Selgitused, kuidas lahendada võrrandit.

$5x + 2 \equiv 0 \pmod{37}$

Esiteks võime viia nagu ikka 2 paremale poole,

$5x \equiv -2 \pmod{37}$

Sisuliselt otsitakse arvu, mis 5-ga korrutades annaks –2 (mod 37), ehk siis –2/5 (mod 37). Kuidas selline arv leida, sest modulaarses arvutuses me tavapäraselt jagada ei saa? Eukleidese algoritm ja teadmine, et 37 on algarv, annavad meile võimaluse leida arvu $a \equiv 1/5 \pmod{37}$ – ehk siis arvu, mis viiega korrutades annab 1, $a*5 \equiv 1 \pmod{37}$ (ehk siis arvu 5 pöördväärtuse (mod 37)) .
Edasi saab juba meie võrrandit korrutada selle arvuga a, saades vasakule poolele $a*5*x \equiv 1*x \equiv x \pmod{37}$, ja paremale poolele $–2*a \pmod{37}$,
ehk siis kokku $x \equiv -2*a \pmod{37}$.

Kuidas leida arv a?
Selleks kasutame Eukleidese algoritmi.
Nimelt kirjutame välja, kuidas arvutame EA abil SÜT (5, 37). Me tegelikult küll teame, et SÜT (5,37) =1, kuid nii saame võimaluse avaldada
1= SÜT (5,37) = u*5 + v*37, kus u ja v on täisarvud, mille me leiame EA abil.

SÜT(5,37) = SÜT(2,5) = 1

Siinjuures kirjutame üles, kuidas jäägiga jagamine täpselt toimub.
37 = 7*5 + 2, ehk siis 2 = 37 – 7*5
5 = 2*2 +1, ehk siis 1 = 5 – 2*2 = 5 – 2* (37 – 7*5) = 15*5 –2*37
See tähendab, et u = 15 ja v = -2

Nüüd vaatame, mis juhtub modulaarses arvutuses:
$1 \equiv 15*5 – 2*37 \pmod{37}$

$-2*37 \equiv 0 \pmod{37}$, seega on meil kokkuvõttes $1 \equiv 15*5 \pmod{37}$,
mis tähendab, et a = 15 ongi 5 pöördväärtus, mida otsisime.

Võttes nüüd uuesti ette esialgse võrrandi $5x \equiv -2 \pmod{37}$, tuleb meil mitte mõlemat poolt jagada 5-ga, vaid korrutada selle pöördväärtusega 15
(nagu tava-aritmeetikaski, kui selle asemel, et jagada 4-ga, korrutame ¼ -ga).
Seega on tulemuseks $15*5x \equiv 15*(-2) \pmod{37}$
Ehk siis $x \equiv 7 \pmod{37}$, sest $15*5 \equiv 1$ ja $15*(–2) \equiv -30 \equiv 7 \pmod{37}$.

Võrrandisüsteemi lahendamine.

$8x + 31y \equiv 6 \pmod{83}$
$2x + 16y \equiv 42 \pmod{83}$

Alustame nagu tavalise võrrandisüsteemiga ja taandame ühe muutujatest välja. Selleks korrutame teist võrrandit 4-ga ja lahutame tulemuse esimesest võrrandist. Järele jääb
$31y - 4*16y \equiv 6 - 4*42 \pmod{83}$
$50y \equiv 4 \pmod{83}$

Nüüd lahendame selle võrrandi. Esmalt on meil jällegi vaja leida 50 pöördväärtus (sellega korrutamine tähendab siin 50-ga jagamist).

Kasutame jällegi EA ja leiame, et $1 = 5*50 - 3*83$
Ehk siis $5*50 \equiv 1 \pmod{83}$

Seetõttu $y \equiv 5*4 \equiv 20 \pmod{83}$

Järgmiseks tuleb arvutada välja ka x.
Asendame y teises võrrandis:

$2x + 16*20 \equiv 42 \pmod{83}$ ehk
$2x \equiv 54 \pmod{83}$

lahendame ka selle võrrandi analoogselt, leides arvu 2 pöördväärtuse
Kasutame EA ja saame, et $1 = 42*2 + 83$,
ehk siis 2 pöördväärtus on 42
Seega $x \equiv 42*54 \equiv 27 \pmod{83}$.

Ehk vastus on : $y \equiv 20 \pmod{83}$ ja $x \equiv 27 \pmod{83}$