$\gcd(a,b) :=$ μέγιστος ακέραιος d έτσι ώστε $d \mid a$ και $d \mid b$

Find_GCD(a,b)

Φεβ 3-11:19 πμ

$$\boxed{a = bq + r}$$

πολ/πο υπόλοιπο

$r \in \{0, 1, \dots, b-1\}$

$$\boxed{\gcd(a,b) = \gcd(b,r)}$$

$$\gcd(r_0, r_1) = \gcd(r_2, r_2) = \gcd(r_2, r_3)$$

Φεβ 3-11:31 πμ

$$18 = 5 \cdot 54 - 1 \cdot 36$$
$$= 54 - 1 \cdot (198 - 3 \cdot 54)$$
$$= 4 \cdot 54 - 1 \cdot 198$$
$$= 4(252 - 1 \cdot 198) - 1 \cdot 198$$
$$= 4 \cdot 252 - 5 \cdot 198$$

Φεβ 3-11:43 πμ

$$sac + tbc = c$$

$$a\left(sc + t\frac{bc}{a}\right) = c$$

επομένως $a \mid c$

Φεβ 3-11:49 πμ

$ax \equiv b \bmod m$

Έχει λύση όταν ω $\gcd(a,m) = 1$

Τότε $\exists\, s,t : sa + tm = 1$

Θέλω ax και το b έχουν το ίδιο υπόλοιπο στη διαίρεση με το m

Θέτουμε x το $\boxed{s \cdot b \bmod m}$

$$sa(sb) + tm = 1$$
$$+ tmb = b$$

Στη διαίρεση με το m πάει στον το υπόλοιπο

Το δεύτερο μέλος της εξίσωσης $ax \equiv b \bmod m$

Θα είναι ίσο με το υπόλοιπο του sab (γιατί το tmb έχει υπόλοιπο 0)

$$(sb)a + 0 = b \bmod m$$
$$x \cdot a = b \bmod m$$

Φεβ 3-11:52 πμ

$3x \equiv 4 \pmod 7$

$$7 = \boxed{2} \cdot 3 + \boxed{1} \quad \text{gcd}$$
$$3 = \boxed{1} \cdot 3 + \boxed{0}$$
$$1 = 7 - 2 \cdot 3$$
$$= \underset{s}{\boxed{-2}} \cdot 3 + \underset{t}{\boxed{1}} \cdot 7$$

Έχω $s \cdot b = -2 \cdot 4 = -8$

Στη διαίρεση με το 7 αυτό θα αφήσει ως υπόλοιπο 7+r

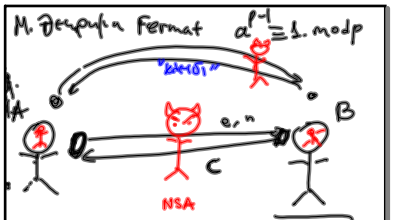
Έχω το ίδιο υπόλοιπο

$$-8 = (-2)7 + \boxed{6}$$

η λύση της εξίσωσης $3x \equiv 4 \bmod 7$ είναι 6

Φεβ 3-12:20 μμ

Μ. Θεώρημα Fermat $a^{p-1} \equiv 1 \mod p$



$C = M^e \mod n$ $\boxed{e \text{ πρώτος}, \; n = p \cdot q}$

Ο Α διαλέγει το e:
η εξίσωση $e \cdot x = 1 \mod ((p-1)(q-1))$
να έχει λύση. Δείτε ότι η λύση

