

# Ασφάλεια Υπολογιστικών Συστημάτων

## 7ο Εξάμηνο

Επιλεκτικά Θέματα Θεωρίας Αριθμών

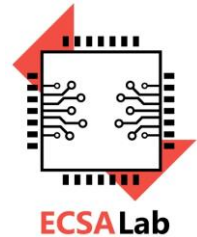
**Διδάσκων** : Δρ. Παρασκευάς Κίτσος

<https://ecsalab.ece.uop.gr/>

Καθηγητής

Εργαστήριο Ηλεκτρονικών Κυκλωμάτων, Συστημάτων  
και Εφαρμογών (ECSA Lab.)

e-mail: [kitsos@uop.gr](mailto:kitsos@uop.gr)



# ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ

- Αναφερόμαστε στο σύνολο των ακεραίων  $\mathbf{Z}=\{\dots,-2, -1, 0, 1, 2, \dots\}$  και στο σύνολο των φυσικών αριθμών  $\mathbf{N}=\{0, 1, 2, \dots\}$
- Έστω δύο ακέραιοι  $a$  και  $d$ . Όταν ο  $d$  διαιρεί τον  $a$ , τότε  $a=kd$  όπου  $k$  ακέραιος και συμβολίζουμε  $d|a$
- Ο  $a$  λέμε ότι είναι **πολλαπλάσιο** του  $d$
- Αν  $a>d$  και  $d|a$  τότε  $|d| \leq a$
- Αν ο  $a$  είναι μη μηδενικός τότε ισχύει,  $1 \leq d \leq |a|$
- Κάθε ακέραιος  $a$  έχει τους **τετριμμένους διαιρέτες**, τους 1 και  $a$
- Οι μη τετριμμένοι διαιρέτες ονομάζονται **παράγοντες** του  $a$ .  
Π.χ. Παράγοντες του 12 είναι οι 2, 3, 4, 6
- Αν ο ακέραιος  $a>1$  έχει μόνο τετριμμένους διαιρέτες (1,  $a$ ) ονομάζεται **πρώτος αριθμός**
- Ένας ακέραιος  $a>1$  που δεν είναι πρώτος ονομάζεται **σύνθετος αριθμός**

# ΘΕΩΡΗΜΑ ΤΗΣ ΔΙΑΙΡΕΣΗΣ

- Ορίζουμε την συνάρτηση «mod» (modulo ) όπως παρακάτω

$$a \bmod n = \begin{cases} a, & \text{αν } n = 0 \\ a - \lfloor a/n \rfloor n, & \text{διαφορετικά} \end{cases}$$

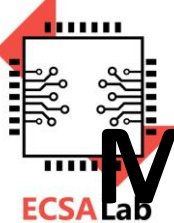
όπου ορίζουμε το **Πηλίκο**  $q$  ( $= a \operatorname{div} n$ ) =  $\lfloor a/n \rfloor$

$\lfloor x \rfloor$  είναι ο μεγαλύτερος ακέραιος

που είναι μικρότερος ή ίσος με τον  $x$

# ΔΙΑΙΡΕΤΟΤΗΤΑ

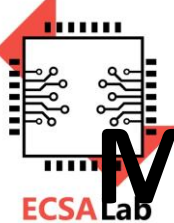
- Αν  $d \mid a$  και  $d \mid b$  τότε ο  $d$  είναι ένας κοινός διαιρέτης των  $a$  και  $b$
- Ο 1 είναι κοινός διαιρέτης δύο οποιωνδήποτε ακεραίων
- Αν  $d \mid a$  και  $d \mid b$  τότε  $d \mid (ax+by)$  για κάθε ακέραιο  $x, y$
- Αν  $a \mid b$  τότε  $|a| \leq |b|$  ή  $b=0$
- Αν  $a \mid b$  και  $b \mid a$  τότε  $a = \pm b$



# ΜΕΓΙΣΤΟΣ ΚΟΙΝΟΣ ΔΙΑΙΡΕΤΗΣ (1/3)

Ο μέγιστος κοινός διαιρέτης (common great divisor) δύο ακεραίων  $a$  και  $b$  -  $\text{gcd}(a, b)$  - που δεν είναι μηδέν είναι ο μεγαλύτερος από τους κοινούς διαιρέτες των  $a$  και  $b$ . π.χ.  
 $\text{gcd}(7, 11) = 1$ ,  $\text{gcd}(0, 6) = 6$ ,  $\text{gcd}(0, 0) = 0$

