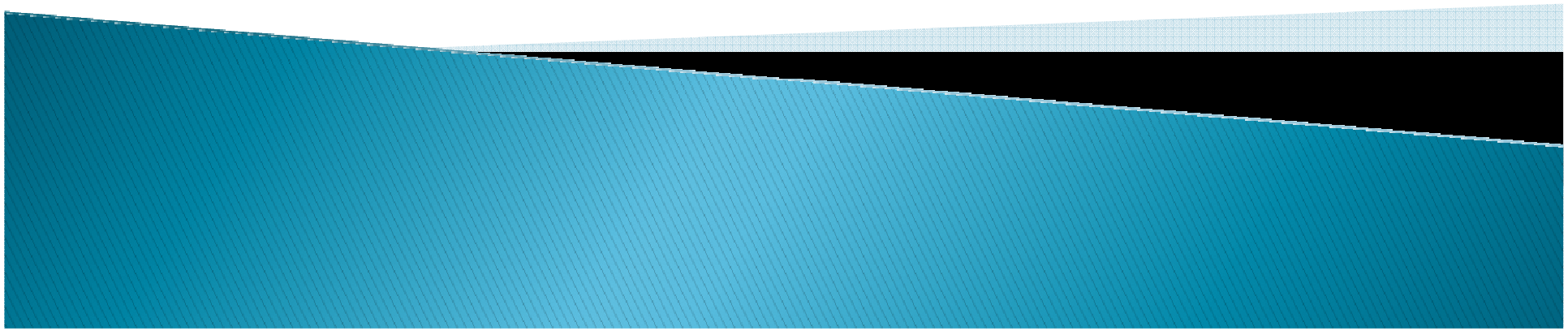
# Teorija brojeva i Linearna algebra

Natjecateljsko programiranje

Luka Kalinovčić, kalinovcic@gmail.com



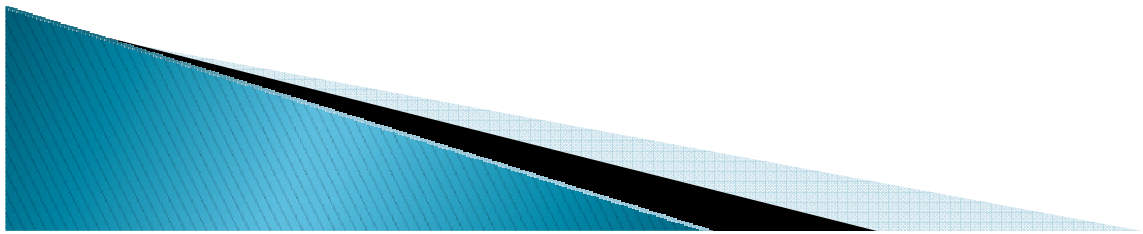
# Modularna aritmetika

- Osnove
- Domaća zadaća

# Osnove

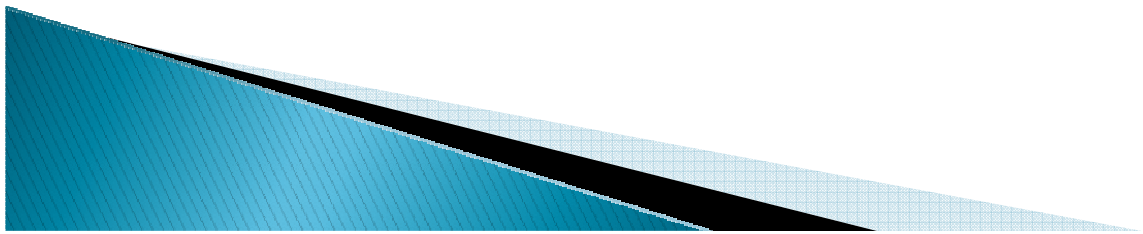
- $(A+B) \bmod M \equiv ((A \bmod M)+(B \bmod M)) \bmod M$
  - $(4+8) \bmod 3 = (1+2) \bmod 3 = 3 \bmod 3 = 0$
- $(A-B) \bmod M \equiv ((A \bmod M)-(B \bmod M)) \bmod M$
  - $(4-8) \bmod 3 = (1-2) \bmod 3 = -1 \bmod 3 = 2$
- $(A \cdot B) \bmod M \equiv ((A \bmod M) \cdot (B \bmod M)) \bmod M$
  - $(4 \cdot 8) \bmod 3 = (1 \cdot 2) \bmod 3 = 2 \bmod 3 = 2$

- $(A/B) \bmod M \equiv ???$



# Osnove

- $(A/B) \bmod M \equiv ???$
- Neka je P prost broj
- $(A/B) \bmod P \equiv (A \cdot B^{-1}) \bmod P$
- $x^{P-1} \bmod P \equiv 1$
- $(x \cdot x^{P-2}) \bmod P \equiv 1$
- $x^{P-2} \equiv x^{-1}$
  - $x^{P-2}$ je modularni inverz broja x (modulo P)!
- $(A/B) \bmod P \equiv (A \cdot B^{P-2}) \bmod P$



# Domaća zadaća

- Lagano

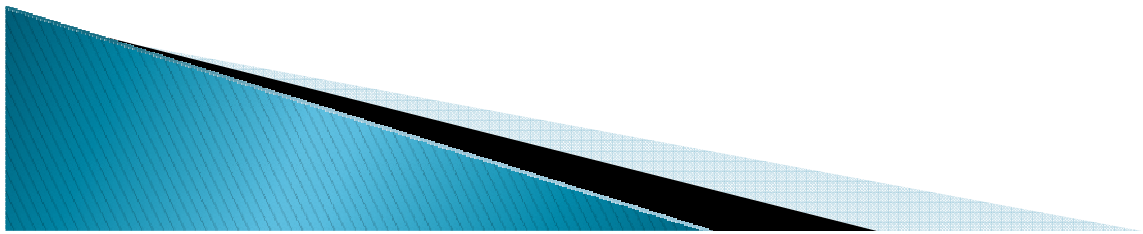
```
MOD = 31337;
x1 = A % MOD;
x2 = B % MOD;
for( int i = 0; i < K-2; ++i ) {
    int x3 = ((long long)C*A +
              (long long)D*B +
                          E) % MOD;
    x1 = x2;
    x2 = x3;
}
```

# Domaća zadaća

- Vlakić
- Permutacije s ponavljanjima:

$$\frac{(A+B+C)!}{A!B!C!} \bmod 24 \cdot 60$$

- Dijeljenje! Kako izračunati?