Έχω δδδ ότι
$(p-1)(q-1)$ διαιρεί το $(ed-1)$

$\Leftrightarrow ed - 1 = k \cdot (p-1)(q-1)$

$\Leftrightarrow \boxed{ed = 1 + k(p-1)(q-1)}$

Φεβ 3-12:33 μμ

Μ. $M^{k(p-1)(q-1)} \mod n$
$\parallel$
1

Fermat: $M^{p-1} = 1 \mod p$
$M^{q-1} = 1 \mod q$

$M^{(p-1)(q-1)} = 1 \mod p$
$M^{(p-1)(q-1)} = 1 \mod q$

p διαιρεί το $M^{(p-1)(q-1)} - 1$
q διαιρεί το $M^{(p-1)(q-1)} - 1$

$n = p \cdot q$ διαιρεί το $M^{(p-1)(q-1)} - 1$
δλδ $M^{(p-1)(q-1)} = 1 \mod n$

Φεβ 3-12:51 μμ

$e \cdot x \equiv 1 \mod ((p-1)(q-1))$

$pq - p - q + 1$ n

δυτικός

Φεβ 3-12:58 μμ

$a_0, a_1, a_2, \ldots$

$\sum_{i=0}^{n} a_i = a_0 + a_1 + \ldots + a_n$

$\sum_{i=0}^{n} a_i = a_0 + \sum_{i=1}^{n} a_i$

$\sum_{i=1}^{n} a_i - \sum_{i=0}^{n-1} a_i = \boxed{a_n - a_0}$

$(a_1 + a_2 + \ldots + a_n) - (a_0 + a_1 + \ldots + a_{n-1})$

Φεβ 3-1:21 μμ

$\sum_{k=1}^{2} (-1)^k = (-1)^1 + (-1)^2 = 0$

$\sum_{k=1}^{4} (-1)^k = (-1)^1 + (-1)^2 + (-1)^3 + (-1)^4$

$= -1 + 1 - 1 + 1 = 0$

Φεβ 3-1:28 μμ

$\boxed{\forall n \; P(n)}$

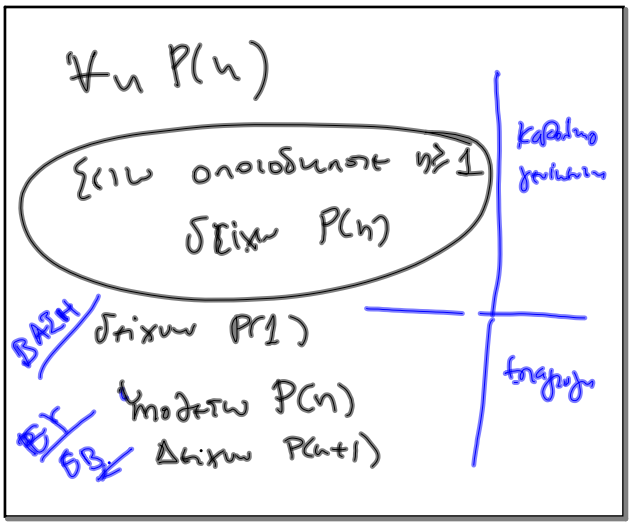
Θδ.Ο. μτ επαγωγή

ΒΑΣΗ δείχνω ότι ισχύει το $P(0)$

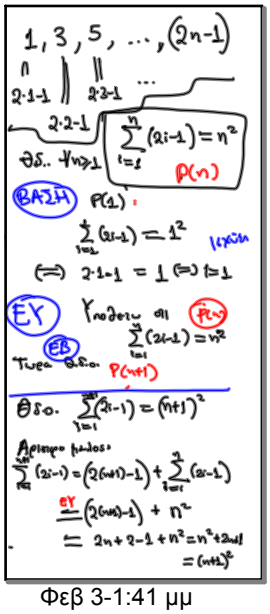
ΕΠΑΓΩΓΙΚΗ ΥΠΟΘΕΣΗ Υποθέτω ότι ισχύει το $P(n)$

ΕΠΑΓΩΓΙΚΟ ΒΗΜΑ Δείχνω ότι ισχύει $P(n+1)$

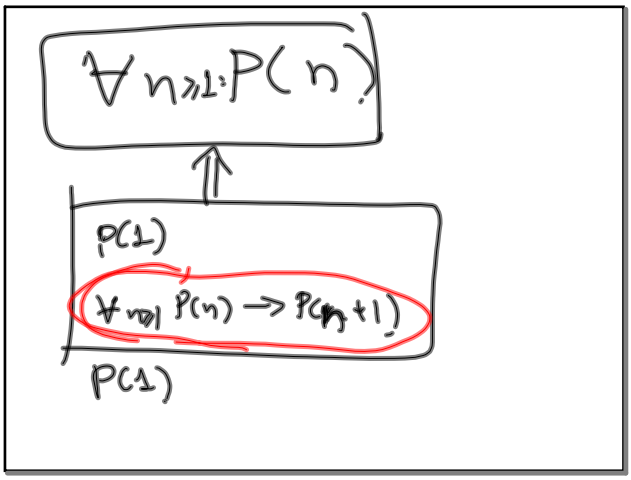
Φεβ 3-1:31 μμ



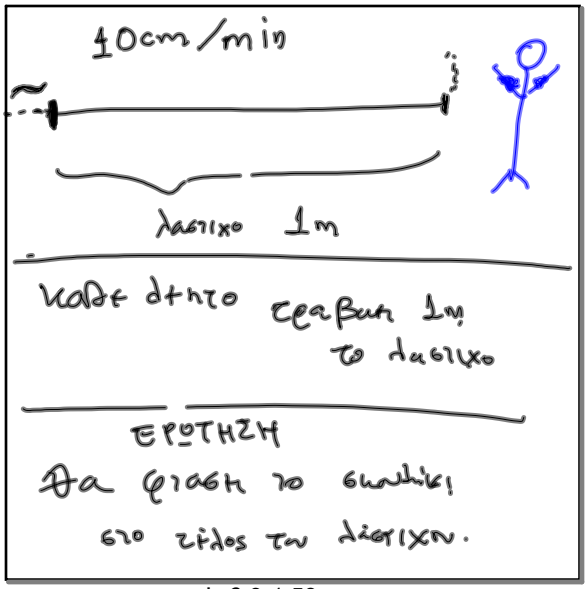
Φεβ 3-1:36 μμ



Φεβ 3-1:41 μμ



Φεβ 3-1:52 μμ



Φεβ 3-1:58 μμ