18RMM4

Himadri Mandal

November 14, 2021

§1 Solution

Problem 1.1

Let a, b, c, d be positive integers such that $ad \neq bc$ and $gcd(a, b, c, d) = 1$. Let S be the set of values attained by $\gcd(an + b, cn + d)$ as n runs through the positive integers. Show that S is the set of all positive divisors of some positive integer.

Solution. Denote $F(a, b, c, d, n) = \gcd(an + b, cn + d)$. Therefore $F(a, b, c, d, n) = F(c, d, a, b, n)$. Note that

$$\gcd(an + b, cn + d) = \gcd((a - c)n + (b - d), cn + d)$$

which means $F(a, b, c, d, n) = F((a - c), (b - d), c, d, n)$. WLOG assume $a + b \geq c + d$

$$F(a, b, c, d, n) = F((a - c), (b - d), c, d, n) \text{ Here, } [(a - c) + (b - d)] < (a + b)$$

The sum $(a + b)$ is strictly decreasing, perform this operation until $(a + b) < (c + d)$ in which case flip the order $(a, b, c, d, n) \to (c, d, a, b, n)$ such that the inequality $(c + d) \geq (a + b)$ is maintained. Also, $\gcd(a, b, c, d) = \gcd(\gcd(a, c), \gcd(b, d)) = \gcd(\gcd(a - c, c), \gcd(b - d, d)) = \gcd(a - c, b - d, c, d) = 1$.
Now note that the sum $(a + b + c + d)$ is also decreasing. Therefore, $c = 0$ at some point. So it suffices to show that

Claim — $ad \neq 0$ and $\gcd(a, b, d) = 1$. Let S be the set of values attained by $\gcd(an + b, d)$ as n runs through the positive integers. S is the set of all positive divisors of some positive integer.

Proof. Let $\mathbb{G} = \{\gcd(an + b, d) : n \geq 1\}$. WLOG assume $\gcd(a, b) = 1$. Let $g = \gcd(a, d)$ $a = g\alpha, d = g\beta$, we would be done if we show that $q|\beta \implies q \in \mathbb{G}$

$$g\alpha n + b \equiv q \pmod{\beta}$$

$$\text{Take } n \equiv \frac{q - b}{g\alpha} \pmod{\beta}$$

which proves the claim. □

And we are done. □