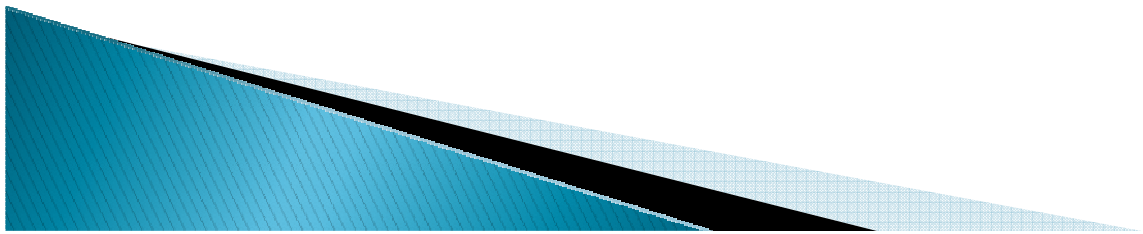
# Domaća zadaća

- Zapisati brojnik i nazivnik kao umnožak faktora.
- Pokratiti sve što se može.
- Kako znamo da je rješenje cijeli broj, sigurno ćemo sve brojeve u nazivniku pokratiti.
- Pomnožiti brojeve u brojniku

$$\frac{(2+3+3)!}{2!3!3!} = \frac{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8}{1\cdot 2\cdot 1\cdot 2\cdot 3\cdot 1\cdot 2\cdot 3}$$

# Domaća zadaća

```
ret = 1;
for( int i = 0; i < A+B+C; ++i ) {
    for( int j = 0; j < A+B+C; ++j ) {
        int g = gcd( gore[i], dole[j] );
        gore[i] /= g;
        dole[j] /= g;
    }
    ret = (ret * gore[i]) % (24*60);
}
```

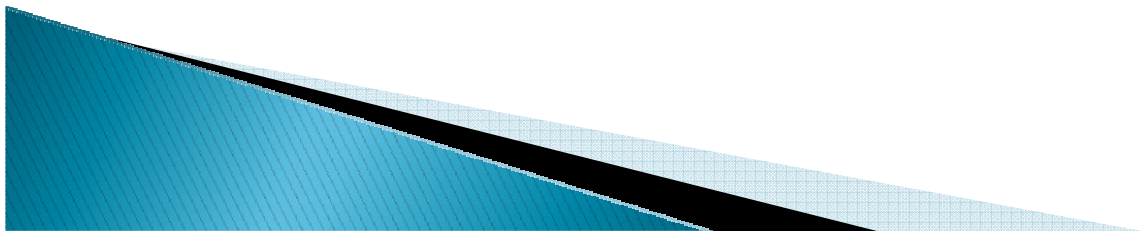


# Modularna aritmetika

- Brzo potenciranje
  Geometrijski niz

# Brzo potenciranje

- $(A^N) \bmod M \equiv ???$
- Rekurzivna metoda
- $A^{2009} = A \cdot A^{2008}$
- $A^{2008} = A^{1004} \cdot A^{1004}$
- $A^{1004} = A^{502} \cdot A^{502}$
- $A^{502} = A^{251} \cdot A^{251}$
- $A^{251} = A \cdot A^{250}$
- ...
- Složenost O(log N)



# Brzo potenciranje

- Iterativna metoda
- $A^{2009} =$

$$A^{1024} \cdot A^{512} \cdot A^{256} \cdot A^{128} \cdot A^{64} \cdot A^{16} \cdot A^{8} \cdot A^{1}$$

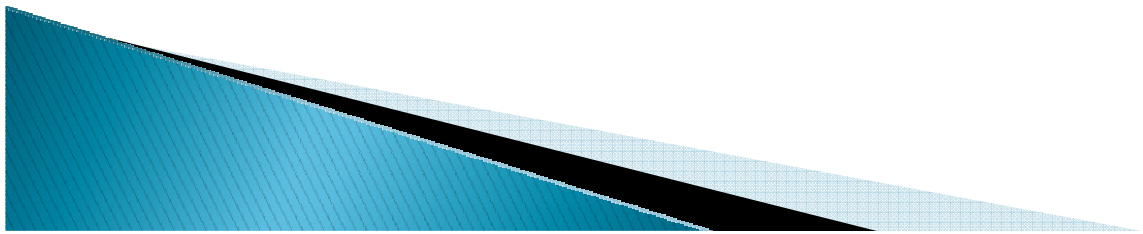
```
ret = 1;
while( n > 0 ) {
    if( n % 2 == 1 ) ret = ret * A % M;
    A = A * A % M;
    n = n / 2;
}
```

OVERFLOW? long long!

