(p-1)!\, a^{(p-1)} \equiv (p-1)! \,(mod p)$$

(follows directly from property 3)

Property 5:

$$a^{(p-1)} \equiv 1 (mod p)$$

Explanation:

from Property 4:

$$(p-1)!\,a^{(p-1)} \equiv (p-1)! \pmod{p}$$

p does not divide $(p-1)!$

$\gcd(p,(p-1)!) = 1$

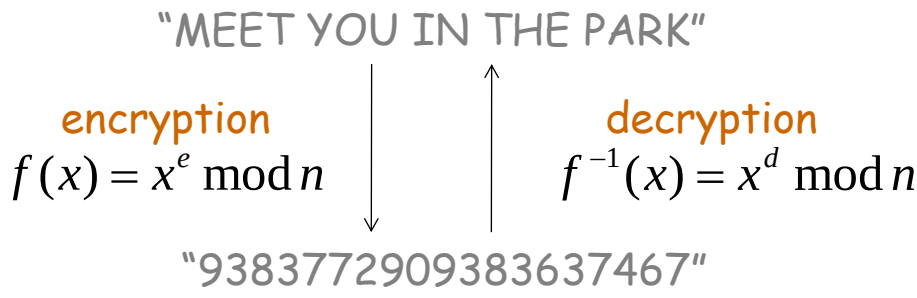
$\overline{(p-1)!} \pmod{p}$ exists

Multiply both sides with: $\overline{(p-1)!}$

$$a^{(p-1)} \equiv 1 \pmod{p}$$

End of Proof

RSA (Rivest-Shamir-Adleman) cryptosystem



$n = p \cdot q$

Large primes

n, e are public keys

p, q, d are private keys

Encryption example: $p = 43 \quad q = 59 \quad e = 13$

$$n = p \cdot q = 2537$$

$$\gcd(e, (p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1$$

Message to encrypt: "STOP"

Translate to equivalent numbers

"18 19 14 15"

Group into blocks of two numbers

"1819 1415"

Apply encryption function to each block

"1819 1415"

$$f(x) = x^e \bmod n$$

$$= x^{13} \bmod 2537$$

Encrypted message: "2081 2182"

$$f(1819) = 1819^{13} \bmod 2537 = 2081$$

$$f(1415) = 1415^{13} \bmod 2537 = 2182$$

Message decryption

M :an original block of the message

"1819 1415"

"2081 2182"

C :respective encrypted block

$$C \equiv M^e \pmod n$$

We want to find M by knowing C, p, q, e

d :inverse of e modulo $(p-1)(q-1)$

$$de \equiv 1 (\mathrm{mod}(p-1)(q-1))$$

by definition of congruent

$$de = 1 + k(p-1)(q-1)$$

Inverse exists because $\gcd(e,(p-1)(q-1)) = 1$

$$\gcd(e,(p-1)(q-1)) = 1 = se + t(p-1)(q-1) \equiv se \bmod (p-1)(q-1)$$

$$d = s$$

$$C \equiv M^e (\mathrm{mod}\, n)$$

$$C^d \equiv \left(M^e\right)^d (\mathrm{mod}\, n)$$

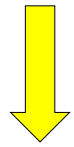
$de = 1 + k(p-1)(q-1)$

$$C^d \equiv M^{de} \equiv M^{1+k(p-1)(q-1)} (\mathrm{mod}\, n)$$

Very likely it holds $\gcd(M, p) = 1$

(because p is a large prime and M is small)

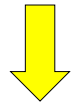
$$\gcd(M, p) = 1$$



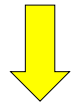
By Fermat's little theorem

$$M^{p-1} \equiv 1 (\mathrm{mod}\ p)$$

$$M^{p-1} \equiv 1 (\mathrm{mod}\ p)$$

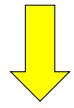


$$\left(M^{p-1}\right)^{k(q-1)} \equiv 1^{k(q-1)} \equiv 1 (\mathrm{mod}\ p)$$



$$M \equiv M (\mathrm{mod}\ p)$$

$$M \cdot \left(M^{p-1}\right)^{k(q-1)} \equiv M \cdot 1 (\mathrm{mod}\ p)$$



$$M^{1+k(p-1)(q-1)} \equiv M (\mathrm{mod}\ p)$$

We showed:

$$M^{1+k(p-1)(q-1)} \equiv M \pmod{p}$$

By symmetry, when replacing p with q :

$$M^{1+k(p-1)(q-1)} \equiv M \pmod{q}$$

By the Chinese remainder problem:

$$M^{1+k(p-1)(q-1)} \equiv M \pmod{pq} \equiv M \pmod{n}$$

We showed:

$$C^d \equiv M^{1+k(p-1)(q-1)} \pmod{n}$$

$$M^{1+k(p-1)(q-1)} \equiv M \pmod{n}$$

$$\Rightarrow C^d \equiv M \pmod{n}$$

In other words:

$$M = C^d \bmod n$$

Decryption example: $p = 43 \quad q = 59 \quad e = 13$

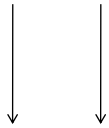
$$n = p \cdot q = 2537$$

$$\gcd(e, (p-1)(q-1)) = \gcd(13, 42 \cdot 58) = 1$$

We can compute: $d = 937$

"2081 2182" $\quad f^{-1}(C) = C^d \bmod n$

$2081^{937} \bmod 2537 = 1819$ $\quad$ $2182^{937} \bmod 2537 = 1415$



"1819 1415"

"18 19 14 15" = "STOP"