

30/11/15

~~30/11/15~~ #4

$$1) a) \quad 256x + 337y = 179$$

$$337 = 1 \cdot 256 + \textcircled{81}$$

$$256 = 3 \cdot 81 + \textcircled{13}$$

$$81 = 6 \cdot 13 + \textcircled{9}$$

$$13 = 3 \cdot 4 + \textcircled{1}$$

Uia Rück

$$1 = 13 - \textcircled{9} \cdot 4 = 13 - 4(81 - 6 \cdot 13) =$$

$$= -4 \cdot 81 + 25 \cdot \textcircled{13} = -4 \cdot 81 +$$

$$+ 25(256 - 3 \cdot 81) =$$

$$= 25 \cdot 256 - 79 \cdot 81 \Rightarrow 1 = 25 \cdot 256 -$$

$$79 \cdot 81 =$$

$$= 25 \cdot 256 - 79(337 - 256)$$

$$= -79 \cdot 337 + 104 \cdot 256$$

$$(256, 337) = 1 \mid 179 \Rightarrow \text{Exakte Lösung}$$

$$1 = -79 \cdot 337 + 104 \cdot 256 \Rightarrow$$

$$\Rightarrow 179 = (-79)(179) 337 + (179 \cdot 104) 256$$

$$x_0 = 179 \cdot 104, \quad y_0 = -79 \cdot 179$$

allgemeine Lösung

$$x = 179 \cdot 104 + 337 \cdot t$$

$$y = -79 \cdot 179 - 256 \cdot t$$

**

f) $5x + 7y + 14z = 44$ Oscar's
rooms

$(5, 7, 14) = 1 \Rightarrow \text{Lucas}$

$5x + 7y + 14z = 1$

$7y + 14z = 7w \Rightarrow x = 3 + 7t$

$5x + 7w = 1 \Rightarrow 5 \cdot 3 + 7(-2) = 1 \Rightarrow w = -2 - 5t$

$t = z$

$\rightarrow 5y + 14z = 7w \Rightarrow$

$y + 2z = 1$

$-1 + 2 \cdot 1 = 1$

$y = -1 + 2 \cdot 5$
 $z = 1 - 5$ $s \in \mathbb{Z}$ $\} \Rightarrow$

$y = (-1 + 2s)w = (-1 + 2s)(-2 - 5t)$

$z = (1 - 5)w = (1 - 5)(-2 - 5t)$

$x = 3 + 7t$ Lucas's rooms (1)

Lucas's rooms (2)

$x = (3 + 7t)44$

$y = (2 + 5t - 4 \cdot 5 - 10st)44$

$z = (-2) + 2 \cdot 5 - 5t + 5st)44$

$x > 0 \quad y > 0, \quad z > 0$

$(3 + 7t)44 > 0 \Rightarrow 7t > -3 \Rightarrow$

$\Rightarrow t \geq 0$

$$y = (2 + 5t - 4 \cdot 5 - 105t) \cdot 4 > 0 \Rightarrow$$

$$\Rightarrow \frac{(2+5t)}{(2+5t)} > \frac{2(2+5t) \cdot 5}{2} \Rightarrow \frac{1}{2} > 5$$

$$(2+5t) \cdot 5 > 2+5t \Rightarrow$$

$$\Rightarrow 5 > 1$$

2) Νομισματο 1770

x Άλφα

x Βετα

$$31x + 21y = 1770$$

και $x, y \geq 0$ και

ακέραιο

$$(31, 21) = 1$$

$$1 = (-2) \cdot 31 + 3 \cdot 21$$

$$x = (-2 + 21t) \cdot 1770$$

$$y = (3 - 31t) \cdot 1770 \geq 0$$

$$-2 + 21t \geq 0 \Rightarrow$$

$$t \geq \frac{2}{21} \Rightarrow$$

$$\boxed{t \geq 1}$$

$$3 - 31t \geq 0 \Rightarrow \frac{3}{31} \geq t \Rightarrow$$

$$\Rightarrow \boxed{0 \geq t} \text{ αδύνατο}$$

$$31(-2 + 21t) + 21(3 - 31t) = 1 \mid 1770$$

$$31(-2) + 31 \cdot 21t + 3 \cdot 21 - 21 \cdot 31t = 1$$

$$3) a \equiv b \pmod{m} \Rightarrow (a, m) = (b, m)$$

$$a - b = km$$

$$a = n \cdot m + u$$

$$b = n' \cdot m + u'$$

$$\text{και } u = u'$$

$(a, m) \mid a$ και m και

είναι ο H.C.C.

$$b = a - km \Rightarrow (a, m) \mid$$

$$(a, m) \mid a \text{ και } m \Rightarrow (a, m) \mid b, a, m$$

$$(a, m) | (b, m) \Rightarrow$$

Me zov idio zovno

$$(b, m) | (a, m) \Leftrightarrow (b, m) = (a, m)$$

$$4) \left. \begin{array}{l} a \equiv b \pmod{m} \\ a = y \pmod{n} \end{array} \right\} \Rightarrow B \equiv y \pmod{(m, n)}$$