- Složenost O(log N), ali brže od rekurzivne metode

# Geometrijski niz

- $(1 + A + A^2 + \ldots + A^N) \bmod M \equiv ???$
- Rekurzivno rješenje
- Za parne N:
  - $1 + A + A^2 + \ldots + A^N = 1 + A \cdot (1 + A + A^2 + \ldots + A^{N-1})$
- Za neparne N:
  - $B = A^2$
  - $1 + A + A^2 + \ldots + A^N =$
  - $= (1 + A^2 + \ldots + A^{N-1}) + (A + A^3 + \ldots + A^N) =$
  - $= (1 + A^2 + \ldots + A^{N-1}) + A \cdot (1 + A^2 + \ldots + A^{N-1}) =$
  - $= (1 + A) \cdot (1 + A^2 + A^4 + \ldots + A^{N-1}) =$
  - $= (1 + A) \cdot (1 + B + B^2 + \ldots + B^{(N-1)/2})$



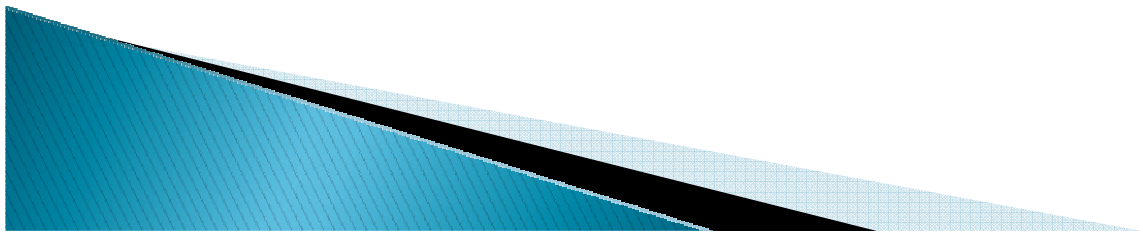
# Greatest common divisor

- Euklidov algoritam
  Prošireni Euklidov algoritam

# Euklidov algoritam

- Primjer: GCD(1683, 873)

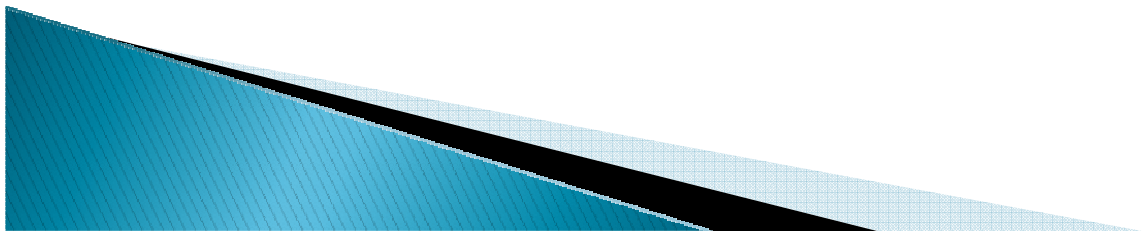
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1683 | 873 | | | | | | |
| | | | | | | | |



# Euklidov algoritam

- Primjer: GCD(1683, 873)

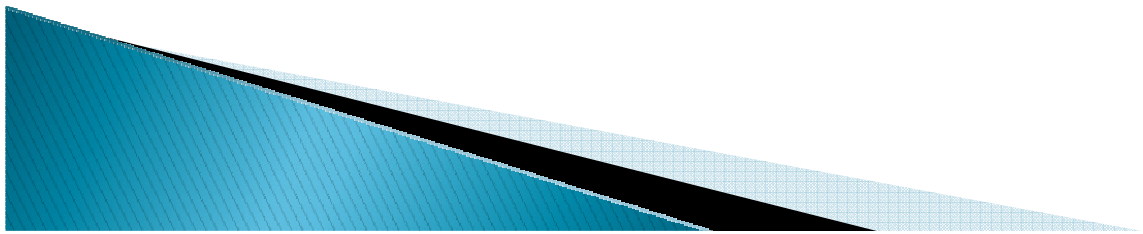
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1683 | 873 | | | | | | |
| | | 1 | | | | | |



# Euklidov algoritam

- Primjer: GCD(1683, 873)

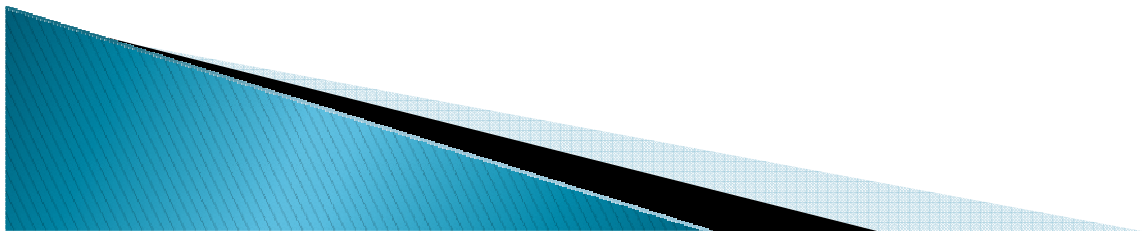
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1683 | 873 | 810 | | | | | |
| | | 1 | | | | | |



# Euklidov algoritam

- Primjer: GCD(1683, 873)

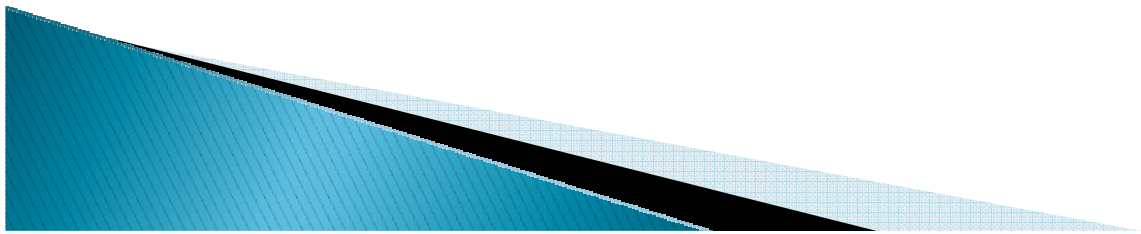
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1683 | 873 | 810 | | | | | |
| | | 1 | 1 | | | | |



