

1. a) Let x, y be integers where $d = ax + by$. If $e|b$ and $e|a$, then $e|ax$ and $e|by$, so $e|ax + by$ thus $e|d$ as desired.

b) We denote the set $S = \{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}$. If $a < 0$ or $b < 0$, set x_0 or y_0 as -1 or else 1. The resulting sum of $ax_0 + by_0$ is positive thus in S . By the Well-Ordering Principle, since S is non-negative and non-empty, let $d = \min(S)$ exists. By our construction of S , d is also the smallest positive integer in the form $ax + by$.

By contradiction, $d \nmid a$, then by the Division Algorithm, there exist integers q, r where $0 \leq r < |d|$ that $r = a - dq$ and $r = a - q(ax + by) = a(1 - qx) + b(-qy)$. Since $d \nmid a$, $r \neq 0$ and $0 < d$, so $0 < r < d$. This implies $r \in S$ and contradicts the minimality of d . This means $d|a$. Conversely, the same contradiction applies for $d \nmid b$, so $d|b$. Hence, $d|a$ and $d|b$ as desired.

c) a) By following the algorithm, we see that $(69, 2025) \rightarrow (24, 69) \rightarrow (21, 24) \rightarrow (3, 21) \rightarrow (0, 3)$. Thus, $\ell(69, 2025) = 5$.

b) Consider for $\ell(2025^{69} - 1, 2025^{420} - 1)$ that:

$$\begin{aligned} & (2025^{69} - 1)(2025^{351} + 2025^{282} + 2025^{213} + 2025^{144} + 2025^{75} + 2025^6) \\ &= 2025^{420} - 2025^6 \\ &= (2025^{420} - 1) - (2025^6 - 1) \end{aligned}$$

Thus:

$$2025^{420} - 1 = (2025^{69} - 1)(2025^{351} + 2025^{282} + \dots + 2025^6) + (2025^6 - 1)$$

And continuing the process with $(2025^{69} - 1)$:

$$2025^{69} - 1 = (2025^6 - 1)(2025^{63} + 2025^{57} + \dots + 2025^3) + (2025^3 - 1)$$

And finally, with $(2025^3 - 1)$:

$$(2025^3 - 1)(2025^3 + 1) = (2025^6 - 1) - (0)$$

With these information, we can see that $(2025^{69} - 1, 2025^{420} - 1) \rightarrow (2025^6 - 1, 2025^{69} - 1) \rightarrow (2025^3 - 1, 2025^6 - 1) \rightarrow (0, 2025^3 - 1)$. Hence, $\ell(2025^{69} - 1, 2025^{420} - 1) = 4$.

c) We prove that for all a and for all $b \geq a$, $\ell(a, b) \leq 2 \log_2(a) + 2$. For the base case $a = 1$, let b be an arbitrary positive integer where $b \geq 1$, we see that $(1, b) \rightarrow (0, 1)$. For all $b \geq 1$, $\ell(1, b) = 2$, and $2 = 2 \log_2(1) + 2$.

For the inductive hypothesis, we assume every integer m where $1 \leq m < k$, for all $b \geq m$, $\ell(m, b) \leq 2 \log_2(m) + 2$. We consider the case k . Let b be an arbitrary positive integer where $b \geq k$ and r be, from the Division Algorithm, where $r = b - kq$ for some integer q and $0 \leq r < b$. We consider all cases for r .

If $r = 0$, then $(k, b) \rightarrow (0, k)$, so $\ell(k, b) = 2$ and $2 < 2 \log_2(k) + 2$ since $k > 1$.

If $1 \leq r \leq \frac{k}{2}$, then $(k, b) \rightarrow (r, k)$ or $1 + \ell(r, k)$. By the induction hypothesis, $\ell(r, k) \leq 2 \log_2(r) + 2$ and $r \leq \frac{k}{2}$, thus:

$$\begin{aligned} 1 + \ell(r, k) &\leq 2 \log_2(r) + 2 + 1 \\ 1 + \ell(r, k) &\leq 2(\log_2(r) + 0.5) + 2 \\ \ell(k, b) &\leq 2 \log_2(\sqrt{2}r) + 2 \leq 2 \log_2\left(\frac{\sqrt{2}}{2}k\right) + 2 \\ \ell(k, b) &< 2 \log_2(k) + 2 \end{aligned}$$

If $r > \frac{k}{2}$, $\lfloor \frac{k}{r} \rfloor = 1$, so the remainder of r divided by k is equal to $k - r$ as $(k - r) = k - r(1)$. This means $(k, b) \rightarrow (r, k) \rightarrow (k - r, r)$. Thus, $\ell(k, b) = 2 + \ell(k - r, r)$. By the induction hypothesis, $\ell(k - r, r) \leq 2 \log_2(k - r) + 2$ and since $k - r < \frac{k}{2}$, we get:

$$\begin{aligned} 2 + \ell(k - r, r) &\leq 2 \log_2(k - r) + 2 + 2 \\ 2 + \ell(k - r, r) &\leq 2(\log_2(k - r) + 1) + 2 \\ \ell(k, b) &\leq 2 \log_2(2(k - r)) + 2 \\ \ell(k, b) &< 2 \log_2(k) + 2 \end{aligned}$$

