Α. Αλγόριθμος Ευκλείδη

Παράδειγμα : Βρείτε τους μέγιστους κοινούς διαιρέτες:

- gcd(8,44)
- gcd(45,35)
- gcd(15,31)
- gcd(10,111)
- gcd(10,120)

Απάντηση

- 44=5*8+4
- 8=2***4**
- (44,8)=4

- 45=1*35+10
- 35=3*10+5
- 10=2***5**
- (45,35)=5

- 31=2*15+1
- 15=15***1**+0
- (31,15)=1

- 111=11*10+1
- 10=10***1**+0
- (111,10)=1

- 120=12***10**+0
- (120,10)=10

Β. Εκτενής Αλγόριθμος Ευκλείδη

Παράδειγμα**:** Να βρείτε τα χ,y αν ξέρω ότι gcd(41,35)=1 ώστε gcd(41,35)=41x+35y

Απάντηση:

- 41=1*35+6
- 35=5*6+5
- 6=1*5+1
- 5=5***1**+0
- gcd(41,35)=1
- Άρα από την εξίσωση έχω 1=6-5
  =6-(35-5.6) -- Πάντα αντικαθιστώ τον μικρότερο
  =6+5*6-35
  =6*6-35
  =6(41-35)-35
  =6*41-6*35-35
  =**6***41-**7***35
- Άρα χ=6 και y=-7

Γ. Η εξίσωση a · x ≡ b mod n

- Έχει **μια λύση** αν και μόνο αν gcd(a,n)=1 την $x=a^{-1}b(modn)$
- **Δεν έχει λύσεις** αν d=gcd(a,n) ≠1 και d **δεν** διαιρεί τον b
- Έχει **d** λύσεις αν d=gcd(a,n) ≠1 και d|b :
    - $x_o, x_o+n/d, x_o+2*n/d, x_o+3*n/d,\ldots,x_0+(d-1)*n/d$
    - Με $x_o=(a/d)^{-1}*(b/d)(modn/d)$

Παράδειγμα: Να λυθεί η εξύσωση 5x ≡ 3mod24

Λύση

gcd(24,5)=1 άρα η εξίσωση έχει μοναδική λύση

Α τρόπος: Δοκιμάζω όλες τις δυνατές περιπτώσεις του x

Β Τρόπος: χρησιμοποιώ τον εκτεταμένο αλγόριθμο του Ευκλείδη:
Θα υπάρχουν a και b ώστε: gcd(24,5)=1=24a+5b , άρα a=-1, b=5

- Άρα 5x ≡ 3*1(mod24)
- 5x ≡ 3(5*5-1*24)(mod24)
- 5x ≡3*5*5-3*24(mod24)
- 5x ≡3*5*5-3*0(mod24)
- 5x ≡3*5*5(mod24)
-
- Επειδή gcd(5,24)=1 έχω:
- x ≡ 3*5mod24
- Άρα x ≡15