# Euklidov algoritam

- Primjer: GCD(1683, 873)

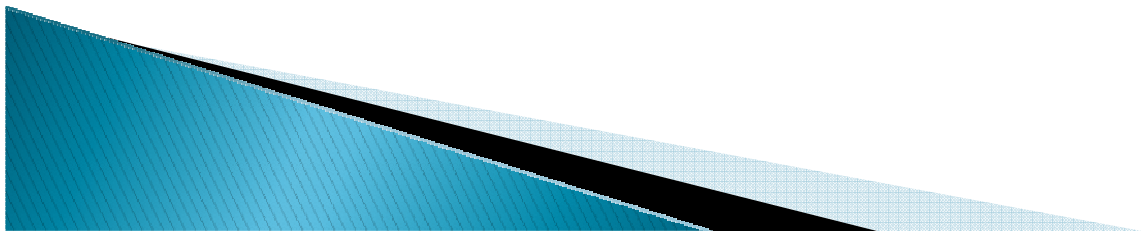
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1683 | 873 | 810 | 63 | | | | |
| | | 1 | 1 | | | | |



# Euklidov algoritam

- Primjer: GCD(1683, 873)

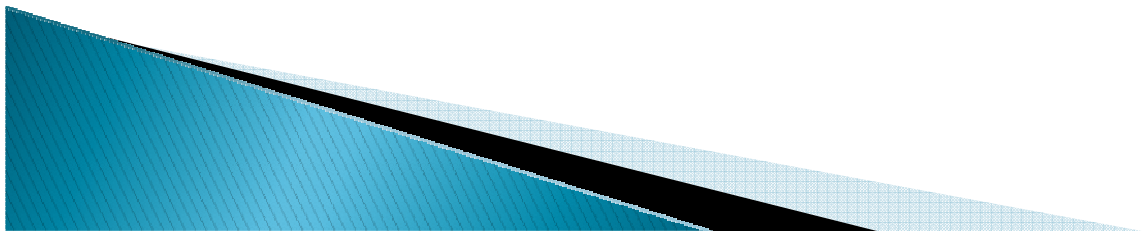
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1683 | 873 | 810 | 63 | | | | |
| | | 1 | 1 | 12 | | | |



# Euklidov algoritam

- Primjer: GCD(1683, 873)

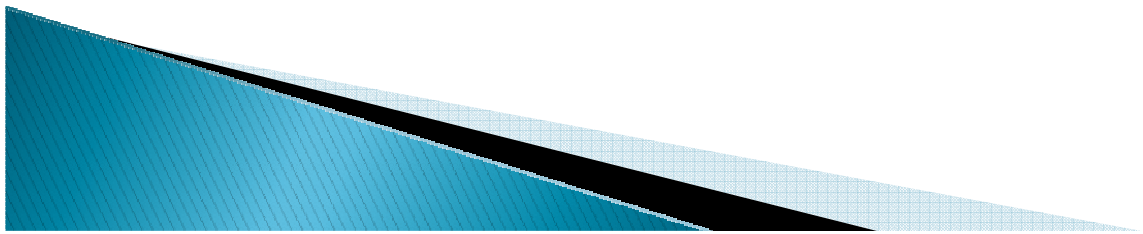
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1683 | 873 | 810 | 63 | 54 | | | |
| | | 1 | 1 | 12 | | | |



# Euklidov algoritam

- Primjer: GCD(1683, 873)

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1683 | 873 | 810 | 63 | 54 | 9 | | |
| | | 1 | 1 | 12 | 1 | | |



# Euklidov algoritam

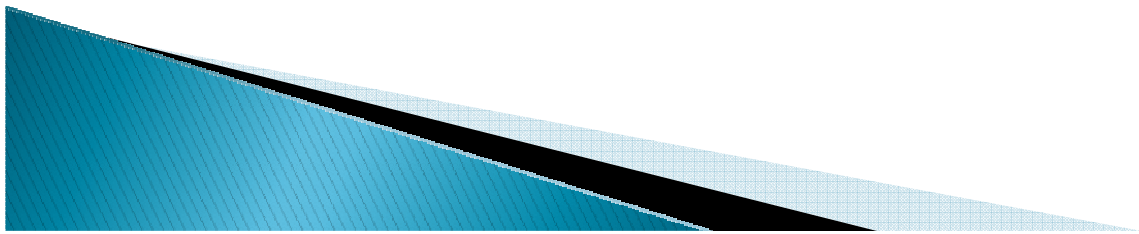
- Primjer: GCD(1683, 873)

| 1683 | 873 | 810 | 63 | 54 | 9 | 0 | |
|---|---|---|---|---|---|---|---|
| | | 1 | 1 | 12 | 1 | 6 | |

Uvjet za prekid

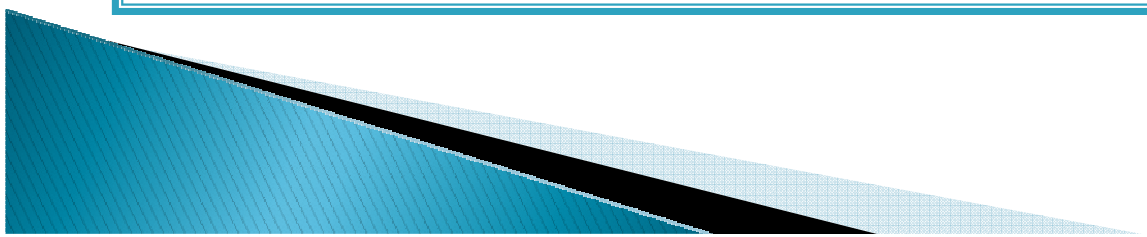
Rezultat!

