Primes and the Fundamental Theorem of Arithmetic

THEOREM: LET $a \in \mathbb{Z}$, $a \notin \{-1,0,1\}$. THEN, a CAN BE EXPRESSED AS A PRODUCT OF PRIMES. THIS REPRESENTATION IS UNIQUE, APART FROM THE ORDER IN WHICH THE FACTORS OCCUR AND THE SIGN. WHEN $a = \pm \prod_{j=1}^{r} p_j^{r_j}$ WHERE EACH $r_j > 0$ AND p_j IS A PRIME, WE SAY THAT a IS WRITTEN IN CANONICAL FORM.

EXERCISE 1: LET $a \in \mathbb{Z}$, $a > 1$. PROVE THAT a IS A SQUARE IF AND ONLY IF IN THE CANONICAL FORM OF a ALL THE EXPONENTS OF THE PRIMES ARE EVEN INTEGERS.

SOLUTION: SUPPOSE FIRST THAT a IS A SQUARE. THEN, THERE EXISTS $m \in \mathbb{Z}$ SUCH THAT $a = m^2$. SINCE $a \notin \{0,1\}$ WE OBSERVE $m \notin \{-1,0,1\}$. THEN, BY THE FUNDAMENTAL THEOREM OF ARITHMETIC, THERE EXIST PRIMES p_i $(1 \le i \le k)$ AND POSITIVE INTEGERS r_i $(1 \le i \le k)$ SUCH THAT $m = \pm \prod_{j=1}^{k} p_j^{r_j}$. WE THUS HAVE $a = m^2 = \left(\prod_{j=1}^{k} p_j^{r_j}\right)^2 = \prod_{j=1}^{k} p_j^{2r_j}$. THIS SHOWS ALL EXPONENTS IN THE CANONICAL FORM OF a ARE EVEN. CONVERSELY, SUPPOSE ALL THE EXPONENTS OF THE PRIMES IN THE CANONICAL FORM ARE EVEN. THEN, WE CAN WRITE $a = \prod_{j=1}^{k} p_j^{r_j}$ WHERE p_j IS A PRIME, $p_i < p_j$ IF $i < j$ $(1 \le i,j \le k)$ AND $r_j > 0$ IS EVEN $(1 \le j \le k)$. THUS, FOR EVERY j $(1 \le j \le k)$, THERE EXISTS $t_j \in \mathbb{N}$ SUCH THAT $r_j = 2t_j$. THEREFORE,

$$a = \prod_{j=1}^{k} p_j^{r_j} = \prod_{j=1}^{k} p_j^{2t_j} = \prod_{j=1}^{k} \left(p_j^{t_j}\right)^2 = \left(\prod_{j=1}^{k} p_j^{t_j}\right)^2.$$

SINCE $\prod_{j=1}^{k} p_j^{t_j} \in \mathbb{Z}$ WE THUS HAVE a IS A SQUARE. THE RESULT FOLLOWS.

EXERCISE 2: An integer is said to be square-free if it is not divisible by the square of any integer greater than 1. Prove:

(i) An integer $m>1$ is square-free if and only if m can be factored into a product of distinct primes.

(ii) Every integer $m>1$ is the product of a square-free integer and a perfect square.

