Number Theory - Day 3

Overview
- Quick Review of Euclidean Alg.
- Bézout's Identity
- Reverse or "Extended" Euclidean Algorithm
- Plus Problems

Euclidean Alg. → gcd(a, b)

- dealing with very large #s

(324, 60)

$\gcd(600, 136)$

$a > b \rightarrow a = q_1 \cdot b + r$

$b = q_2 \cdot r + r_2$

$r_n = q_{n+1} \cdot r_{n+1} + 0$

$600 = 4 \cdot 136 + 56$

$136 = 2 \cdot 56 + 24$

$56 = 2 \cdot 24 + 8$

$24 = 3 \cdot 8 + 0$

$\Rightarrow \gcd(600, 136) = 8$

Bézout's Id.

Diophantine Equations → $x, y, z \ldots$ every var $\in \mathbb{Z}^+$ or $\mathbb{Z}^-$

→ 1 eq., 2 variables

$2x + 3y = 16$

→ 2 eq., 3 variables

$2x + 3y + 7z = 12$

$3x + 11y + z = 18$

There exists integers a, b such that for $(x, y) \in \mathbb{Z}$

$ax + by = \gcd(x, y)$ $\quad ax + by = m \cdot \gcd(x, y)$

$(x, y) = (12, 18)$

$\gcd(12, 18) = 6$

$a \cdot 12 + b \cdot 18 = 6$

$a = -1, b = 1$ ✓ $(-1, 1)$

$a \cdot 12 + b \cdot 18 = 6m$ ($m = 13$)

$(-m, m)$

$a \cdot 12 + b \cdot 18 = 13 \cdot 6$

$(-13, 13)$

Reverse Euclidean Alg.

$81a + 57b = 3$

$\gcd(81, 57)$

$81 = 1(57) + 24$

$57 = 2(24) + 9$

$24 = 2(9) + 6$

$9 = 1(6) + 3$

$6 = 2(3) + 0$

$\gcd(81, 57) = 3$

$9 = 57 - 2(24)$

$3 = 9 - 1(6)$

$3 = 9 - 1(24 - 2(9))$

$= 9 - 1(24) + 2(9)$

$= 3(9) - 1(24)$

$6 = 24 - 2(9)$

$3(57 - 2(24)) - 1(24)$

$3(57) - 2(24) - 1(24)$

$3(57) - 3(24)$

$24 = 81 - 1(57)$

$3(57) - 3(81 - 1(57))$

$3(57) - 3(81) + 3(57)$

$-3(81) + 6(57)$

$-3(81) + 6(57) = 3$

$81a + 57b = 3$

$a = -3, b = 6$

$527a + 341b = \gcd(527, 341)$

(1) use the E.A. to find $\gcd(527, 341)$ ✓

(2) use R.E.A to find a substitution for $\gcd(527, 341)$ ✓

(3) represent in problem statement form ✓

$527 = 1(341) + 186$

$341 = 1(186) + 155$

$186 = 1(155) + 31$

$155 = 5(31) + 0$

→ gcd of $527, 341 = 31$

$527a + 341b = 31$

$31 = 186 - 1(155)$

$155 = 341 - 1(186)$

$31 = 186 - 1(341 - 1(186))$

$= 186 - 1(341) + 1(186)$

$= 2(186) - 1(341)$

$527 = 1(341) + 186$

$186 = 527 - 1(341)$

$= 2(527 - 1(341)) - 1(341)$

$= 2(527) - 2(341) - 1(341)$

$= 2(527) - 3(341) = 31$ → $31 \cdot 12$

$527(a) + 341(b) = 31$

$2 \quad -3 \rightarrow \boxed{(2, -3)}$ ← Bézout's Id. for 527 and 341

$ax + by = \gcd(x, y)$

$az + by = \gcd(x, y) \cdot m$

$(2m, -3m)$

$(24, -36)$

$ax + by + cz = \gcd(x, y, z)$ ✓

25. **(1959 IMO)** Show that

$$\frac{21N + 4}{14N + 3}$$

cannot be reduced further for every integer N.

$\frac{4}{2} = 2$

$\frac{25}{17}$ ✓

$\frac{a}{b}$

$\gcd(a, b) \neq 1$

$\gcd(21N + 4, 14N + 3) = 1$

$\gcd(a, b)$ assume WLOG $a > b$

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

$\gcd(21N + 4, 14N + 3) \rightarrow 1$

$= \gcd(21N + 4 - (14N + 3), 14N + 3)$

$= \gcd(7N + 1, 14N + 3)$

$= \gcd(7N + 1, 7N + 2) \rightarrow \gcd(1, 7N + 1) = 1$

(consecutive

$\gcd(a, a + 1)$

$= \gcd(a, 1) = 1$

Prove that if $\gcd(a, b) = 1$

then $\gcd(ab, a^2 + b^2) = 1$

Lemma 1 ⇒ $\gcd(c, d) = 1$

then $\gcd(c, ck + d) = 1$ for any k

$= \gcd(c, d) = 1$

Lemma 2 : if $\gcd(c_1, d) = 1$

$\gcd(c_2, d) = 1$

$\gcd(c_1 c_2, d) = 1$

$\gcd(5, 12) = 1$ $\quad \gcd(85, 12)$

$\gcd(17, 12) = 1$ $\quad = 1$

Lemma 2 implies that

if $\gcd(a, b^2) = 1$

then $\gcd(a, a^2 + b^2) = 1$

$\gcd(b, a^2 + b^2) = 1$

$\boxed{\gcd(ab, a^2 + b^2) = 1}$

27. **(2006 AMC 12A)** Two farmers agree that pigs are worth 300 dollars and that goats are worth 210 dollars. When one farmer owes the other money, he pays the debt in pigs or goats, with "change" received in the form of goats or pigs as necessary. (For example, a 390 dollar debt could be paid with two pigs, with one goat received in change.) What is the amount of the smallest positive debt that can be resolved in this way?

Chicken McNugget Thrm Inter

$300p + 210g = x \cdot m$

$p, g \in \mathbb{Z}$

$x = \gcd(210, 300) \cdot m$

$\Rightarrow m = 1$

$\gcd(300, 210) = \boxed{30}$

$300p + 210g = 30(10p + 7g)$

$3g - 2p = 30$ exactly

$\boxed{30}$ can be made and its the smallest possible value