GCD(1683, 873) = 9



# Euklidov algoritam

```
gcd( A, B ) {
    r1 = A;
    r2 = B;
    while( r2 != 0 ) {
        q = r1 / r2;
        r3 = r1 - q*r2;
        r1 = r2;
        r2 = r3;
    }
    return r1;
}
```



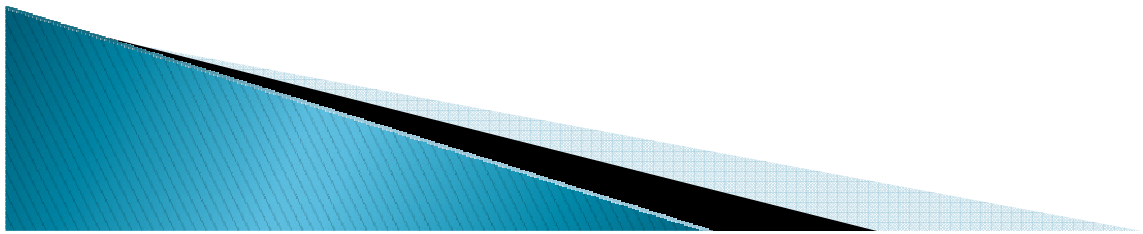
# Euklidov algoritam

- Rekurzivna implementacija

```
int gcd( int A, int B ) {
    if( B == 0 ) return A;
    else return gcd( B, A%B );
}
```

- … ili …

```
return B ? gcd( B, A%B ) : A;
```



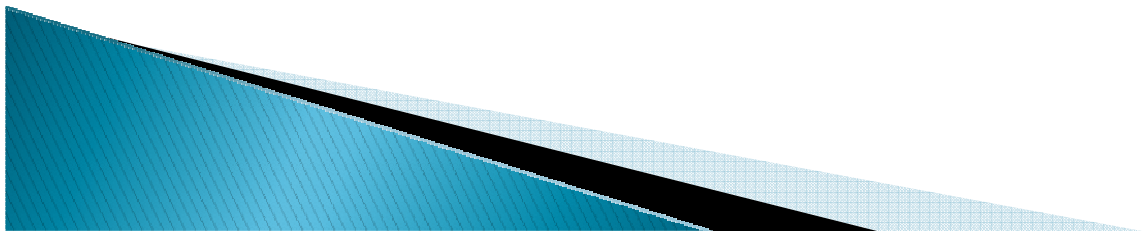
# Prošireni Euklidov algoritam

- Primjer: GCD(1683, 873)

| 1683 | 873 | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| 1 | 0 | | | | | | |
| 0 | 1 | | | | | | |

$1 \cdot 1683 + 0 \cdot 873 = 1683$

$0 \cdot 1683 + 1 \cdot 873 = 873$



# Prošireni Euklidov algoritam

- Primjer: GCD(1683, 873)

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1683 | 873 | 810 | | | | | |
| | | 1 | | | | | |
| 1 | 0 | 1 | | | | | |
| 0 | 1 | −1 | | | | | |

$$1 \cdot 1683 - 1 \cdot 873 = 810$$

# Prošireni Euklidov algoritam

- Primjer: GCD(1683, 873)

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1683 | 873 | 810 | 63 | | | | |
| | | 1 | 1 | | | | |
| 1 | 0 | 1 | −1 | | | | |
| 0 | 1 | −1 | 2 | | | | |

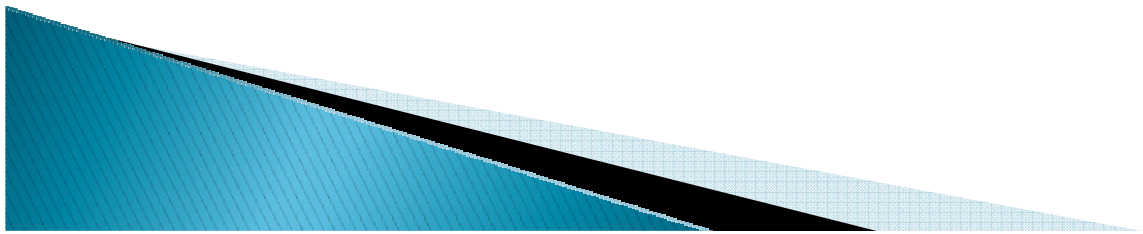
$$-1 \cdot 1683 + 2 \cdot 873 = 63$$

# Prošireni Euklidov algoritam

- Primjer: GCD(1683, 873)

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1683 | 873 | 810 | 63 | 54 | | | |
| | | 1 | 1 | 12 | | | |
| 1 | 0 | 1 | −1 | 13 | | | |
| 0 | 1 | −1 | 2 | −25 | | | |

$$13 \cdot 1683 - 25 \cdot 873 = 54$$

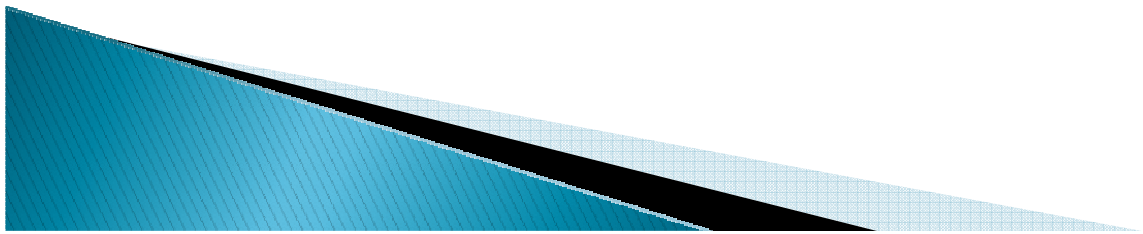


# Prošireni Euklidov algoritam

- Primjer: GCD(1683, 873)

