Tema

1. Numărul minim și maxim de pași pt algoritmul lui Euclid

Nr minim de pași : at când numerele sunt egale (a, a).
algoritmul se oprește după un singur pas deoarece ~~restul~~

$a = a \cdot 1 + 0$ => restul este 0 / nul

~~=> multiplu~~ $(a, a) = a$

1 pas deci $(a, 0)$ sau $(0, a)$

~~Cel mai lung exemplu~~

Nr maxim de pași: este la 2 numere prime în care a este primul nr prim și b este ~~următorul / numărul~~ ~~cel de înainte nr prim~~ este nr prim care este înainte / după a consecutiv.

exemplu ar fi $(55, 34) = 34 \cdot 1 + 21$

$34 = 21 \cdot 1 + 13$

$21 = 13 \cdot 1 + 8$

$13 = 8 \cdot 1 + 5$

$8 = 5 \cdot 1 + 3$

$5 = 3 \cdot 1 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2 + 0$

8 pași 34 este al 8 nr prim

~~Cel mai mare nr~~

Cel mai mare nr de pași ar fi pentru un număr (a_n, a_{n-1})

~~nr de pași = al n nr prim~~

(a_n, a_{n-1})

$n-1$ nr de pași

nr de pași = locul celui mai mic nr prim dintre cele 2 nr prime care fac ~~CCMMDC~~ CMMMDC.

2. Nr de operații elementare pentru algoritmul lui Euclid.

Fiecare pas este o împărțire a/b

apoi o scădere $r = a - b \cdot q$

și o comparare pentru a verifica dacă $r = 0$

se face până la 0

prima are k pași, iar $r = a - b \cdot q$ are k pași $\Rightarrow$ 2k pași în total

3 Nr de operații elementare pentru algoritmul lui Euclid extins.

$$(a,b) = u \cdot a + v \cdot b$$

$(30,12) \Rightarrow 30 = 12 \cdot 2 + 6$

$12 = 6 \cdot 2 + 0$

$\Rightarrow (30,12) = 6 \Rightarrow 6 = 30 - 12 \cdot 2 \Rightarrow$

$\Rightarrow u = 1, v = -2 \Rightarrow 6 = 1 \cdot 30 + (-2) \cdot 12$

se fac 2 înmulțiri și 2 scăderi pentru a calcula u și v

folosește la fel ca la alg Euclid dar se păstrează 2 variabile care ac-tualizează coeficienții Bézout

se face o împărțire pt a calcula cât de multe ori încape un nr în altul

se face o scădere pt a calcula restul

se fac 2 înmulțiri și 2 scăderi

fiecare pas conține aproximativ 4 operații în loc de 2 (ca la Euclid simplu) ≠8

Euclid cu k pași $\Big|$ => Euclid extins face 4k operații

4. $\sum_{d|n} \varphi(d) = n$

$\varphi(p) = p-1$ $\quad \varphi(p^a) = p^a - p^{a-1}$ p este prim

$\varphi(a \cdot b) = \varphi(a)\,\varphi(b)$ dacă $(a,b) = 1$

$n = \prod_{i=1}^{k} p_i^{a_i} \Rightarrow \varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$

nr de elemente din $\varphi(n)$: $\{k \in \mathbb{Z} \mid 1 \le k \le n,\ (k,n) = 1\}$ =>

=> $\varphi(n)$ reprezintă numărul de numere prime cu ~~k~~ $\le n$

x nr întreg și d toți divizorii lui n.

Pt fiecare $d|n$ definim mulțimea: $S_d = \{k \mid 1 \le k \le n,\ (k,n) = d\}$

conține $\{1, \dots, n\}$ => $(k,n) = d$

dacă $k \in S_d$ => $k = d \cdot m$ $\quad (m, \frac{n}{d}) = 1$ $\Big/$ => m este coprim cu $\frac{n}{d}$

m poate fi $\varphi(\frac{n}{d})$ valori distincte

S_d are exact $\varphi(\frac{n}{d})$ elemente

Dacă adunăm mărimile acestor mulțimi at toți div lui d,

=> ~~fac~~ 1 ... n toate nr => $\sum_{d|n} \varphi(n/d) = n$

~~(55667, 77665)~~ (55667, 77665)