SOLUTION: Let $m \in \mathbb{N}$, $m>1$. Then, by the F.T.A, m can be written in canonical form as follows: $m = \prod_{j=1}^{k} p_j^{r_j}$ where $p_1 < p_2 < \ldots < p_j < \ldots < p_k$ are all primes and $r_j \in \mathbb{N}$ $(1 \leq j \leq k)$. Suppose there exists ℓ $(1 \leq \ell \leq k)$ such that $r_\ell \geq 2$. Then, $m = \left(\prod_{\substack{j=1 \\ j \neq \ell}}^{k} p_j^{r_j}\right) \cdot p_\ell^{r_\ell - 2} \cdot p_\ell^2$ which implies that $p_\ell^2 \mid m$, contradicting that m is square-free. Therefore, for every j $(1 \leq j \leq k)$, it must be $r_j = 1$. So, m is a product of distinct primes. Conversely, we proceed by showing the contrareciprocal proposition is true. So, assume that m is not square-free. Then, it admits a divisor of the form d^2 where $d>1$. Then, by Ex. 1, in the canonical form of d^2, all the exponents of the primes are even integers. Since $d>1$, there must exist a prime q such that $q^2 \mid d^2$. Then, as $q^2 \mid d^2$ and $d^2 \mid m$ we thus have $q^2 \mid m$. This shows that $m \neq p_1 . p_2 . \ldots . p_k$ for distinct primes p_j $(1 \leq j \leq k)$. We conclude that if the primes occuring in the prime factorization are distinct then m is square-free. This shows that (i) holds. We next prove the latter part of the exercise.

Let $m \in \mathbb{N}$, $m>1$. Let $m = \prod_{j=1}^{k} p_j^{r_j}$ be the canonical form of m. Since r_j is a positive integer, by the algorithm division theorem, for every j $(1 \leq j \leq k)$ there exist $\alpha_j, \beta_j \in \mathbb{N}$ such that $r_j = 2\alpha_j + \beta_j$ where $\beta_j \in \{0, 1\}$. Consider now the sets $A = \{j : \beta_j = 0\}$ and $B = \{j : \beta_j = 1\}$. Note that $A \cup B = \{1, \ldots, k\}$

AND $A \cap B = \phi$. IN ADDITION,

$$m = \prod_{j=1}^{k} p_j^{r_j} = \prod_{j \in A \cup B} p_j^{2\alpha_j + \beta_j} = \left(\prod_{j \in A} p_j^{2\alpha_j+\beta_j}\right) \cdot \left(\prod_{j \in B} p_j^{2\alpha_j+\beta_j}\right) = \left(\prod_{j \in A} p_j^{2\alpha_j}\right) \cdot \left(\prod_{j \in B} p_j^{2\alpha_j+1}\right).$$

$$= \left(\prod_{j \in A} p_j^{2\alpha_j}\right) \cdot \left(\prod_{j \in B} p_j^{2\alpha_j} \cdot p_j\right) = \left(\prod_{j \in A} p_j^{2\alpha_j}\right)\left(\prod_{j \in B} p_j^{2\alpha_j}\right)\left(\prod_{j \in B} p_j\right) = \left(\prod_{j \in A \cup B} p_j^{2\alpha_j}\right) \cdot \left(\prod_{j \in B} p_j\right).$$

CONSIDER $a := \prod_{j \in A \cup B} p_j^{2\alpha_j}$ AND $b := \prod_{j \in B} p_j$. NOTE THAT $a, b \in \mathbb{N}$. NOTICE THAT

$a = \prod_{j=1}^{k} p_j^{2\alpha_j} = \prod_{j=1}^{k} (p_j^{\alpha_j})^2 = \left(\prod_{j=1}^{k} p_j^{\alpha_j}\right)^2$ WHICH SHOWS THAT a IS A SQUARE. MOREOVER, SINCE b IS A PRODUCT OF DISTINCT PRIMES, BY (i) ABOVE, b IS SQUARE-FREE.

WE THUS HAVE $m = a \cdot b$ WHERE a IS A SQUARE AND b IS SQUARE-FREE.

EXERCISE 3: A POSITIVE INTEGER m IS CALLED SQUARE-FULL, OR POWERFUL, IF $p^2 \mid m$ FOR EVERY PRIME FACTOR p OF m. IF m IS SQUARE-FULL, SHOW THAT IT CAN BE WRITTEN IN THE FORM $m = a^2 \cdot b^3$, WITH $a, b \in \mathbb{N}$.