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1683 | 873 | 810 | 63 | 54 | 9 | | |
| | | 1 | 1 | 12 | 1 | | |
| 1 | 0 | 1 | −1 | 13 | −14 | | |
| 0 | 1 | −1 | 2 | −25 | 27 | | |

$$-14 \cdot 1683 + 27 \cdot 873 = 54$$

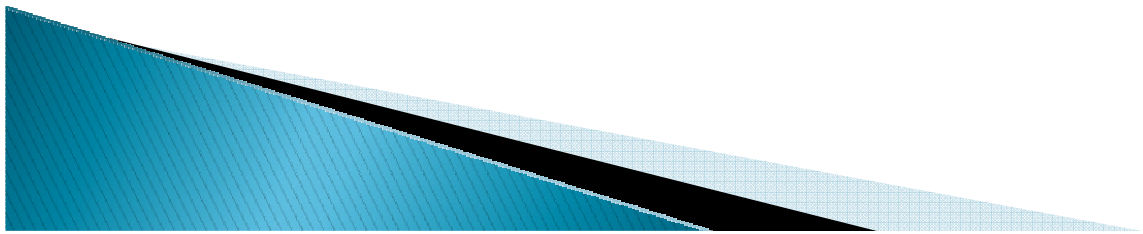


# Prošireni Euklidov algoritam

- Primjer: GCD(1683, 873)

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1683 | 873 | 810 | 63 | 54 | 9 | 0 | |
| | | 1 | 1 | 12 | 1 | 6 | |
| 1 | 0 | 1 | −1 | 13 | −14 | | |
| 0 | 1 | −1 | 2 | −25 | 27 | | |

$$-14 \cdot 1683 + 27 \cdot 873 = 54$$

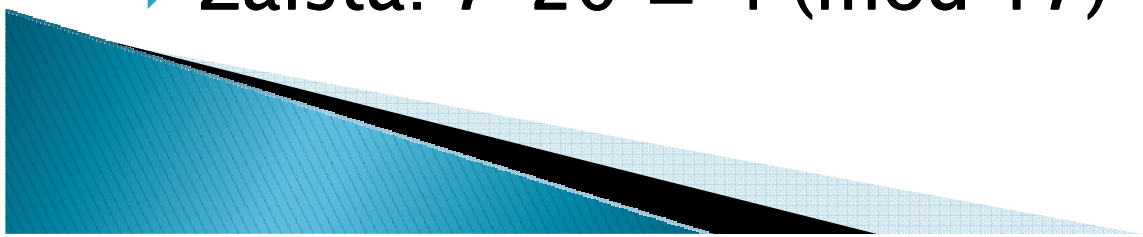


# Prošireni Euklidov algoritam

```
extended_gcd( A, B ) {
    r1 = A; x1 = 1; y1 = 0;
    r2 = B; x2 = 0; y2 = 1;
    while( r2 != 0 ) {
        q = r1 / r2;
        r3 = r1 - q*r2;
        x3 = x1 - q*x2;
        y3 = y1 - q*y2;
        r1 = r2; x1 = x2; y1 = y2;
        r2 = r3; x2 = x3; y2 = y3;
    }
    // vrijedi: x1*A + y1*B == r1
}
```

# Prošireni Euklidov algoritam

- Primjena:
- Rješavanje modularnih jednadžbi:
- $7x \equiv 4 \pmod{17}$
- $7x + 17y = 4$
- Proširenim Euklidovim algoritom nađemo rješenje temeljne jednadžbe $7x' + 17y' = 1$:
  - $7 \cdot 5 + 17 \cdot (-2) = 1$
- Množimo s 4
  - $7 \cdot 20 + 17 \cdot (-8) = 4$
- Zaista: $7 \cdot 20 \equiv 4 \pmod{17}$