- Αν  $a \mid b$  τότε  $\text{gcd}(a, b) = a$ .
- Αν  $a$  και  $b$  είναι μη μηδενικοί ακέραιοι, τότε
$$1 \leq \text{gcd}(a, b) \leq \min(|a|, |b|)$$
- $\text{gcd}(a, b) = \text{gcd}(b, a)$
- $\text{gcd}(a, b) = \text{gcd}(-a, b)$
- $\text{gcd}(a, b) = \text{gcd}(|a|, |b|)$
- $\text{gcd}(a, 0) = |a|$
- $\text{gcd}(a, ka) = |a|$  για κάθε ακέραιο  $k$
- $\text{gcd}(a, n) = \text{gcd}(a+kn, n)$  για κάθε ακέραιο  $k, n$

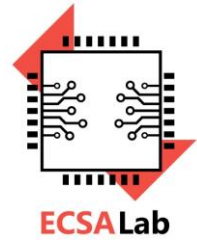


# ΜΕΓΙΣΤΟΣ ΚΟΙΝΟΣ ΔΙΑΙΡΕΤΗΣ (2/3)

- Αν δύο ακέραιοι  $a$  και  $b$  έχουν μοναδικό κοινό διαιρέτη τον 1, δηλ. αν  $\gcd(a, b)=1$ , τότε λέγονται πρώτοι μεταξύ τους ή σχετικά (αμοιβαία) πρώτοι  
π.χ. οι αριθμοί 8 και 15 είναι σχετικά πρώτοι αφού
  - οι διαιρέτες του 8 είναι 1, 2, 4 και 8
  - οι διαιρέτες του 15 είναι 1, 3, 5 και 15
  - Ο μόνος κοινός διαιρέτης είναι ο 1

# ΜΕΓΙΣΤΟΣ ΚΟΙΝΟΣ ΔΙΑΙΡΕΤΗΣ (3/3)

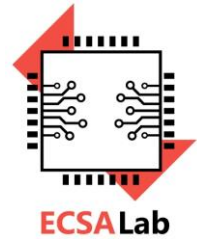
- Αν για τους ακέραιους  $a$ ,  $b$  και  $p$  ισχύει  $\gcd(a, p) = 1$  και  $\gcd(b, p) = 1$  τότε  $\gcd(ab, p) = 1$
- Για όλους τους πρώτους  $p$  και τους ακεραίους  $a$ ,  $b$  αν  $p \mid ab$  τότε  $p \mid a$  ή  $p \mid b$
- Ένας σύνθετος  $a$  μπορεί να γραφεί κατά μοναδικό τρόπο ως ένα γινόμενο της μορφής  $a = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$ , όπου οι  $p_1, p_2, \dots, p_s$  είναι πρώτοι,  $p_1 < p_2 < \dots < p_s$  και οι  $e_1, e_2, \dots, e_s$  είναι θετικοί ακέραιοι



# ΑΛΓΟΡΙΘΜΟΣ ΤΟΥ ΕΥΚΛΕΙΔΗ

- Για οποιονδήποτε μη αρνητικό ακέραιο  $a$  και οποιονδήποτε θετικό ακέραιο  $b$ ,  
 **$\gcd(a, b) = \gcd(b, a \bmod b)$**





# ΑΝΕΠΤΥΓΜΕΝΗ ΜΟΡΦΗ

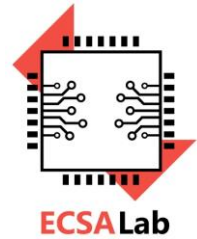
## ΑΛΓΟΡΙΘΜΟΥ ΤΟΥ ΕΥΚΛΕΙΔΗ...