Q $a \pmod{4}$	$a \pmod{24}$
$13 \pmod{4}$	$13 \pmod{24}$
$\equiv$	$\equiv$
1	13

$$\begin{array}{l} a - b = km \Rightarrow \\ a - y = 2n \end{array} \quad \begin{array}{l} \Rightarrow \\ \Rightarrow B - y = 2n - km = \end{array}$$

~~$$a - y = 2n$$~~

$$B - y = 22'(m, n) - k k'(m, n)$$

$$\Rightarrow B - y = (22' - k k')$$

Onou $n = 2'(m, n)$

$$\cdot (m, n) (=)$$

$$m = k'(m, n)$$

$$(=) \Rightarrow B \equiv y \pmod{(m, n)}$$

Διοφαντικές Εξισώσεις

$$ax + by = c \quad \text{εχσ}$$

ακέραιες λύσης αυν

$$(a, b) \mid c$$

Βρίσκουμε μια λύση χρησιμοποιώντας
του ΜΚΔ και του αλγόριθμο του
Ευκλείδη $ax_0 + by_0 = (a, b)$

Την χρησιμοποιούμε για να γνίσουμε λύση

$$\mathbb{Z}_m = \{ [0]_m, [1]_m, [m-1]_m \}$$

ορίζεται πρόσθεση και ποτ/κός με τα-
ξύ των κλάσεων.

Η πρόσθεση δύε έχει προβλεπόμενο

$$[a]_m \oplus [b]_m = [a+b]_m$$

Ο ποτ/κός έχει προβλεπόμενο όταν
m σύνθετος

$$[a]_m \odot [b]_m = [a \cdot b]_m$$

Μας ενδιαφέρει να γινίξουμε αν
μια κλάση έχει αντίστροφη

$$\exists b \text{ με } [0]_m \odot [b]_m = [1]_m$$

$$\left. \begin{array}{l} ax \equiv b \pmod{m} \\ a \cdot c \equiv 1 \pmod{m} \end{array} \right\} \Rightarrow \textcircled{a}$$

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

$$\Rightarrow x \equiv c \cdot b \pmod{m}$$

$$[a]_m^{-1} = [c]_m$$

Οι αντιστρέφουσες κλάσεις στο $\mathbb{Z}_m$ είναι
ακριβώς $\varphi(m)$ η συνάρτηση του
Euler

$$\varphi(p) = p - 1$$

$$\varphi(m) = ;$$

It φ είναι πολλακλή $\Leftrightarrow \text{Av}(m, k) = 1$,

$$\text{τότε } \varphi(mk) = \varphi(m)\varphi(k)$$

$$\varphi(p^k) = p^{k-1} \varphi(p) = p^{k-1}(p-1) \quad \text{⊕}$$

⊕ $\Rightarrow \varphi(n)$ υπολογίζεται με την
πρωτογενή ανάλυση

Πρόβλημα

Av γνωρίζετε το $\varphi(n)$, μπορείτε
να βρείτε το $n ; ;$

n.x

n=5, 8, 10

$$\varphi(n) = 4 \Rightarrow n = ; \quad \varphi(7) = 4$$

$$\varphi(5) = 5 - 1 = 4$$

$$\varphi(8) = \varphi(2) \cdot 2^{3-1} = 4$$

$$p \text{ πρώτος} \Rightarrow \varphi(p) = p - 1 = 4 \Rightarrow p = 5$$

$$p^2 \Rightarrow \varphi(p^2) = p \varphi(p) = p(p-1) = 4 \Rightarrow$$

$$\Rightarrow p \mid 4 \Rightarrow p = 2 \Rightarrow \varphi(2^2) = 4$$

$$p^3 \Rightarrow \varphi(p^3) = p^2 \varphi(p) = 4 \Rightarrow$$

$$\Rightarrow 2^2 \mid 4 \Rightarrow p = 2 \Rightarrow \varphi(2^3) = 4$$

$\varphi(9)$ με $p, 9$ πρώτοι

$$\varphi(p, q) = \varphi(p)\varphi(q) = (p-1)(q-1) = 4$$

$$p-1 = 1 \quad \text{και} \quad q-1 = 4 \Rightarrow p = 2$$

$$= 1 \cdot 4$$

$$q = 5$$

$$\varphi(10) = 4$$

Λemma

Τηνος του Gauss

Για η φυσικό αριθμό

$$n = \sum_{k|n} \varphi(k)$$

$$k|n$$

n

$$n = 10, \text{ διαιρετες: } 1, 2, 5, 10$$

$$\varphi(1) = 1$$

$$\varphi(2) = 1$$

$$\varphi(5) = 4$$

$$\varphi(10) = \varphi(2 \cdot 5) = \varphi(2)\varphi(5) = 4$$

Λemma

$$\mathbb{Z}_m = \{ [0]_m, [1]_m, \dots, [m-1]_m \}$$

Εστω ότι οι αντιστοιχίες κλάσης
δίνονται

$$\{ [a_1]_m, [a_2]_m, [a_3]_m, \dots,$$

$$[a_{\varphi(m)}]_m \}$$
 και

α ακαίρεος με $(a, m) = 1$, τότε

$$, \text{TOTAL} \quad \{ [a,]_m, \dots, [a \varphi(m)]_m \} =$$

$$= \{ [a a,]_m, \dots, [a a \varphi(m)]_m \}$$