SOLUTION: LET $m \in \mathbb{N}$ SUCH THAT m IS SQUARE-FULL. BY FTA, m CAN BE WRITTEN AS A FINITE PRODUCT OF PRIMES. LET $m = \prod_{j=1}^{k} p_j^{\alpha_j}$ BE THE CANONICAL FORM OF m. SINCE m IS SQUARE-FULL, FOR EVERY j $(1 \le j \le k)$ WE HAVE $p_j^2 \mid m$. THIS SHOWS THAT $\alpha_j \geq 2$ FOR EVERY j $(1 \le j \le k)$. AS $\alpha_j \in \mathbb{N}$ $(1 \le j \le k)$, BY THE DAT, THERE EXIST $q_j, r_j \in \mathbb{N}$ SUCH THAT $\alpha_j = 2q_j + r_j$ WITH $r_j \in \{0,1\}$.

LET CONSIDER THE SETS $A := \{j : r_j = 0\}$ AND $B := \{j : r_j = 1\}$. NOTE $A \cap B = \phi$ AND $A \cup B = \{1, 2, \ldots, k\}$. WE ALSO NOTICE, FOR EVERY $j \in B$, $\alpha_j = 2q_j + 1$ AND $\alpha_j \geq 3$. THEN, $\alpha_j - 3 = 2(q_j - 1) \geq 0$. WE THEREFORE HAVE

$$m = \prod_{j \in A \cup B} p_j^{\alpha_j} = \left(\prod_{j \in A} p_j^{\alpha_j}\right) \cdot \left(\prod_{j \in B} p_j^{\alpha_j}\right) = \left(\prod_{j \in A} p_j^{2q_j}\right) \cdot \left(\prod_{j \in B} p_j^{2(q_j-1)} \cdot p_j^3\right)$$

$$= \left(\prod_{j \in A} p_j^{2q_j}\right)\left(\prod_{j \in B} p_j^{2(q_j-1)}\right)\left(\prod_{j \in B} p_j^3\right) = \prod_{j \in A} (p_j^{q_j})^2 \cdot \prod_{j \in B} (p_j^{(q_j-1)})^2 \cdot \prod_{j \in B} p_j^3$$

$$= \left(\prod_{j \in A} p_j^{q_j} \cdot \prod_{j \in B} p_j^{q_j-1}\right)^2 \cdot \left(\prod_{j \in B} p_j\right)^3 = a^2 \cdot b^3 \text{ WHERE}$$

$a := \prod_{j\in A} p_j^{q_j} \cdot \prod_{j\in B} p_j^{q_j-1} \in \mathbb{N}$ AND $b := \prod_{j\in B} p_j \in \mathbb{N}$. THE RESULT FOLLOWS.

EXERCISE 4: SHOW THAT EVERY POSITIVE INTEGER WHICH HAS REMAINDER 2 IN THE DIVISION BY 3 HAS A PRIME FACTOR WITH THIS PROPERTY AS WELL.

SOLUTION: LET $m \in \mathbb{N}$. BY THE DIVISION ALGORITHM THEOREM AND THE ASSUMPTION, $m = 3q+2$ FOR SOME $q \in \mathbb{N}$. SINCE $m > 1$, WE OBSERVE THERE EXISTS A PRIME p SUCH THAT $p \mid m$. NOTE THAT $3 \nmid p$. IN FACT, IF $3 \mid p$ THEN $3 \mid m$ AND SO $3 \mid 2$, A CONTRADICTION. THUS, BY THE ADT AND SINCE p IS AN ARBITRARY PRIME, WE HAVE EVERY PRIME FACTOR OF m IS EITHER OF THE FORM $3k+1$ OR $3k+2$ FOR SOME $k \in \mathbb{N}$. NOW, SUPPOSE EVERY PRIME FACTOR OF m IS A PRIME OF THE FORM $3k+1$. BY THE FTA, $m > 1$ IS A PRODUCT OF PRIMES NUMBERS WHICH ARE ALL OF THE FORM $3k+1$. THAT IS, THERE EXIST $\alpha_j > 0$, $k_j > 0$ AND PRIMES p_j $(1 \le j \le k)$ SUCH THAT $m = \prod_{j=1}^{k} p_j^{\alpha_j} = \prod_{j=1}^{k} (3k_j+1)^{\alpha_j}$. AS THE PRODUCT OF INTEGERS OF THE FORM $3k+1$ IS ALSO OF THAT FORM (YOU CAN PROVE THIS BY INDUCTION), THERE EXISTS $\ell \in \mathbb{N}$ SUCH THAT $m = 3\ell+1$. WE THUS HAVE $3\ell+1 = m = 3q+2$ WHICH IMPLIES THAT $3(\ell-q) = 1$. AS $\ell - q \in \mathbb{Z}$, THIS SHOWS THAT $3 \mid 1$, A CONTRADICTION. HENCE, IT CANNOT HAPPEN THAT EVERY PRIME FACTOR OF m IS A PRIME OF THE FORM $3k+1$. THEREFORE, THERE EXISTS A PRIME $p > 1$ SUCH THAT $p \mid m$ AND p IS OF THE FORM $3k+2$ FOR SOME $k \in \mathbb{N}$.