- Αν  $\gcd(a, b)$  με  $a, b$  ακέραιοι (όχι και οι δύο μηδέν) τότε υπάρχουν ακέραιοι αριθμοί  $x, y$  τέτοιοι ώστε  $d = \gcd(a, b) = xa + yb$
- Η ανεπτυγμένη μορφή του αλγορίθμου Ευκλείδη στην αναδρομική της έκδοση δίνεται από τον παρακάτω ψευδοκώδικα

### Ευκλείδης2( $a, b$ )

```
1  if  $b = 0$ 
2    then return ( $a, 1, 0$ )
3  ( $d', x', y'$ )  $\leftarrow$  Ευκλείδης2( $b, a \bmod b$ )
4  ( $d, x, y$ )  $\leftarrow$  ( $d', y', x' - \lfloor a/b \rfloor y'$ )
5  return ( $d, x, y$ )
```

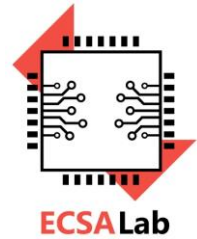
- Ο αλγόριθμος έχει σαν είσοδο ένα ζεύγος μη αρνητικών ακεραίων  $a, b$  και επιστρέφει στην έξοδο μια τριάδα αριθμών της μορφής  $(d, x, y)$  η οποία ικανοποιεί τη σχέση  $d = \gcd(a, b) = xa + yb$



# ...ΑΝΕΠΤΥΓΜΕΝΗ ΜΟΡΦΗ

## ΑΛΓΟΡΙΘΜΟΥ ΤΟΥ ΕΥΚΛΕΙΔΗ

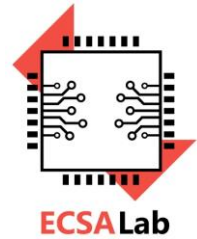
- Αν θέλουμε να εκτελέσουμε τη συνάρτηση Ευκλείδης2(a,b) με  $(a,b)=(14, 11)$  στη πρώτη κλήση της συνάρτησης Ευκλείδης2(14, 11), η συνάρτηση καλεί τον εαυτό της με ορίσματα  $(11, 14 \bmod 11) = (11, 3)$ . Μετά καλεί τον εαυτό της διαδοχικά με  $(a, b)$  τα  $(3, 2)$ ,  $(2, 1)$  και  $(1, 0)$
- Όταν εκτελείται με  $(a,b) = (1, 0)$  αντιμετωπίζει τη συνθήκη «if b = 0» οπότε θέτει  $d \leftarrow a (=1)$ ,  $x \leftarrow -1$ ,  $y \leftarrow 0$
- Συνεχίζει με τις άλλες τιμές των  $(a, b)$



# ΑΝΕΠΤΥΓΜΕΝΗ ΜΟΡΦΗ ΤΟΥ ΕΥΚΛΕΙΔΗ: ΑΣΚΗΣΗ (1/3)

- Βρείτε το  $\gcd(11, 14)$ . Έπειτα χρησιμοποιήστε την ανεπτυγμένη μορφή του αλγορίθμου Ευκλείδη και βρείτε τους ακεραίους  $x$  και  $y$  για τους οποίους ισχύει  $14x + 11y = 1$ .

**Λύση:** Έχουμε  $\gcd(11, 14) = \gcd(11, 14 \bmod 11)$   
 $= \gcd(11, 3) = \gcd(3, 11 \bmod 3) = \gcd(3, 2) =$   
 $\gcd(2, 3 \bmod 2) = \gcd(2, 1) = \gcd(1, 2 \bmod 1) =$   
 $\gcd(1, 0) = 1$

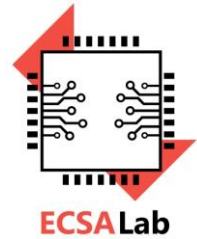


# ΑΝΕΠΤΥΓΜΕΝΗ ΜΟΡΦΗ ΤΟΥ ΕΥΚΛΕΙΔΗ: ΑΣΚΗΣΗ (2/3)

Ευκλείδης2( $a, b$ )

```
1  if  $b = 0$ 
2  then return ( $a, 1, 0$ )
3  ( $d', x', y'$ ) ← Ευκλείδης2( $b, a \bmod b$ )
4  ( $d, x, y$ ) ← ( $d', y', x' - \lfloor a/b \rfloor y'$ )
5  return ( $d, x, y$ )
```

