Theorem 1. *Fundamental Theorem of Arithmetic. A positive integer $p > 1$ is a product of prime numbers in essentially one way only.*

> The theorem can be proved by mathematical induction plus some simple but skilled ingenuity. E. Zermelo . . . gave such a proof in 1912 and published it in 1934. *Others imitated him.*
>
> —*Eric Temple Bell [1]*

Proof. We shall provide our own proof based on *strong induction*, perhaps it will be an imitation of Zermelo's . . ..

Bases:

We prove that the proposition holds for the integers: 2, 3, 4, 5, and 6:

Number	Expressed as the *unique* product of primes
2	2
3	3
4	2×2
5	5
6	2×3

From the above, it is trivial to see that the proposition is true for *all* integers in $[2, 6]$; each of the numbers is either prime or a unique product of prime numbers.

Inductive hypotheses:

Each of the integers from 2 to n can be expressed as a *unique product* of prime numbers. These are the inductive hypotheses, we shall assume them to be true.

Induction:

We will prove the conditional statement of which the inductive hypotheses are the antecedent and P_{n+1} the consequent[1], i.e., we prove that $P_0 \land P_1 \land \cdots \land P_n \implies P_{n+1}$ where P denotes our proposition that every integer can be expressed as a *unique product* of primes[2].

Number	Expressed as the *unique* product of primes
2	2
3	3
$\vdots$	$\vdots$
n_1	$p_{11} \times p_{12} \times \cdots \times p_{1a}$ (these are a primes)
n_3	$p_{31} \times p_{32} \times \cdots \times p_{3c}$ (these are c primes)
n_4	$p_{41} \times p_{42} \times \cdots \times p_{4d}$ (these are d primes)
n_2	$p_{21} \times p_{22} \times \cdots \times p_{2b}$ (these are b primes)
$\vdots$	$\vdots$
n	$p_{n1} \times p_{n2} \times \cdots \times p_{nk}$ (these are k primes)

Just for convenience, prime factors of numbers in the above table are arranged in a non-decreasing order.

Existence:

Consider the number $n + 1$. Two cases emerge:

1. $n + 1$ is prime. Clearly, P_{n+1} is true in this case.
2. $n + 1$ is not prime. Then there must be two factors of $n + 1$ whose product is $n + 1$. Let the two factors be n_1 and n_2. Then, from inductive hypotheses, n_1 and n_2 can themselves be expressed as unique products of a and b primes respectively.

$$\begin{aligned} n + 1 &= n_1 \times n_2 \\ &= (p_{11} \times p_{12} \times \cdots \times p_{1a}) \times (p_{21} \times p_{22} \times \cdots \times p_{2b}) \end{aligned}$$

   Thus, $n + 1$ can be expressed as a product of $a + b$ primes.

In either case, $n + 1$ can be expressed as a product of primes.

Uniqueness:

The same two cases for $n + 1$ emerge:

[1] See [2] for details

[2] This is also called the *prime factorization* of an integer $n > 1$

1. $n+1$ is prime. Then, by definition, its only prime factor is $n+1$ which gives a *unique* prime factorization.
2. $n+1$ is not prime. Let it have two *different* prime factorizations (because of the two pairs n_1, n_2 and n_3, n_4): $n+1 = n_1 \times n_2 = n_3 \times n_4$. Let there be no prime common in $a+b$ primes in $n_1 \times n_2$ and $c+d$ primes in $n_3 \times n_4$:

$$\begin{aligned} &n+1 \\ &\quad = (p_{11} \times p_{12} \times \cdots \times p_{1a}) \times (p_{21} \times p_{22} \times \cdots \times p_{2b}) \\ &\quad = (p_{31} \times p_{32} \times \cdots \times p_{3c}) \times (p_{41} \times p_{42} \times \cdots \times p_{4d}) \end{aligned}$$

Conclusion: □

Theorem 2. *The remainder when any number $p \in \mathbb{N}$ is divided by 9 is the same as the remainder when the sum of digits of p is divided by 9.*

Proof. We use mathematical induction on the number of digits in p. Concretely, we use the notation $a \bmod b$ to denote the remainder when a is divided by b ($a, b \in \mathbb{N}$).

Basis: The sum of digits of a single-digit number is the number itself. This trivially proves that the proposition P of the theorem holds for all single-digit numbers, i.e., $P(1)$ is true.

Inductive hypothesis: Let the remainder when a k-digit number, $p_k = d_k d_{k-1} \ldots d_2 d_1$, is divided by 9 be r_k:

$$p_k \bmod 9 = r_k \tag{1}$$

where $0 \leq r_k < 9$.

We assume that P holds for p_k. Let s_k denote the sum of digits of p_k. The inductive hypothesis then becomes

$$p_k \bmod 9 = r_k \implies s_k \bmod 9 = r_k \tag{2}$$

where

$$s_k = \sum_{i=1}^{k} d_i$$

Induction: To form p_{k+1}, a $(k+1)$-digit number, we juxtapose a digit d_0 to p_k. Then it follows that

$$p_{k+1} = 10 \cdot p_k + d_0 = 9 \cdot p_k + p_k + d_0$$

and since $(9 \cdot p_k) \bmod 9 = 0$,

$$p_{k+1} \bmod 9 = (p_k \bmod 9 + d_0 \bmod 9) \bmod 9 \tag{3}$$

From (1),

$$p_{k+1} \bmod 9 = (r_k + d_0 \bmod 9) \bmod 9 \tag{4}$$

Now, the sum of digits of p_{k+1}:

$$s_{k+1} = s_k + d_0 \tag{5}$$

and hence

$$s_{k+1} \bmod 9 = (s_k \bmod 9 + d_0 \bmod 9) \bmod 9$$

which, from inductive hypothesis (2), becomes

$$s_{k+1} \bmod 9 = (r_k + d_0 \bmod 9) \bmod 9 \tag{6}$$

Conclusion: Since the right hand sides of (4) and (6) are the same,

$$p_{k+1} \bmod 9 = s_{k+1} \bmod 9$$

Togther, the Basis and Induction prove the theorem. □

Next, we provide an alternate proof.