EXERCISE 5: GIVEN THAT $p \nmid m$ FOR ALL PRIMES $p \le \sqrt[3]{m}$, SHOW THAT $m > 1$ IS EITHER A PRIME OR THE PRODUCT OF TWO PRIMES.

SOLUTION: ASSUME TO THE CONTRARY THAT $m > 1$ CONTAINS AT LEAST THREE PRIME FACTORS. THAT IS, $m = \prod_{j=1}^{k} p_j$ WHERE p_j IS PRIME AND $k \geq 3$. SINCE p_j IS PRIME AND $p_j \mid m$ THEN, BY THE ASSUMPTION, $p_j > \sqrt[3]{m}$ $(1 \le j \le k)$. WE THEREFORE HAVE

$m = \sqrt[3]{m} \cdot \sqrt[3]{m} \cdot \sqrt[3]{m} < p_1 \cdot p_2 \cdot p_3 \leqslant \prod_{j=1}^{k} p_j = m$ WHICH IS A CONTRADICTION. THEN $r < 3$. THUS, $r \in \{1, 2\}$. SO, m IS EITHER A PRIME OR A PRODUCT OF 2 PRIMES.

EXERCISE 6: PROVE THAT $\sqrt{p}$ IS IRRATIONAL FOR ANY PRIME $p > 1$.

SOLUTION: ASSUME $\sqrt{p}$ IS RATIONAL FOR SOME $p > 1$. THEN, THERE EXIST $a, b \in \mathbb{N}$ SUCH THAT $\sqrt{p} = \frac{a}{b}$. WITHOUT LOSS OF GENERALITY, WE CAN ASSUME $\gcd(a,b) = 1$. THEN WE HAVE $pb^2 = a^2$. SO $p \mid a^2$ WHICH IMPLIES THAT $p \mid a$. THEN, $a = pk$ FOR SOME $k \in \mathbb{N}$. THEN, $pb^2 = a^2 = (pk)^2 = p^2k^2$ AND $p(b^2 - pk^2) = 0$. SINCE $p > 1$ IT MUST BE $b^2 = pk^2$. THIS SHOWS THAT $p \mid b^2$ AND SO $p \mid b$. NOW, SINCE $p \mid a$ AND $p \mid b$ WE GET $p \mid \gcd(a,b) = 1$ WHICH IS A CONTRADICTION AS $p > 1$. HENCE $\sqrt{p}$ IS IRRATIONAL.

EXERCISE 7: IF $a > 0$ AND $\sqrt[m]{a}$ IS RATIONAL, SHOW THAT $\sqrt[m]{a}$ MUST BE AN INTEGER.

