Homework 2

Sean Eva

February 2022

14. *Proof.* We will proceed by mathematical induction.
Base Case: Consider when $n = 1,$. Then it holds that $f_{k+1}f_{k-1} - f_k^2 = f_2 f_0 - f_1^2 = 1 * 0 - 1^2 = -1 = (-1)^1$.
Inductive Step: Assume the equality holds for $n = k$, that is to say that $f_{k+1}f_{k-1} - f_k^2 = (-1)^k$. We want to show that $f_{k+2}f_k - f_{k+1}^2 = (-1)^{k+1}$. So then we have

$$\begin{aligned} f_{k+2}f_k - f_{k+1}^2 &= (f_k + f_{k+1})f_k - f_{k+1}^2 \\ &= f_k^2 + f_{k+1}f_k - f_{k+1}^2 \\ &= f_{k+1}(f_k - f_{k+1}) + f_k^2 \\ &= f_{k+1}(-f_{k-1}) + f_k^2 \\ &= (f_{k+1}f_{k-1} - f_k^2)(-1)^1 \\ &= (-1)^k(-1)^1 \\ &= (-1)^{k+1}. \end{aligned}$$

Therefore, since $n = k$ implied that $n = k + 1$ is true then we know that the equality is true for all $n \in \mathbb{N}$ by mathematical induction. □

34. *Proof.* We will proceed by mathematical induction.

Base Case: Consider when $n = 1$, then it holds that $F^n = \begin{pmatrix} f_2 & f_1 \\ f_1 & f_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$.

Inductive Step: Assume the equality holds for $n = k$, that is to say that $F^k = \begin{pmatrix} f_{k+1} & f_k \\ f_k & f_{k-1} \end{pmatrix}$. Then we want to show that the equality is true for $n = k + 1$. By matrix multiplication we have that $F^{k+1} = F^k * F = \begin{pmatrix} f_{k+1} & f_k \\ f_k & f_{k-1} \end{pmatrix} * \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} f_{k+1} + f_k & f_{k+1} \\ f_{k+1} & f_k \end{pmatrix} = \begin{pmatrix} f_{k+2} & f_{k+1} \\ f_{k+1} & f_k \end{pmatrix}$. This shows that the equality holds for $n = k + 1$. Therefore, since $n = k$ is true implies that $n = k + 1$ is true, the equality is true for all $n \in \mathbb{Z}^+$ by mathematical induction. □

35. *Proof.* From the LHS we get that $\det(F^n) = \det(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n) = \det(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix})^n = (-1)^n$.

From the RHS we get that $\det(\begin{pmatrix} f_{n+2} & f_{n+1} \\ f_{n+1} & f_n \end{pmatrix}) = f_{n+2}f_n - f_{n+1}^2$.

Therefore, we have that $f_{n+2}f_n - f_{n+1}^2 = (-1)^n$ as desired from Exercise 14. □

16. *Proof.* Consider $a = 6, b = 3, c = 8$. We get that $6|3 * 8, 6|24$. However, $6 \not| 3$ and $6 \not| 8$ as desired. □

23. *Proof.* We can represent a number with decimal expansion $(a_n a_{n-1}...a_1 a_0)_1 0$ as $10x+a_0$ where $x = a_n a_{n-1}...a_1$ and $a_0 = 5$ as specified in the rule. Therefore, if we take $(10x+5)^2 = 100x^2 + 100x + 25 = 100x(x+1) + 25$. In this expansion we have the $(a_n a_{n-1}...a_1) * ((a_n a_{n-1}...a_1) + 1)$ represented as $x(x+1)$, and the coefficient 100 to this term moves the number over two digits to allow us to add 25 to the end as appending the digits with 25 as in the rule. This shows the rule as intended. Therefore, the rule is verified and valid. □

20. *Proof.* Consider the $n+1$ integers, $1, 11, 111, ..., 111...111(n+11s)$. When divided by n, they leave $n+1$ remainders. By the pigeonhole principle, two of these remainders are equal, so the difference in the corresponding integers, an integer of the form 111...000, is divisible by n. If n is relatively prime to 10, then we may divide out all powers of 10, to obtain an integer of the form 111...1 that remains divisible by n. □