- Έχουμε την εκτέλεση της συνάρτησης Ευκλείδης2( $a, b$ ) με  $(a, b) = (14, 11)$ .
- Στην πρώτη κλήση της Ευκλείδης2(14, 11) η συνάρτηση καλεί τον εαυτό της με όρισμα (11, 3). Μετά καλεί τον εαυτό της διαδοχικά με (3, 2), (2, 1) και (1, 0).
- Όταν εκτελείται με  $(a, b) = (1, 0)$ , έχουμε  $b = 0$  άρα  $d \leftarrow a (=1)$ ,  $x \leftarrow 1$ ,  $y \leftarrow 0$ .
- Για  $(a, b) = (2, 1)$  έχουμε  $y \leftarrow x - \lfloor a/b \rfloor y = 1 - \lfloor 2/1 \rfloor 0 = 1$ ,  $x = 0$
- Για  $(a, b) = (3, 2)$  έχουμε  $y \leftarrow x - \lfloor a/b \rfloor y = 0 - \lfloor 3/2 \rfloor 1 = -1$ ,  $x = 1$
- Για  $(a, b) = (11, 3)$  έχουμε  $y \leftarrow x - \lfloor a/b \rfloor y = 1 - \lfloor 11/3 \rfloor (-1) = 4$ ,  $x = -1$

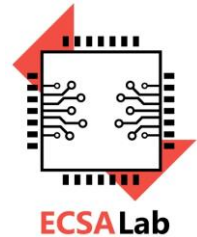


# ΑΝΕΠΤΥΓΜΕΝΗ ΜΟΡΦΗ ΤΟΥ ΕΥΚΛΕΙΔΗ: ΑΣΚΗΣΗ (3/3)

Ευκλείδης2( $a, b$ )

```
1  if  $b = 0$ 
2  then return ( $a, 1, 0$ )
3  ( $d', x', y'$ )  $\leftarrow$  Ευκλείδης2( $b, a \bmod b$ )
4  ( $d, x, y$ )  $\leftarrow$  ( $d', y', x' - \lfloor a/b \rfloor y'$ )
5  return ( $d, x, y$ )
```

- Για  $(a, b) = (14, 11)$  έχουμε  $y \leftarrow x - \lfloor a/b \rfloor y = -1 - \lfloor 14/11 \rfloor 4 = -5, x = 4$ .
- Άρα για  $x = 4$  και  $y = -5$  ισχύει  $d = \gcd(a, b) = ax + by = 14(4) + 11(-5) = 1$



# Η ΣΥΝΑΡΤΗΣΗ $\phi(n)$ ΤΟΥ ΕΥΛΕΡ

- Η συνάρτηση  $\phi(n)$  δηλώνει τον αριθμό των θετικών ακεραίων που είναι μικρότεροι από τον  $n$  και αμοιβαία πρώτοι με τον  $n$ 
  - Αν  $p$  πρώτος τότε,  $\phi(p)=p-1$
  - Αν  $p$  και  $q$  με  $p \neq q$  πρώτοι, τότε το γινόμενο τους είναι  $n = p * q$  και  $\phi(n) = \phi(p*q) = \phi(p)*\phi(q) = (p - 1)*(q - 1)$
  - Αν  $p$  πρώτος και  $k \geq 1$ , τότε  $\phi(p^k)=p^k-p^{k-1}$
  - Αν  $\gcd(a, b)=1$ , τότε  $\phi(ab)=\phi(a)\phi(b)$

# ΘΕΩΡΗΜΑ EULER

- Εάν  $\gcd(a, n)=1$  και  $n>1$  τότε  $a^{\phi(n)} \equiv 1 \pmod{n}$  για κάθε  $a$
- Ο αντίστροφος του  $a$  ( $a^{-1}$ ) είναι ο  $x = a^{\phi(n)-1} \pmod{n}$
- **Παράδειγμα:** Βρείτε τον αντίστροφο του 5 modulo 7
  - Ο 7 είναι πρώτος, άρα  $\phi(7)=7-1=6$ . Και ο αντίστροφος είναι ο  $x=5^{6-1} \pmod{7}=3$