SOLUTION: LET $a > 0$. SUPPOSE THAT $\sqrt[m]{a}$ IS RATIONAL. THEN, THERE EXIST $r, s \in \mathbb{N}$ SUCH THAT $\sqrt[m]{a} = \frac{r}{s}$ AND $\gcd(r,s) = 1$. THIS MEANS $s^m \cdot a = r^m$. SINCE $\gcd(r,s) = 1$ WE HAVE $\gcd(r^m, s^m) = 1$. SO, SINCE $r^m \mid r^m$ WE HAVE THAT $r^m \mid s^m \cdot a$ WHICH IMPLIES $r^m \mid a$. THEN, $r^m \cdot k = a$ FOR SOME $k \in \mathbb{N}$. THEN, $r^m = s^m \cdot a = s^m \cdot r^m \cdot k$ AND $r^m(1 - s^m k) = 0$. AS $r^m > 0$ WE MUST HAVE $s^m k = 1$. THIS SHOWS THAT $s^m = k = 1$ AND SO, $s = 1$ (IF $s > 1$ THEN $s^m > 1$, A CONTRADICTION). THUS, $\sqrt[m]{a}$ IS IRRATIONAL.

EXERCISE 8: FOR $m \geqslant 2$, SHOW THAT $\sqrt[m]{m}$ IS IRRATIONAL.

SOLUTION: LET $m \in \mathbb{N}$, $m \geqslant 2$. SUPPOSE THAT $\sqrt[m]{m}$ IS RATIONAL. THEN, BY EX.7, $\sqrt[m]{m}$ MUST BE AN INTEGER. ASSUME $\sqrt[m]{m} = a$ FOR SOME $a > 0$. THEN, $a^m = m = \binom{m}{1} < \sum_{k=0}^{m} \binom{m}{k} = 2^m$ BY THE

BINOMIAL THEOREM. SO, $a^m < 2^m$ IMPLIES THAT $a < 2$. THUS, $a = 1$. THIS MEANS THAT $m = a^m = 1^m = 1$, A CONTRADICTION. THEREFORE, $\sqrt[m]{m}$ IS NOT RATIONAL.

EXERCISE 9: SHOW THAT THERE ARE INFINITELY MANY PRIMES.

SOLUTION:

(i) SUPPOSE THERE ARE FINITELY MANY PRIMES p_j $(1 \leq j \leq m)$ AND LET p_m BE THE LARGEST ONE. CONSIDER THE INTEGER $N := p_m! + 1$. SUPPOSE THERE EXIST j $(1 \leq j \leq m)$ SUCH THAT $N = p_j$. THEN, $p_j \mid N$ AND $p_j \mid p_m!$ IMPLIES THAT $p_j \mid 1$, A CONTRADICTION. THIS SHOWS THAT N IS NOT IN OUR LIST OF PRIMES $p_1, p_2, \dots, p_m$. WE THUS HAVE THAT N IS COMPOSITE. AS $N > 1$, THERE EXISTS k $(1 \leq k \leq m)$ SUCH THAT $p_k \mid N$. SINCE p_k IS ONE OF THE FACTORS OF $p_m!$ WE ALSO HAVE $p_k \mid p_m!$. THIS SHOWS THAT $p_k \mid (N - p_m!)$ AND SO, $p_k \mid 1$, WHICH IS A CONTRADICTION AS $p_k > 1$. THEREFORE, THERE ARE INFINITELY MANY PRIMES.