29. *Proof.* Suppose $n > 1$ as if $n = 1$, then $\frac{1}{1}$ is an integer. Suppose $m < n$ so that,

$$\begin{aligned}\frac{1}{n}+\frac{1}{n+1}+...+\frac{1}{n+m} &\leq \frac{1}{n}+\frac{1}{n+1}+...+\frac{1}{2n-1}\\ &< \frac{1}{n}+\frac{1}{n}+...+\frac{1}{n}\\ &< \frac{n}{n}\\ &< 1.\end{aligned}$$

Therefore, $\frac{1}{n}+\frac{1}{n+1}+...+\frac{1}{n+m}$ is not an integer. Now suppose that $m \geq n$. Then, by Bertrand's Postulate, there is a prime p such that $n < p < 2n < n+m$. Let p be the largest such prime in the interval. Then $n+m < 2p$, if not, then there is another prime q such that $p < q < 2p < n+m$ which contradicts the choice of p. To come to the contradiction, let $\frac{1}{n}+\frac{1}{n+1}+...+\frac{1}{n+m} = x$ where x is an integer. In this, p occurs as a factor in only one denominator in the expression because $2p > n+m$. Now, let $Q = \prod_{k=n}^{n+m} k$ and $Q_i = \frac{Q}{i}, i = n, n+1, ..., n+m$. Multiply x by Q to get, $Q_n, Q_{n+1} + ... + Q_p + ... + Q_{n+m} = Qx$. We can rewrite this as $Q_p = Qx - (Q_n + Q_{n+1} + ... + Q_{p-1} + Q_{p+1} + ... + Q_{n+m}) = pN$ where N is an integer. Thus, $p|Q_p$ which is a contradiction as $Q_i = \frac{Q}{i}, i = n, n+1, ..., n+m$.. Therefore, $\frac{1}{n}+\frac{1}{n+1}+...+\frac{1}{n+m}$ □

34. *Proof.* According to the prime number theorem $\frac{\pi(x)}{\frac{x}{\ln x}} = 1$ where $\pi(x)$ is the number of primes less than or equal to x. Dirichlet's Theorem states that if a, b are relatively prime positive integers, then there are infinite number of primes in the arithmetic progression $an + b, n = 1, 2, 3, ...$ Let's choose a common difference d where d is an even number and a number b, which is coprime to d. Fix a number M. Consider the terms of the arithmetic progression $an + b$ for which $an + b < M$. Suppose there is no such pair of successive prime with the same common difference. So, if there is a prime for $n = 1$, then for $n = 2$. there will be no prime and so on. Thus, the maximum number of primes is possible when we have a prime for $n = 1, 3, 7, 15, ...$ That is, when the common difference of the different values of n is in the sequence of powers of 2. That is, according to the above logic, the maximum number of primes varies in a logarithmic fashion, that is $\log(M)$. For a general number x, it must vary as $\log(x)$. But according to the prime number theorem, the actual number of primes is a lot more than that. Thus, by the pigeonhole principle, there must be at least one common different (out of the powers of 2), for which we have tow pairs of successive primes. For large values of M, there will an infinite number of primes with common difference as even there are infinite number of primes in the arithmetic progression. Therefore, for any integer N, there will be more than N pair of successive primes having a common difference of an even integer. □

11. *Proof.* Let $d = (a^2 + b^2, a + b)$ then we have that $d|a^2 + b^2, d|a + b$ and $d|a^2, d|b^2.d|a, d|b$. Therefore, $d \leq (a^2, b^2, a, b)$ Now since we know that $d \leq (a, b)$ and we are given that $(a, b) = 1$ then we know that $d \leq (a^2, b^2, 1) = 1$ □

22. *Proof.* For $n = 1, a_1 = 1 * a_1$. Let $n = k$ and let the greatest common divisor of $a_1, a_2, ..., a_{k-1}, a_k$ be d, which is the least positive integer that is a linear combination of $a_1, a_2, ..., a_{k-1}, a_k$. So, $a_1x_1 + a_2x_2 + ... + a_kx_k = d$. Let D be the gcd of $a_1, a_2, ..., a_k, a_{k+1}$. So then, $D = (a_1, a_2, ..., a_k, a_{k+1}) = ((a_1, a_2, ..., a_k), a_{k+1}) = (d, a_{k+1})$. Since we have that D is the gcd of d and a_{k+1}, there are integers y_1, y_2 such that $dy_1 + a_{k+1}y_2$ is least. So $D = dy_1 + a_{k+1}y_2$. Now we get that $D = (a_1x_1 + a_2x_2 + ...a_kx_k)y_1 + a_{k+1}y_2 = a_1(x_1y_1) + a_2(x_2y_1) + ... + a_k(x_ky_1) + a_{k+1}y_2$. Therefore, $a_1, a_2, ..., a_{n-1}, a_n$, not all zero, is the least positive integer that is a linear combination of $a_1, a_2, ..., a_n$. □