# ΤΕΛΕΣΤΗΣ MODULO

- Ισότητα υπολοίπων
  - $a \bmod n = b \bmod n$  γράφουμε  $a \equiv b \pmod{n}$  και λέμε «ότι ο  $a$  είναι **ισότιμος** ή **ισοϋπόλοιπος** ή **ισοδύναμος** με τον  **$b$ , modulus  $n$** ». Ο θετικός αριθμός  $n$  ονομάζεται **modulus**.
  - $a \equiv b \pmod{n}$  αν οι  $a$  και  $b$  έχουν το ίδιο υπόλοιπο όταν διαιρούνται με τον  $n$ .
  - $a \equiv b \pmod{n}$  αν και μόνο αν  $n \mid (b-a)$ .
  - Αν ο  $a$  δεν είναι **ισοδύναμος** με τον  **$b$ , modulus  $n$**  γράφουμε  $a \not\equiv b \pmod{n}$

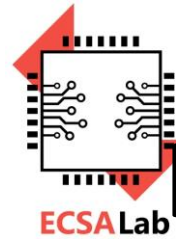


# ΙΔΙΟΤΗΤΕΣ ΤΕΛΕΣΤΗ MODULO

- Για τον τελεστή modulo (modulo operator) ισχύουν τα παρακάτω
  - $a \equiv b \pmod n$  εάν  $n \mid (a - b)$ 
    - π.χ.  $23 \equiv 8 \pmod 5$  αφού  $23 - 8 = 15 = 5 \times 3$ .
    - π.χ.  $-11 \equiv 5 \pmod 8$  αφού  $-11 - 5 = -16 = 8 \times (-2)$
    - π.χ.  $81 \equiv 0 \pmod 27$  αφού  $81 - 0 = 81 = 27 \times 3$
  - $a \equiv b \pmod n$  συνεπάγεται ότι  $b \equiv a \pmod n$ 
    - π.χ.  $10 \equiv 20 \pmod 10$  και  $20 \equiv 10 \pmod 10$
  - $a \equiv b \pmod n$  και  $b \equiv c \pmod n$  συνεπάγεται ότι  $a \equiv c \pmod n$ 
    - π.χ.  $10 \equiv 20 \pmod 10$  και  $20 \equiv 50 \pmod 10$  τότε  $10 \equiv 50 \pmod 10$

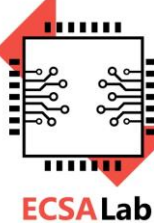
# MODULAR ΑΡΙΘΜΗΤΙΚΗ

- Μία πολύ σημαντική τεχνική με αριθμητικές πράξεις με βάση το mod είναι η modular αριθμητική mod (modular arithmetic). Ισχύουν οι ιδιότητες:
  - $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$ .
    - Π.χ.  $11 \bmod 8 = 3, 15 \bmod 8 = 7$   
 $[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$   
με χρήση της ιδιότητας  $(11 + 15) \bmod 8 = 26 \bmod 8 = 2$
  - $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$ .
    - Π.χ.  $[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$   
με χρήση της ιδιότητας  $(11 - 15) \bmod 8 = -4 \bmod 8 = 4$
  - $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$ .
    - Π.χ.  $[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$  με χρήση της ιδιότητας  $(11 \times 15) \bmod 8 = 165 \bmod 8 = 5$



# MODULAR ΕΚΘΕΤΟΠΟΙΗΣΗ (1/5)

- Χρησιμοποιεί την μέθοδο του Επαναλαμβανόμενου Τετραγωνισμού και Πολλαπλασιασμού
- Βασίζεται σε επαναλαμβανόμενες τετραγωνοποιήσεις της βάσης
- Βασίζεται στην δυαδική αναπαράσταση του εκθέτη

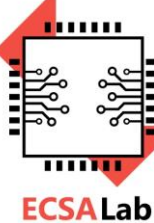


# MODULAR ΕΚΘΕΤΟΠΟΙΗΣΗ (2/5)

- Στηρίζεται στην εξής ιδέα. Αν ο εκθέτης  $e$  είναι μια δύναμη του 2, ας πούμε  $e = 2^k$ , τότε μπορούμε να “εκθετοποιήσουμε” με διαδοχικούς τετραγωνισμούς:

$$a^e = a^{2^k} = \left( \left( \left( \dots \left( a^2 \right)^2 \dots \right)^2 \right)^2 \right)^2$$