$77665 = 55667 \cdot 1 + 21998$

$55667 = 21998 \cdot 2 + 11671$

$21998 = 11671 \cdot 1 + 10327$

~~10327~~

$11671 = 10327 \cdot 1 + 1344$

$10327 = 1344 \cdot 7 + 919$

$1344 = 919 \cdot 1 + 425$

$919 = 425 \cdot 2 + 69$

$425 = 69 \cdot 6 + 11$

~~$11 = 7 \cdot 1 + 4$~~ ~~$69 = 11 \cdot 6 + 3$~~

$58 = 1 \cdot 58 + 0$

$69 = 11 \cdot 6 + 3$

$11 = 3 \cdot 3 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2 + 0$

$\Rightarrow (55667, 77665) = 1 \Rightarrow$ nr prime intre ele

Cel mi dirout :

$\Rightarrow 1 = u \cdot 55667 + v \cdot 77665$

$x_{55667} = (1, 0) \quad x_{77665} = (0, 1)$

$x_{21998} = x_{77665} - x_{55667} \cdot 1$

$(0, 1) - (1, 0) \cdot 1 = (-1, 1)$

$x_{11671} = x_{55667} - x_{21998} \cdot 2$

$(1, 0) - (-1, 1) \cdot 2 = (3, -2)$

$x_{10327} = x_{21998} - x_{11671} \cdot 1$

$(-1, 1) - (3, -2) = (-4, 3)$

~~$x_{1344} = x_{10327} - x_{1344} \cdot 7$~~

$(-4, 3)$

$$X_{43} = X_{44} - X_{103} \cdot 7$$

$$(3, -2) - [-4, 3) = (\pm, -5)$$

$$X_{98} = X_{103} - X_{43} \cdot \pm$$

$$(-4, 3) - (\pm, -5) \cdot \pm = (-4, 3) - (4, -83) = (-53, 38)$$

$$X_{425} = X_{43} - X_{820} \cdot 7$$

$$(\pm, -5) - (-53, 38) = (60, -43)$$

$$X_{69} = X_{929} - X_{425} \cdot 2$$

$$(-53, 38) - (60, -43) \cdot 2 = (-53, 38) - (120, -86) = [2\pm 3, 24$$

$$= (1098, -\pm 8\pm) - [-2028, 743) = (2138, -1532)$$

$$X_2 = X_{24} - X_3 \cdot 3$$

$$(1098, -\pm 8\pm) - (-6\pm 61, 983) \cdot 3$$

$$= (1098, -\pm 8\pm) - [-2028, 743) = (2138, -1532)$$

$$X_1 = X_{983} - X_2 \cdot 1$$

$$(-6\pm 61, 983) - [2138, -1532) = [-2874, 2071)$$

$$1 = (-28 \cdot 4, 2) \cdot 5566\pm + 2071\pm \cdot \pm\pm 65$$

inversul ~~mod~~ modular al lui 55 modulo 89

$$55x \equiv 1 \pmod{89}$$

$$(55, 89) = 1$$

$$89 = 55 \cdot 1 + 34$$
$$55 = 34 \cdot 1 + 21$$
$$34 = 21 \cdot 1 + 13$$
$$21 = 13 \cdot 1 + 8$$
$$13 = 8 \cdot 1 + 5$$
$$8 = 5 \cdot 1 + 3$$
$$5 = 3 \cdot 1 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$2 = 1 \cdot 2 + 0$$

$x_{55} = (1,0)$ $\quad x_{89} = (0,1)$

$x_{34} = x_{89} - x_{55} = (0,1) - (1,0) = (-1,1)$

$x_{21} = x_{55} - x_{34} = (1,0) - (-1,1) = (2,-1)$

$x_{13} = x_{34} - x_{21} = (-1,1) - (2,-1) = (-3,2)$

$x_8 = x_{21} - x_{13} = (2,-1) - (-3,2) = (5,-3)$

$x_5 = x_{13} - x_8 = (-3,2) - (5,-3) = (-8,5)$

$x_3 = x_8 - x_5 = (5,-3) - (-8,5) = (13,-8)$

$x_2 = x_5 - x_3 = (-8,5) - (13,-8) = (-21,13)$

$x_1 = x_3 - x_2 = (13,-8) - (-21,13) = (34,-21)$

$1 = 34 \cdot 55 + (-21) \cdot 89$

$x = 34 \pmod{89}$

$55^{-1} = 34 \pmod{89}$