24. *Proof.* We can construct the combination $1 = 5(3k+2) - 3(5k+3)$. This shows using the Euclidean algorithm that $(3k+2, 5k+3) = 1$ and that they are relatively prime. □

10. *Proof.* Let a, b be a pair of integers, there exists $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$. Consider the set $K = \{ax + by | x, y \in \mathbb{Z}\}$. Let k be the smallest positive element of K. Since $k \in K$, there are $x, y \in \mathbb{Z}$ so that $k = ax+by$. Therefore, we can rewrite this as $a = qk+r, 0 \leq r < k$. Therefore, it can be written as $r = a - qk = a - q(ax + by) = a(1 - qx) + b(-qy) \in K$. Since k is the smallest positive element in K. This implies that r must be 0. Thus, $a = qk$ and therefore, $k|a$ and $k|b$. This implies that k is a common divisor of a and b, and therefore, $k \leq \gcd(a, b)$. Since $\gcd(a, b)$ divides both a and b, and $k = ax + by, \gcd(a, b)$ divides k. Since $\gcd(a, b)$ divides k and $k \leq \gcd(a, b)$, get the result that $k = \gcd(a, b)$. Therefore, this becomes $\gcd(a, b) = ax + by$. □

23. *Proof.* Let $m \in \mathbb{Z}$ so that d has no more than m bits and that q has $2m$ bits, appending extra 0 to the front of q is necessary. Then, $m = O(\log_2 q) = O(\log_2 d)$. Then we can use the algorithm for dividing q by d in $O(m^2) = O(\log_2 q \log_2 d)$ bit operations. Now let n be the number of steps needed in the Euclidean algorithm to find (a, b). Then we know that $n = O(\log_2 a)$. Let q, r, then the total number of bit operations for divisions in the Euclidean algorithm is $\sum_{i=1}^{n} O(\log_2 q \log_2 r) = \sum_{i=1}^{n} O(\log_2 q \log_2 b) = O(\log_2 b \sum_{i=1}^{n} \log_2 q_i) = O(\log_2 b \log \prod_{i=1}^{n} q_i$. Dropping the remainders in each step of the Euclidean algorithm, the system of inequalities $r_i \geq r_{i+1} q_{i+1}$ for $i = 0, 1, 2, ..., n-1$, multiplying these inequalities together yields $\prod_{i=0}^{n-1} r_i \geq \prod_{i=1}^{l} r_i q_i$. Cancelling common factors reduces this to $a = r_0 \geq r_n \prod_{i=1}^{n} q_i$. Therefore, from above, the total number of bit operations is $O(\log_2 b \log_2 \prod_{i=1}^{n} q_i) = O(\log_2 b \log_2 a) = O((\log_2 a)^2)$. □

9. *Proof.* Let n be a powerful number. So, the prime factorization of n is, $n = p_1^{2x_i} \times p_2^{2x_2} \times ... \times p_r^{2x_r} \times q_1^{2x_1+3} \times ... \times q_s^{2x_s+3} = (p_1^{x_1} \times p_2^{x_2} \times ... \times p_r^{x_r} \times q_1^{x_1} \times ... \times q_s^{x_s})^2 \times (q_1 \times q_2 \times ... \times q_s)^3$. Thus, n is written as a product of a square and a cube. Therefore, every powerful number can be written as the product of a perfect square and perfect cube. □

18. *Proof.* Let $2 = \alpha\beta$. Since, $N(\alpha\beta) = N(\alpha)N(\beta)$, therefore we get that $4 = N(2) = N(\alpha)N(\beta)$. Then, the possible values of $N(\alpha)$ are $1, 2, 4$. Now, let $\alpha = a + b\sqrt{-5}$ then, $a^2 + 5b^2 = 1, 2, 4$. So either $b = 0$ and $a = \pm 1$ or $b = 0$ and $a = \pm 2$. Since $a = \pm 1, b = 0$ is excluded, therefore, $a = \pm 2, b = 0$ but then $N(\alpha) = 4, N(\beta) = 1$. Hence 2 is a prime number of the form $a + b\sqrt{-5}$. □