

Theorem 0.2. GCD Is a Linear Combination (integer linear combination).

For any nonzero integers a and b , there exist integers s and t such that

$$\gcd(a, b) = as + bt.$$

Moreover, $\gcd(a, b)$ is the smallest positive integer of the form $as + bt$.

Euclidean Algorithm. If a, b are positive integers, we may find $\gcd(a, b)$ by repeated use of the division algorithm to produce a decreasing sequence of integers $r_1 > r_2 > \cdots > r_k > 0$, where the last nonzero remainder r_k is equal to $\gcd(a, b)$.

$$\begin{array}{ll} a = bq_1 + r_1 & 0 < r_1 < b \\ b = r_1q_2 + r_2 & 0 < r_2 < r_1 \\ r_1 = r_2q_3 + r_3 & 0 < r_3 < r_2 \\ & \vdots \\ r_{k-3} = r_{k-2}q_{k-1} + r_{k-1} & 0 < r_{k-1} < r_{k-2} \\ r_{k-2} = r_{k-1}q_k + r_k & 0 < r_k < r_{k-1} \\ r_{k-1} = r_kq_{k+1} + 0 & \end{array}$$

Theorem 0.2. Euclid's Lemma.

If p is a prime that divides ab , then p divides a or p divides b .

Theorem 0.3. Fundamental Theorem of Arithmetic.

Every integer greater than 1 is a prime or a product of primes. This product is unique, except for the order in which the factors appear. Thus if

$$\begin{aligned} n &= p_1p_2 \cdots p_r, & \text{and} \\ n &= q_1q_2 \cdots q_s, \end{aligned}$$

where the p 's and q 's are primes, then $r = s$ and, after renumbering the q 's, we have $p_i = q_i$ for all i .

Proof of (9). Let S be the set of positive integers n satisfying

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Base case.

S contains 1 since $1 = \frac{1(1+1)}{2}$.

Inductive step.

Let n be a positive integer and suppose that $n \in S$.

By this assumption,

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Adding $n+1$ to both sides, we have

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\ 1 + 2 + \cdots + n + (n+1) &= \frac{n^2 + n + 2n + 1}{2} \\ 1 + 2 + \cdots + n + (n+1) &= \frac{n^2 + 3n + 1}{2} \\ 1 + 2 + \cdots + n + (n+1) &= \frac{(n+1)[(n+1) + 1]}{2}. \end{aligned}$$

Therefore $n+1 \in S$.

By the First Principle of Mathematical Induction, S contains all positive integers. \square

Proof of (10). By exhaustion, we analyze the small postage values to see which can be composed of 4 and 9 cent stamps.

1			15	
2			16	$4 \cdot 4$
3			17	$1 \cdot 9 + 2 \cdot 4$
4	$1 \cdot 4$		18	$2 \cdot 9$
5			19	
6			20	$5 \cdot 4$
7			21	$1 \cdot 9 + 3 \cdot 4$
8	$2 \cdot 4$		22	$2 \cdot 9 + 1 \cdot 4$
9	$1 \cdot 9$		23	
10			24	$6 \cdot 4$
11			25	$1 \cdot 9 + 4 \cdot 4$
12	$3 \cdot 4$		26	$2 \cdot 9 + 2 \cdot 4$
13	$1 \cdot 9 + 1 \cdot 4$		27	$3 \cdot 9$
14			28	$7 \cdot 4$

Sketch of the rest of proof. Argue that $24, 25, 26, 27 \in S$, and for $n > 27$, $n - 4 \in S \Rightarrow n \in S$. The Second Principle of Mathematical Induction gives the desired result, namely, that 23 is the largest amount that cannot be composed of 4 and 9 cent stamps.

Question. How is the question related to expressing

$$\begin{aligned} 1 &= 4 \cdot s + 9 \cdot t, \\ -1 &= 4 \cdot s' + 9 \cdot t' \quad ? \end{aligned}$$