- Με αυτόν τον τρόπο υπολογίζουμε τον  $a^e$ , όπου  $e = 2^k$ , με  $k$  τετραγωνισμούς



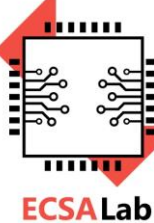
# MODULAR ΕΚΘΕΤΟΠΟΙΗΣΗ (3/5)

- Αν ο εκθέτης δεν είναι δύναμη του 2, τότε χρησιμοποιούμε τη δυαδική του αναπαράσταση. Έστω ότι ο  $e$  είναι ένας  $k$ -bit ακέραιος,  $2^{k-1} \leq e \leq 2^k - 1$ . Τότε,

$$\begin{aligned} e &= 2^{k-1} e_{k-1} + 2^{k-2} e_{k-2} + \dots + 2^1 e_1 + 2^0 e_0, \quad (\text{με } e_{k-1} = 1) \\ &= (2^{k-2} e_{k-1} + 2^{k-3} e_{k-2} + \dots + e_1) \cdot 2 + e_0 \\ &= (\dots((2e_{k-1} + e_{k-2}) \cdot 2 + e_{k-3}) \cdot 2 + \dots + e_1) \cdot 2 + e_0. \end{aligned}$$

και

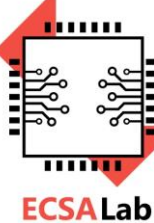
$$\begin{aligned} a^e &= a^{(\dots((2e_{k-1} + e_{k-2}) \cdot 2 + e_{k-3}) \cdot 2 + \dots + e_1) \cdot 2 + e_0} \\ &= \left( a^{(\dots((2e_{k-1} + e_{k-2}) \cdot 2 + e_{k-3}) \cdot 2 + \dots + e_1)} \right)^2 \cdot a^{e_0} \\ &= \left( \dots \left( \left( \left( a^2 \cdot a^{e_{k-2}} \right)^2 \cdot a^{e_{k-3}} \right)^2 \cdot \dots \right)^2 \cdot a^{e_1} \right)^2 \cdot a^{e_0} \end{aligned}$$



# MODULAR ΕΚΘΕΤΟΠΟΙΗΣΗ (4/5)

- Ο  $a^e$  μπορεί να υπολογιστεί σε  $k - 1$  βήματα, όπου κάθε βήμα συνίσταται σε τετραγωνισμό του ενδιάμεσου αποτελέσματος και, αν το αντίστοιχο ψηφίο  $e_i$  του  $e$  ( $= \text{Bit}(e, i)$ ) είναι 1, σε έναν επιπλέον πολλαπλασιασμό με  $a$ .
- Για το  $a^e \bmod n$ , παίρνουμε το υπόλοιπο modulo  $n$  μετά από κάθε τετραγωνισμό και πολλαπλασιασμό:

$$a^e \bmod n =$$
$$= \left( \dots \left( \left( \left( a^2 \cdot a^{e_{k-2}} \bmod n \right)^2 \cdot a^{e_{k-3}} \bmod n \right)^2 \cdot \dots \right)^2 \cdot a^{e_1} \bmod n \right)^2 \cdot a^{e_0} \bmod n.$$

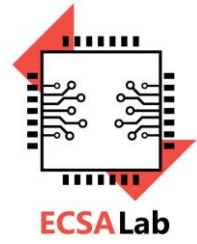


# MODULAR ΕΚΘΕΤΟΠΟΙΗΣΗ (5/5)

ModΔυναμη( $a, e, n$ )

```
1  $b \leftarrow a$   
2 for  $i \leftarrow \text{BitLength}(e) - 2$  downto 0 do  
3    $b \leftarrow b^2 \cdot a^{\text{Bit}(e, i)} \bmod n$   
4 return  $b$ 
```

- Το δυαδικό μήκος  $k$  του  $e$  είναι  $\lfloor \log_2 e \rfloor + 1$ , ο υπολογισμός του  $a^e \bmod n$  μπορεί να γίνει με
  - $m$  τετραγωνισμούς
  - $m$  πολλαπλασιασμούς
  - $m$  διαιρέσεις, όπου  $m = \lfloor \log_2 e \rfloor$



Απορίες???