Pledge: *I pledge my honor that I have abided by the Stevens Honor System.* -Eric Altenburg

---

1: Our proof of the fundamental theorem of arithmetic took the Euclidean division algorithm for granted, but it too warrants proof! Prove it. That is, prove that for any two positive integers n and d, there are unique integers q and r such that $n = qd + r$ and $0 \leq r < d$.

Proof. (Contradiction) To show the existence of q and r, consider the set $S = \{n + dx : x \in \mathbb{Z}\} \cap \mathbb{N}$. From this we know that $n \in S$ and because of its construction, S is a non-empty subset of $\mathbb{N}$. By the Well-Ordering Principle, there is a least element in S called s_0 such that $s_0 = n + dx_0$ where $x_0 \in \mathbb{Z}$. From this, we claim that $0 \leq s_0 < d$. Now, assume $d \leq s_0$. This can be rewritten as $0 \leq s_0 - d$ which implies that $s_0 - d \in S$ as $s_0 - d = n + d(x_0 - 1)$. Because of our assumption that s_0 was the least element in S, this is a contradiction showing the existence of q and r. They are derived by reordering the equation $s_0 - d = n + d(x_1 - 1)$ as follows,

$$\begin{aligned} s_0 - d &= n + d(x_0 - 1) \\ s_0 - d &= n + dx_0 - d \\ s_0 &= n + dx_0 \\ n &= (-x_0)d + s_0. \end{aligned}$$

Therefore, $q = -x_0$, $r = s_0$, and because $0 \leq d - s_0$, we have $0 \leq r < d$.

To show that q and r are unique, suppose we have r_1, r_2, q_1, q_2 such that $n = q_1d + r_1 = q_2d + r_2$ where $0 \leq r_1 \leq r_2 < d$. From this we can see that $0 \leq (r_2 - r_1)$ and after rewriting $n = q_1d + r_1 = q_2d + r2$, we find that $r_2 - r_1 = (q_1 - q_2)d$. Now the inequality can be written as,

$$\begin{aligned} 0 &\leq (r_2 - r_1) < d \\ 0 &\leq (q_1 - q_2)d < d. \end{aligned}$$

This inequality shows that a multiple of d is less than d itself, and this can only happen when $(q_1 - q_2)$ is 0. Therefore, we can say that $0 = (q_1 - q_2)d = r_2 - r_1$ which means $r_2 = r_1$ and $q_2 = q_1$. □

2: In class, we proved a lower bound on the prime counting function $\pi(n) =| \{p \text{ prime } \mid p \leq n\} |$ by using the fact that every natural number can be written in the form rs^2, where $r, s \in \mathbb{N}$ and r is *square-free*, meaning that it is not a multiple of any square number greater than 1. Prove that it is indeed the case that every natural number admits such a decomposition.

Proof. Using the fundamental theorem of arithmetic to prove every natural number n can be written in the form rs^2 where $r, s \in \mathbb{N}$ and r is square-free does not work when $n = 1$. However, $n = 1$ can be written in the form of rs^2 when $r = s = 1$ which gives $1 = 1 \cdot 1^2$; this satisfies the decomposition. Now, when $n > 1$ the fundamental theorem of arithmetic can be used. We can break this proof into cases.

Case 1: n's prime factorization includes prime numbers with both even and odd powers.

Then

$$n = (p_1^{2a_1} \cdot p_2^{2a_2} \cdot \ldots \cdot p_k^{2a_k}) \cdot (q_1^{2b_1+1} \cdot q_2^{2b_2+1} \cdot \ldots \cdot q_j^{2b_j+1})$$

where every p_i is a prime number with an even power, and every q_i is a prime number with an odd power. This can be rewritten as

$$n = (p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k} \cdot q_1^{b_1} \cdot q_2^{b_2} \cdot \ldots \cdot q_j^{b_j})^2 \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_j.$$

If every a_i and b_i are 0, then n must be a square-free number, and in this case, we can let $s = 1$ giving us our decomposition of $n = r(1)^2$ where r must be a square-free number. However, if not every a_i and b_i are 0, then n is the product of a perfect square and a square-free number also giving us the desired decomposition of $n = rs^2$.
Case 2: n's prime factorization only includes prime numbers with even powers.
Then

$$\begin{aligned} n &= p_1^{2a_1} \cdot p_2^{2a_2} \cdot \ldots \cdot p_k^{2a_k} \\ &= (p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k})^2 \end{aligned}$$

where every p_i is a prime numbers with an even power. This means that n must be a perfect square. Let $r = 1$ which gives the desired decomposition of $n = (1)s^2$.
Case 3: n's prime factorization only includes prime numbers with odd powers.
Then

$$\begin{aligned} n &= q_1^{2b_1+1} \cdot q_2^{2b_2+1} \cdot \ldots \cdot q_j^{2b_j+1} \\ &= (q_1^{b_1} \cdot q_2^{b_2} \cdot \ldots \cdot q_j^{b_j})^2 \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_j \end{aligned}$$

where every q_i is a prime number with an odd power. If all b_i are 0, then $n = q_1 \cdot q_2 \cdot \ldots \cdot q_j$ which means n is a square-free number. To get the desired decomposition, let $s = 1$ giving $n = r(1)^2$ where r must be a square-free number. However, if not all b_i are 0, then n is the product of a perfect square and a square-free number also giving us the desired decomposition of $n = rs^2$. □

3: When presented with a prime number greater than 3, the mathematician Evelyn Lamb has been known to observe that it is one away from a multiple of 3! This is a double entendre, because the claim is true regardless of whether the exclamation point is understood as an exclamation or as the mathematical symbol for the factorial. Prove that every prime greater than 3 is one away from a multiple of 3! (three factorial).

Proof. By the Euclidean division algorithm, any prime number n such that $n > 3$ can be written as $n = qd + r$ where n and d are positive integers, q and r are unique integers, and $0 \leq r < d$. In this instance, let $d = 6$ which gives $n = q6 + r$. Since n is a prime number, d and r must be co-prime because if they are not, then n would be a multiple of another number that is not 1 or itself no longer making it prime. Additionally, due to the constriction on r, the only possible values of r that are co-prime with $d = 6$ are 1 and 5. Now n can be written in the following two ways,

1. $n = q6 + 1$
2. $n = q6 + 5$,

or it can simply be expressed as $n = q6 \pm 1$. □