(ii) ASSUME THAT THERE ARE ONLY FINITELY MANY PRIMES, SAY p_j $(1 \leq j \leq m)$. LET $A \subseteq \{1, \dots, m\}$ SUCH THAT $|A| = r$ AND CONSIDER $a := \prod_{j \in A} p_j$, $b := \prod_{j \in \{1, \dots, m\} \setminus A} p_j$. NOTE a AND b HAVE NO COMMON FACTORS. IN ADDITION, GIVEN j $(1 \leq j \leq m)$, WE EITHER HAVE $j \in A$ OR $j \in \{1, \dots, m\} \setminus A$. THIS SHOWS FOR EVERY j $(1 \leq j \leq m)$, EITHER $p_j \mid a$ OR $p_j \mid b$. SINCE $a > 1$, $b > 1$ THE NUMBER $a + b > 1$ MUST HAVE A PRIME FACTOR. THAT IS, $p_k \mid a + b$ FOR SOME $1 \leq k \leq m$. IT FOLLOWS FROM THE ABOVE COMMENTS THAT EITHER $p_k \mid a$ OR $p_j \mid b$. ASSUME NEXT THAT $p_k \mid a$. THEN, $p_k \mid (a+b) - a$. THAT IS, $p_k \mid b$. SIMILARLY, IF $p_k \mid b$, AS $p_k \mid a + b$ WE GET $p_k \mid a$. WE THEREFORE HAVE $p_k \mid \gcd(a, b)$ WHICH IMPLIES THAT $p_k \mid 1$, A CONTRADICTION AS $p_k > 1$. HENCE, THERE ARE INFINITELY MANY PRIMES.

EXERCISE 10: PROVE THAT IF $m > 2$ THEN THERE EXISTS A PRIME P SUCH THAT $m < P < m!$.

SOLUTION: Let $m > 2$. We claim that $m < m! - 1$ for every $m \geq 3$. To prove our claim we proceed by induction. If $m = 3$ then $3! - 1 = 6 - 1 = 5 > 3$. Assume now $h! - 1 > h$ for some $h \in \mathbb{N}$, $h > 3$. Then, $(h+1)! = (h+1)\, h! > (h+1)(h+1) > (h+1).2$. This shows that $(h+1)! - 1 > 2(h+1) - 1 = 2h + 1 = (h+1) + h > h+1$. Then, by the PMI, the inequality holds for all $m \in \mathbb{N}$, $m \geq 3$. This proves our claim. We now observe $m < m! - 1 < m!$ for $m > 2$.

If $m! - 1$ is prime we are done. Suppose next that $m! - 1$ is not a prime. Since $m! - 1 > 1$ there exists a prime p such that $p \mid m! - 1$. Then $p < m! - 1 < m$. Assume $p \leq m$. Then $p \mid m!$ as p is a factor of $m!$. Since $p \mid m!$ and $p \mid (m! - 1)$ we have $p \mid 1$ which is a contradiction. Then $m < p$ and so $m < p < m!$ as we wanted to show.

EXERCISE 11: For $m \in \mathbb{N}$, $m > 1$, show that every prime divisor of $m! + 1$ is an odd integer that is greater than m.

SOLUTION: Since $m \geq 2$ we observe $m!$ is even and so $m! + 1$ is odd. Then, $2 \nmid m! + 1$. This means that every prime divisor of $m! + 1$ is different to 2. Let p be a prime such that $p \mid m! + 1$. We know that $p \neq 2$ and so p is odd. Assume that $p \leq m$. Then $p \mid m!$ and since $p \mid m! + 1$ we get $p \mid 1$, a contradiction. Hence, $p > m$.

EXERCISE 12: Assuming that p_m is the m-th prime number, establish the following statements:

(i) $p_m > 2m - 1$ for $m \geq 5$.

(ii) None of the integers $P_m = \prod_{j=1}^{m} p_j + 1$ is a perfect square.

(iii) The sum $\sum_{j=1}^{m} \frac{1}{p_j}$ is never an integer.

SOLUTION:

(i) We proceed by induction on $m \geq 5$. Note that $p_5 = 11 > 9 = 10 - 1 = 2 \cdot 5 - 1$. We next assume that $p_h > 2h - 1$ for some $h > 5$. Observe p_h is the h-th prime and it is odd. Then $p_h + 1$ is even which means the next possible prime is $p_h + 2$. Then, $p_{h+1} \geq p_h + 2$. Hence,

$$p_{h+1} \geq p_h + 2 > 2h - 1 + 2 = (2h+2) - 1 = 2(h+1) - 1.$$

This shows the inequality holds for $h+1$ when it is true for h. Therefore, by the PMI the inequality $p_m > 2m - 1$ for $m \in \mathbb{N}$, $m \geq 5$.