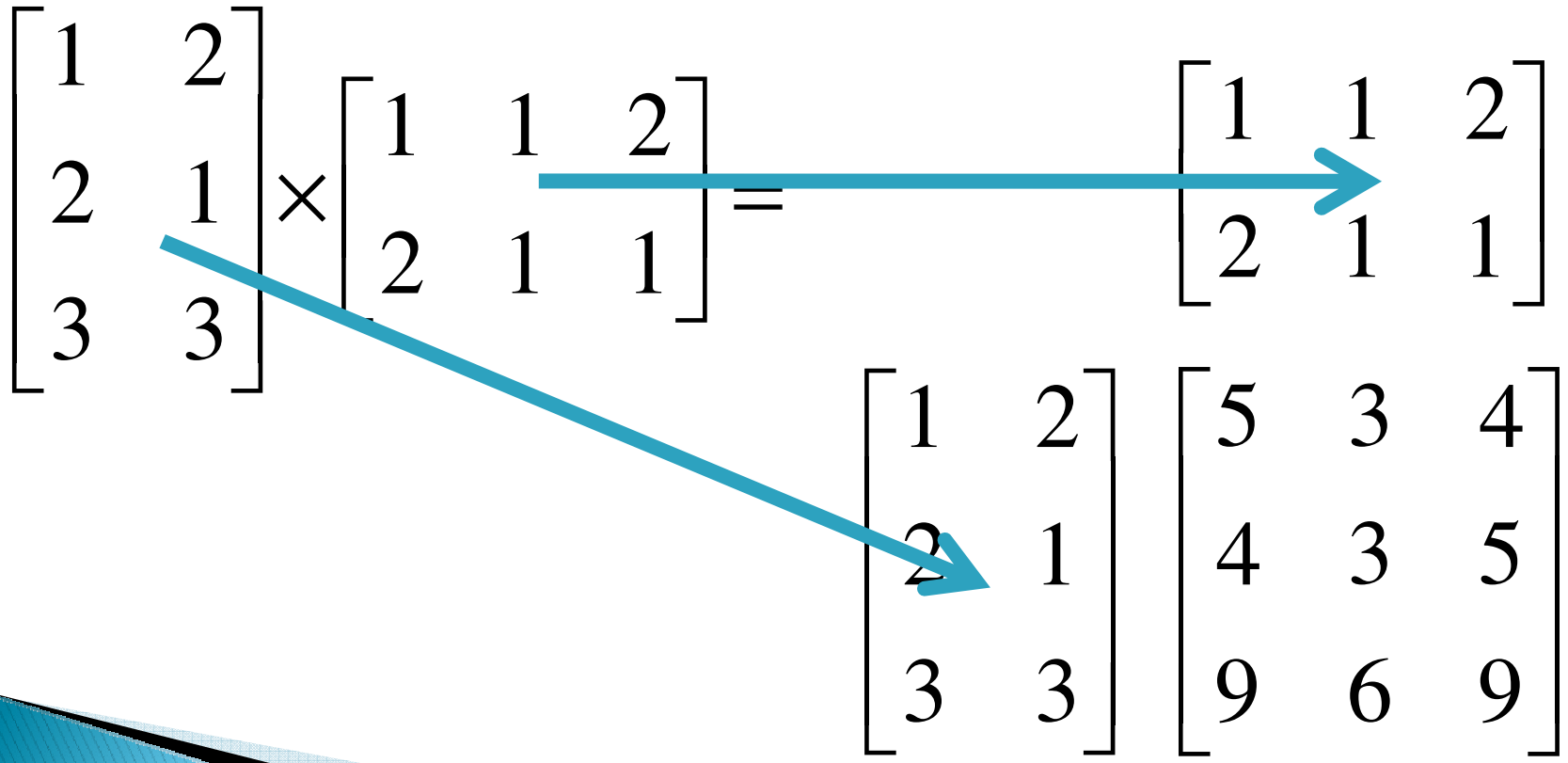


# Matrice

- Množenje matrica
- Linearne diferencijske jednadžbe

# Množenje matrica

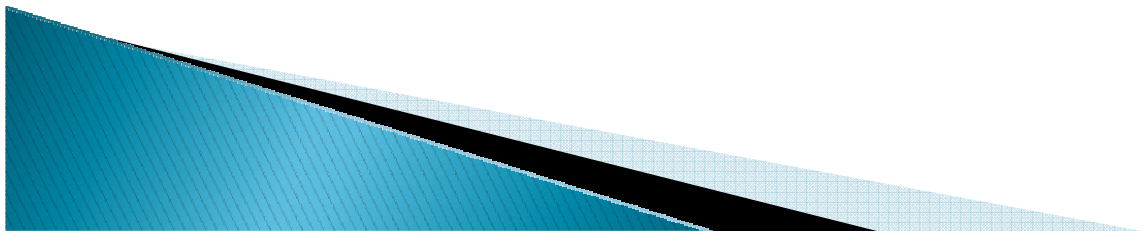
$$C(i,j) = \sum A(i,k) \cdot B(k,j)$$



# Linearne diferencijske jednadžbe

- Fibonaccijev niz:
  - F[0] = 1
  - F[1] = 1
  - F[k] = F[k–1] + F[k–2]
- Cilj je pronaći matricu koja će vektor $\begin{bmatrix} F[k-2] \\ F[k-1] \end{bmatrix}$

transformirati u vektor $\begin{bmatrix} F[k-1] \\ F[k] \end{bmatrix}$

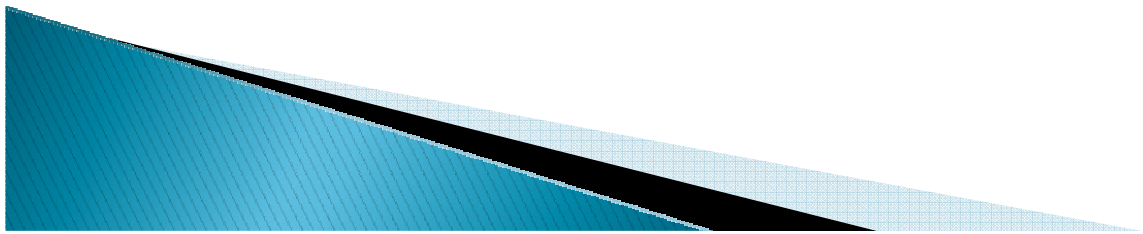


# Linearne diferencijske jednadžbe

- Fibonaccijev niz:
  - F[0] = 1
  - F[1] = 1
  - F[k] = F[k-1] + F[k-2]

$$\begin{bmatrix} F[k-2] \\ F[k-1] \end{bmatrix}$$

$$\begin{bmatrix} ? & ? \\ ? & ? \end{bmatrix} \begin{bmatrix} F[k-1] \\ F[k] \end{bmatrix}$$

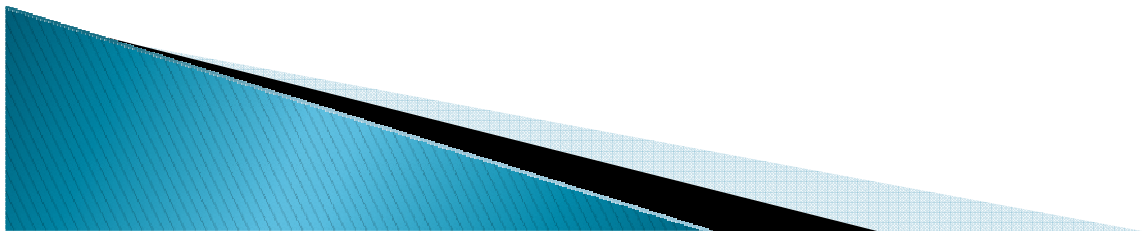


# Linearne diferencijske jednadžbe

- Fibonaccijev niz:
  - F[0] = 1
  - F[1] = 1
  - F[k] = F[k-1] + F[k-2]

$$\begin{bmatrix} F[k-2] \\ F[k-1] \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} F[k-1] \\ F[k] \end{bmatrix}$$