Hence, for all $k \geq 2$, $\ell(k, b) \leq 2 \log_2(k) + 2$ holds true. By induction on a , the bound $\ell(a, b) \leq 2 \log_2(a) + 2$ holds for all $1 \leq a \leq b$.

d) By Proposition 2.13, $\gcd(a, c)|c$ and $\gcd(a, c)|a$, so the fractions $\frac{-c}{ad-bc}$ and $\frac{a}{ad-bc}$ are indeed integers. Thus:

$$(an + b)\left(\frac{-c}{ad - bc}\right) + (cn + d)\left(\frac{a}{ad - bc}\right) = \frac{-can - bc + can + ad}{ad - bc} = \frac{ad - bc}{ad - bc} = 1$$

Hence, there exist integers x and y where $(an + b)x + (cn + d)y = 1$. By Corollary 2.18, the existence of such x and y implies that the $\gcd(an + b, cn + d) = 1$ as desired.

e) a) The remainder is going to be 1.

b) To start, we convert the hints in the form of congruences:

$$(625 \equiv 2 \pmod{89}) \quad (800 \equiv -1 \pmod{89}) \quad (2^{11} \equiv 1 \pmod{89})$$

We note that $625 \cdot 18 - 800 \cdot 9 = 2(2025)$. Under Lemma 3.9, we add $(625 \cdot 18 \equiv 36 \pmod{89})$ and $(800 \cdot -9 \equiv 9 \pmod{89})$, so $(4050 \equiv 45 \pmod{89})$. By Exercise 3.5, let m, a, b, c be integers and we see that $(45 \cdot 90 \equiv 45 \cdot 1 \pmod{89})$ can be expressed in the form $(ac \equiv bc \pmod{m})$. Since $\gcd(45, 89) = 1$ and $\frac{89}{\gcd(45, 89)} = 1$, so we get:

$$90 \equiv 1 \pmod{\frac{89}{\gcd(45, 89)}}$$

$$2 \cdot 3^2 \cdot 5 \equiv 1 \pmod{89}$$

Using Lemma 3.9 again and multiplying by itself 22 times, we get $(2^{22} \cdot 3^{44} \cdot 5^{22} \equiv 1 \pmod{89})$. We do the same with $(2^{11} \equiv 1 \pmod{89})$ and multiply by itself to get $(2^{22} \equiv 1 \pmod{89})$. Using congruence's symmetric property for $(1 \equiv 2^{22} \pmod{89})$ and applying its transitive property to $(2^{22} \cdot 3^{44} \cdot 5^{22} \equiv 1 \pmod{89})$ and $(1 \equiv 2^{22} \pmod{89})$, we get:

$$2^{22} \cdot 3^{44} \cdot 5^{22} \equiv 2^{22} \pmod{89}$$

This implies $89 | 2^{22} \cdot (3^{44} \cdot 5^{22} - 1)$. Since $89 \nmid 2^{22}$ and 89 is a prime, by Euclid's Lemma, $89 | 3^{44} \cdot 5^{22} - 1$. Since $3^{44} \cdot 5^{22} = 2025^{11}$, we get $89 | 2025^{11} - 1$ as desired.

c) To start, we note that $11 \cdot 184 + 1 = 2025$. Thus, for $2025^{11} - 1$:

$$\begin{aligned} &= 2025^{10}(11 \cdot 184 + 1) - 1 \\ &= 2025^{10} \cdot 11 \cdot 184 + 2025^{10} - 1 \\ &= 2025^{10} \cdot 11 \cdot 184 + 2025^9(11 \cdot 184 + 1) - 1 \\ &= 2025^{10} \cdot 11 \cdot 184 + 2025^9 \cdot 11 \cdot 184 + \dots + 2025^2 \cdot 11 \cdot 184 + 2025 \cdot 11 \cdot 184 + 11 \cdot 184 + 1 - 1 \\ &= 11 \cdot 184(2025^{10} + 2025^9 + \dots + 2025^1 + 1) \end{aligned}$$

Since $(2025 \equiv 1 \pmod{11})$, by Lemma 3.9, each element in the sum expressible by 2025^k for some $k \in \mathbb{N}$ when multiplying $(2025 \equiv 1 \pmod{11})$ by itself k times results in $(2025^k \equiv 1 \pmod{11})$. Meanwhile, $1 \equiv 1 \pmod{11}$, so applying Lemma 3.9 again and summing all the 11 terms in the sum, we get:

$$2025^{10} + 2025^9 + \dots + 2025^1 + 1 \equiv 11 \pmod{11}$$

Since $11 | 11$ and $11 | (2025^{10} + 2025^9 + \dots + 2025^1 + 1) - 11$, it implies that:

$$11 | (2025^{10} + 2025^9 + \dots + 2025^1 + 1)$$

Thus, there exist $q \in \mathbb{Z}$ where $11q$ is equal to the sum. Hence, $2025^{11} - 1 = 11 \cdot 184(11q)$, which gives us the $11^2 | 2025^{11} - 1$ as desired.