(ii) Note that $p_1 = 2$. Then $\prod_{j=1}^{m} p_j$ is even and so $P_m = \prod_{j=1}^{m} p_j + 1$ is odd. By the DAT we observe $P_m = 4q_m + r_m$ for some $q_m, r_m \in \mathbb{N}$ and $r_m \in \{0,1,2,3\}$. As P_m is odd we have $r_m \notin \{0,2\}$ and so, $r_m \in \{1,3\}$. Suppose now that $r_m = 1$. Then $P_m = 4q_m + 1$ which implies $\prod_{j=1}^{m} p_j = 4q_m$ and so $\prod_{j=2}^{m} p_j = 2q_m$. Then $2 \mid \prod_{j=2}^{m} p_j$ and since 2 is prime there exists k $(2 \leq k \leq m)$ such that $2 \mid p_k$ and p_k is even. This implies that $k = 1$ since $p_1 = 2$ is the only even prime number. This is a contradiction since $k > 1$. Therefore $r_m = 3$.

Assume now that P_m is a perfect square. Then, there exists $t \in \mathbb{N}$ such that $P_m = t^2$. Since $t^2 = P_m$ is odd we have that t is odd. So, $t = 2\ell + 1$ for some $\ell \in \mathbb{N}$. Then,

$4q_m + 3 = P_m = t^2 = (2\ell+1)^2 = 4\ell^2 + 4\ell + 1$ which implies $4q_m + 2 = 4\ell^2 + 4\ell$. We thus have $4(\ell^2 + \ell - q_m) = 2$ and since $\ell^2 + \ell - q_m \in \mathbb{Z}$, we have $4 \mid 2$ which is a contradiction. This shows that P_m is not a perfect square.

(iii) Suppose that $\sum_{j=1}^{m} \frac{1}{p_j}$ is an integer. Then $\sum_{j=1}^{m} \frac{1}{p_j} = a$ for some $a \in \mathbb{Z}$. Let $b := \prod_{j=1}^{m} p_j$. Then, we observe $\left(\prod_{i=1}^{m} p_i\right) \sum_{j=1}^{m} \frac{1}{p_j} = \sum_{j=1}^{m} \prod_{i=1}^{m} \frac{p_i}{p_j} = \sum_{j=1}^{m} \prod_{\substack{i=1 \\ i \neq j}}^{m} p_i$. Let $k \in \mathbb{N}$, $1 \leq k \leq m$. Note that $p_k \mid \prod_{i=1}^{m} p_i$ and since $a \in \mathbb{Z}$, $p_k \mid \left(\prod_{i=1}^{m} p_i\right) \cdot a$. That is, $p_k \mid \sum_{j=1}^{m} \prod_{\substack{i=1 \\ i \neq j}}^{m} p_i$.

Recall that $p_k \mid p_k \cdot c$ for every $c \in \mathbb{Z}$. Then, $p_k \mid \prod_{\substack{i=1 \\ i \neq j}}^{m} p_i$ for every $j \neq k$. This shows that $p_k \mid \sum_{\substack{j=1 \\ j \neq k}}^{m} \left(\prod_{\substack{i=1 \\ i \neq j}}^{m} p_i\right)$. Now we observe $\sum_{j=1}^{m} \left(\prod_{\substack{i=1 \\ i \neq j}}^{m} p_i\right) = \prod_{\substack{i=1 \\ i \neq k}}^{m} p_i + \sum_{\substack{j=1 \\ j \neq k}}^{m} \left(\prod_{\substack{i=1 \\ i \neq j}}^{m} p_i\right)$ which yields that $p_k \mid \prod_{\substack{i=1 \\ i \neq k}}^{m} p_i$. Since p_k is prime, there exists ℓ $(1 \leq \ell \leq m)$, $\ell \neq k$ such that $p_k \mid p_\ell$ which is a contradiction as p_ℓ is prime. We therefore have $a \notin \mathbb{Z}$.