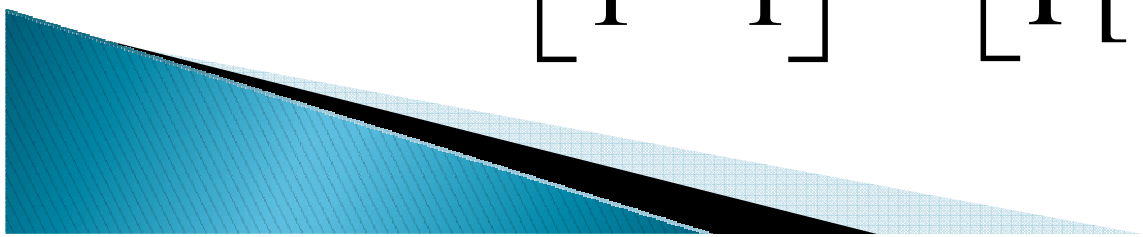


# Linearne diferencijske jednadžbe

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \times \begin{bmatrix} F[0] \\ F[1] \end{bmatrix} = \begin{bmatrix} F[1] \\ F[2] \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \times \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \times \begin{bmatrix} F[0] \\ F[1] \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \times \begin{bmatrix} F[1] \\ F[2] \end{bmatrix} = \begin{bmatrix} F[2] \\ F[3] \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^{k} \times \begin{bmatrix} F[0] \\ F[1] \end{bmatrix} = \begin{bmatrix} F[k] \\ F[k+1] \end{bmatrix}$$



# Linearne diferencijske jednadžbe

- Primjer 1:
  - F[0] = 0
  - F[1] = 0
  - F[k] = 2·F[k−1] − F[k−2] + 5

$$\begin{bmatrix} F[k-2] \\ F[k-1] \end{bmatrix}$$

$$\begin{bmatrix} ? & ? \\ ? & ? \end{bmatrix} \begin{bmatrix} F[k-1] \\ F[k] \end{bmatrix}$$

Trebamo u stanje dodati konstantu 1!

# Linearne diferencijske jednadžbe

- Primjer 1:
  - F[0] = 0
  - F[1] = 0
  - F[k] = 2·F[k−1] − F[k−2] + 5

$$\begin{bmatrix} F[k-2] \\ F[k-1] \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} ? & ? & ? \\ ? & ? & ? \\ ? & ? & ? \end{bmatrix} \begin{bmatrix} F[k-1] \\ F[k] \\ 1 \end{bmatrix}$$

# Linearne diferencijske jednadžbe

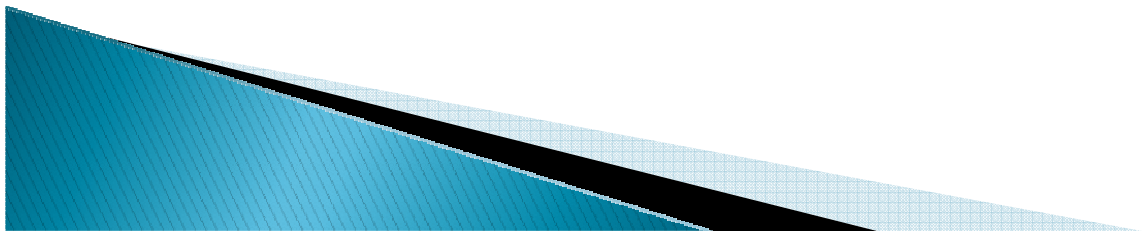
- Primjer 1:
  - F[0] = 0
  - F[1] = 0
  - F[k] = 2·F[k−1] − F[k−2] + 5

$$\begin{bmatrix} F[k-2] \\ F[k-1] \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 & 0 \\ -1 & 2 & 5 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} F[k-1] \\ F[k] \\ 1 \end{bmatrix}$$

# Linearne diferencijske jednadžbe

- Primjer 2:
  - $F[0] = 0$
  - $F[1] = 0$
  - $F[k] = 2 \cdot F[k-1] - F[k-2] + 5$
  - Izračunajte $F[0] + F[1] + F[2] + \ldots + F[n]$
- Rješenje: niz S pamti sumu
  - $S[0] = 0$
  - $S[k] = S[k-1] + F[k]$
- $S[k] = S[k-1] + 2 \cdot F[k-1] - F[k-2] + 5$



# Linearne diferencijske jednadžbe

- Primjer 2:
  - F[0] = 0
  - F[1] = 0
  - F[k] = 2·F[k–1] – F[k–2] + 5
  - S[k] = S[k–1] + 2·F[k–1] – F[k–2] + 5
- Vektor stanja:

$$\begin{bmatrix} F[k-2] \\ F[k-1] \\ S[k-1] \\ 1 \end{bmatrix}$$

# Linearne diferencijske jednadžbe

- Primjer 2:
  - F[0] = 0
  - F[1] = 0
  - F[k] = 2·F[k−1] − F[k−2] + 5
  - S[k] = S[k−1] + 2·F[k−1] − F[k−2] + 5

$$\begin{bmatrix} F[k-2] \\ F[k-1] \\ S[k-1] \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 2 & 0 & 5 \\ -1 & 2 & 1 & 5 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} F[k-1] \\ F[k] \\ S[k] \\ 1 \end{bmatrix}$$