1. Tétel. *Legyenek a, b, n egész számok, $n > 1$. Ekkor az $ax \equiv b \mod n$ megoldható $\iff (a,n) \mid b$. Ez esetben pontosan (a,n) darab inkongruens megoldás van* mod n.

Bizonyítás. Definíció szerint

$$ax \equiv b \mod n \iff ax + ny = b.$$

Szükséges feltétel: Mivel (a,n) osztja a bal oldalt, osztja a jobb oldalt is, azaz $(a,n) \mid b$.
Elégséges feltétel: A *bővített euklideszi algoritmus* szerint létezik olyan $\hat{x}, \hat{y}$, hogy

$$a\hat{x} + n\hat{y} = (a,n).$$

Beszorozva $b/(a,n)$-el kapjuk:

$$\frac{b}{(a,n)} \cdot \hat{x} \cdot a + \frac{b}{(a,n)} \cdot \hat{y} \cdot n = \frac{b}{(a,n)} \cdot (a,n) = b,$$

azaz

$$x \equiv \frac{b}{(a,n)}\hat{x} \mod n.$$

Jegyezzük meg, hogy ez egy megoldás modulo n, tehát nem csak x, hanem $\{x + kn : k \in \mathbb{Z}\}$ is megoldások.

Megoldások száma, speciális eset: Először megmutatjuk, hogy ha $(a,n) = 1$, akkor egy megoldás van modulo n (azaz, ha x_1, x_2 két megoldás, akkor $x_1 \equiv x_2 \mod n$).

Tegyük fel tehát, hogy $(a,n) = 1$ és legyen (x_1, y_1) és (x_2, y_2) két megoldása az $ax + ny = b$ egyenletnek. Ekkor

$$\begin{matrix} ax_1 + ny_1 = b \\ ax_2 + ny_2 = b \end{matrix} \implies ax_1 + ny_1 = ax_2 + ny_2 \implies a(x_1 - x_2) = n(y_2 - y_1).$$

Azaz $n \mid a(x_1 - x_2)$. Mivel $(a,n) = 1$, ezért $n \mid x_1 - x_2$, tehát $x_1 \equiv x_2 \mod n$.

Megoldások száma, általános eset: Az általános esetben legyen $d = (a,n)$. Az általános esetet visszavezetjük a korábbi speciális esetre (mikor az együttható és a modulus relatív prímek voltak.) Legyen

$$a' = a/d, \quad b' = b/d, \quad n' = n/d$$

és tekintsük az

$$a'x \equiv b' \mod n'$$

kongruenciát. Itt x pontosan akkor megoldás, ha x megoldása az eredeti $ax \equiv b \mod n$ kongruenciának.

A speciális eset miatt tudjuk, hogy mivel $(a', n') = 1$, ezért ennek egyértelmű megoldása van modulo n', azaz az $\{x_0 + kn' : k \in \mathbb{Z}\}$ az összes megoldás. A korábbi megjegyzés szerint ezek lesznek az eredeti kongruencia megoldásai is. Ezek között keressük a *lényegesen különböző* megoldásokat, azaz melyek *különböznek* modulo n. Két ilyen megoldás azonos egymással modulo n, azaz

$$x_0 + k_1 n' \equiv x_0 + k_2 n' \mod n,$$

ha

$$n \mid (k_1 - k_2)n'.$$

Mivel $n = d \cdot n'$, ezért ez pontosan akkor teljesül, ha $d \mid k_1 - k_2$. Tehát a *különböző* megoldások modulo n a következőek:

$$x_0 + kn' : k = 0, 1, \ldots, d - 1.$$

□

Összefoglalva:
Tekintsük az $ax \equiv b \mod n$ kongruenciát.

1. A *bővített euklideszi algoritmus* segítségével számoljuk ki az $\hat{x}, \hat{y}$ egészeket és az (a, n) legnagyobb közös osztót, melyre
$$a\hat{x} + n\hat{y} = (a, n).$$

2. Ha $(a, n) \nmid b$, akkor nincs megoldás.

3. Ha $(a, n) \mid b$, akkor (a, n) megoldás van modulo n, és ezek:
$$x_k = \frac{b}{(a, n)}\hat{x} + k \cdot \frac{n}{(a, n)} : \quad k = 0, 1, \ldots, (a, n) - 1.$$

Példa: *Oldjuk meg a* $21x \equiv 14 \mod 35$ *konruenciát!*

- A A *bővített euklideszi algoritmus* segítségével kiszámoljuk az $\hat{x}, \hat{y}$ egészeket és a $(21, 35)$ legnagyobb közös osztót, melyre
$$21\hat{x} + 35\hat{y} = (21, 35).$$
Nevezetesen a szokásos számolási szabályok szerint (mivel a későbbiekben nem használjuk az $\hat{y}$-t, ezt nem tüntetjük fel a táblázatban):

i	q_i	r_i	$\hat{x}_i$
-1	–	21	1
0	–	35	0
1	0	21	1
2	1	14	-1
3	1	7	2
4	2	0	–

- Ekkor $(21, 35) = 7$ és mivel $7 \mid 14$, így van megoldás.

- A *lényegesesen* különböző megoldások száma $(21, 35) = 7$. Mivel $\hat{x} = 2$, ezek a következők:
$$x_k = \frac{14}{7} \cdot 2 + k \cdot \frac{35}{7} = 4 + 5k : \quad k = 0, 1, 2, 3, 4, 5, 6.$$