**MATH 465 NUMBER THEORY, SPRING TERM 2025, SOLUTIONS 3**

1. Show that if $ad - bc = \pm 1$, then $(a+b, c+d) = 1$.
We have $(a+b, c+d) | (a+b)d - b(c+d) = ad - bc = \pm 1$.

2. Suppose that $m \in \mathbb{N}$ and $n \in \mathbb{N}$. Prove that there are integers $a$, $b$ such that $(a, b) = m$ and $[a, b] = n$ if and only if $m|n$.
First suppose that $m|n$. Then choose $a = m$, $b = n$. Then $(a, b) = m(1, b/m) = m$ and $[a, b] = ab/(a, b) = mn/m = n$. Now suppose that there are $a$, $b$ with $(a, b) = m$ and $[a, b] = n$. Then there are $u$, $v \in \mathbb{N}$ such that $a = um$, $b = vm$. Hence $muv = \frac{mumv}{m} = \frac{ab}{(a,b)} = [a, b] = n$.

3. Find $(1819, 3587)$, and obtain the complete solution in integers $x$ and $y$ to $1819x + 3587y = (1819, 3587)$.

| | | | |
|---|---|---|---|
| | 3587 | 1 | 0 |
| 1 | 1819 | 0 | 1 |
| 1 | 1768 | 1 | −1 |
| 34 | 51 | −1 | 2 |
| 1 | 34 | 35 | −69 |
| 2 | 17 | −36 | 71 |

Thus $17 = (16801, 2024) = (71)1819 + (-36)3587 = (71 + 211t)1819 + (-36 - 107t)3587$ for any $t \in \mathbb{Z}$.

4. Let $\{F_n : n = 1, 2, \ldots\}$ be the Fibonacci sequence defined by $F_1 = 1$, $F_2 = 1$, $F_{n+1} = F_n + F_{n-1}$ and let

$$\theta = \frac{1+\sqrt{5}}{2} = 1.6180339887498948482045868343656\ldots.$$

(i) Prove that

$$F_n = \frac{\theta^n - (-\theta)^{-n}}{\sqrt{5}}.$$

(ii) Suppose that $a$ and $b$ are positive integers with $b < a$ and we adopt the notation used in the description of Euclid's algorithm. Prove that for $k = 0, 1, \ldots, s-1$ we have $F_k \le r_{s-1-k}$ and

$$s \le 1 + \frac{\log 2b\sqrt{5}}{\log \theta}.$$

This shows that Euclid's algorithm runs in time at most linear in the bit size of $\min(a, b)$.

(i) $\theta$ and $\phi = -1/\theta = (1-\sqrt{5})/2$ are both solutions to $x^2 - x - 1 = 0$ and hence to $x^{n+1} = x^n + x^{n-1}$. Moreover (i) holds for $n = 0$ and 1 and hence by induction for all $n$. (ii) $r_{s-1} \geq 1 \geq 0 = F_0$ and $r_{s-2} \geq 1 = F_1$. Suppose that $2 \leq k \leq s-1$ and $F_j \leq r_{s-1-j}$ holds for $0 \leq j \leq k-1$. Then $r_{s-1-k} = r_{s-1-(k-1)}q_{s-k+1} + r_{s-1-(k-2)} \geq r_{s-1-(k-1)} + r_{s-1-(k-2)} \geq F_{k-1} + F_{k-2}$, so by induction on $k$, $r_{s-1-k} \geq F_k$. Let $k = s-1$. Then $F_{s-1} \leq r_0 = b$ and the desired inequality follows by taking logs and applying the formula for $F_{s-1}$.