Proof. Let p be a k-digit natural number

$$p = d_{k-1} d_{k-2} \ldots d_0$$

and

$$s = d_{k-1} + d_{k-2} + \cdots + d_0$$

be the sum of its digits.

$$\begin{aligned}\therefore p &= \sum_{i=0}^{k-1} 10^i \cdot d_i \\ &= \sum_{i=0}^{k-1} (9+1)^i \cdot d_i\end{aligned}$$

We use binomial expansion to get:

$$\begin{aligned}p &= \sum_{i=0}^{k-1} (\binom{i}{0} \cdot 9^i + \binom{i}{1} \cdot 9^{i-1} + \binom{i}{2} \cdot 9^{i-2} + \cdots + \binom{i}{i-1} \cdot 9 + \binom{i}{i} \cdot 1) \cdot d_i \\ &= \sum_{i=0}^{k-1} (m+1) \cdot d_i\end{aligned}$$

where m is a multiple of 9.

$$\begin{aligned}p &= (m+1) \cdot (d_0 + d_1 + \cdots + d_{k-1}) \\ &= (m+1) \cdot s \\ \therefore p \bmod 9 &= m \bmod 9 + s \bmod 9 \\ &= s \bmod 9\end{aligned}$$

since m mod 9, the remainder when a multiple of 9 is divided by 9, is 0. □

Theorem 3. *The n^{th} fibonacci number, $fib(n)$, can be expressed as* $fib(n) = \frac{\varphi^n - \hat{\varphi}^n}{\sqrt{5}}$, *where* $\varphi = \frac{1+\sqrt{5}}{2}$ *and* $\hat{\varphi} = \frac{1-\sqrt{5}}{2}$ *(Abraham De Moivre's theorem).*

Proof. φ and $\hat{\varphi}$ are the two roots of the equation $x^2 = x + 1$, or equivalently, $x = 1 + \frac{1}{x}$. Therefore,

$$\varphi = 1 + \frac{1}{\varphi} \tag{7}$$

and

$$\hat{\varphi} = 1 + \frac{1}{\hat{\varphi}} \tag{8}$$

The fibonacci sequence is recursively defined as follows:

$$fib(n) = \begin{cases} 1 & \text{if } n = 1 \\ 1 & \text{if } n = 2 \\ fib(n-1) + fib(n-2) & otherwise \end{cases} \tag{9}$$

The first few terms of fibonacci sequence are: $1, 1, 2, 3, 5, 8, 13$. We use mathematical induction to prove the theorem.

Basis: It is trivial to verify that the theorem holds for $n = 2$:

$$\begin{aligned}fib(2) &= \frac{\varphi^2 - \hat{\varphi}^2}{\sqrt{5}} \\ &= \frac{1}{\sqrt{5}} \cdot \frac{1}{4} \cdot (6 + 2\sqrt{5} - 6 + 2\sqrt{5}) \\ &= 1\end{aligned}$$

and $n = 1$:

$$\begin{aligned}fib(1) &= \frac{\varphi^1 - \hat{\varphi}^1}{\sqrt{5}} \\ &= \frac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}{\sqrt{5}} \\ &= \frac{\frac{2\cdot\sqrt{5}}{2}}{\sqrt{5}} \\ &= 1\end{aligned}$$

Inductive hypothesis: We *assume* that the hypothesis holds for n and $n-1$, i.e.

$$fib(n) = \frac{\varphi^n - \hat{\varphi}^n}{\sqrt{5}} \tag{10}$$

and

$$fib(n-1) = \frac{\varphi^{n-1} - \hat{\varphi}^{n-1}}{\sqrt{5}} \tag{11}$$

Induction: We need to prove that inductive hypothesis is true for $n+1$ *assuming* it holds for *both* $n, n-1$. In other words, we need to prove that

$$fib(n+1) = \frac{\varphi^{n+1} - \hat{\varphi}^{n+1}}{\sqrt{5}}$$

From (9),

$$\begin{aligned}
fib(n+1) &= fib(n) + fib(n-1) \\
&= \frac{\varphi^n - \hat{\varphi}^n}{\sqrt{5}} + \frac{\varphi^{n-1} - \hat{\varphi}^{n-1}}{\sqrt{5}} \\
&= \frac{(\varphi^n + \varphi^{n-1}) - (\hat{\varphi}^n + \hat{\varphi}^{n-1})}{\sqrt{5}} \ldots \textit{from inductive hypothesis } (10), (11) \\
&= \frac{\varphi^n(1+\frac{1}{\varphi}) - \hat{\varphi}^n(1+\frac{1}{\hat{\varphi}})}{\sqrt{5}} \\
&= \frac{\varphi^n(\varphi) - \hat{\varphi}^n(\hat{\varphi})}{\sqrt{5}} \ldots \textit{from } (7),\ (8)
\end{aligned}$$

$$fib(n+1) = \frac{\varphi^{n+1} - \hat{\varphi}^{n+1}}{\sqrt{5}} \tag{12}$$

Conclusion: De Moivre's theorem follows from (10), (11), and (12).

□

Theorem 4. *The natural numbers x and y are relatively prime (i.e. $GCD(x,y) = 1$). Prove that x and $x \pm y$ are relatively prime.*

Proof. Let us say that x and y are relatively prime, but x and $x+y$ are *not*. This means that 1 is the only common factor of x and y but that some natural number, $f > 1$, is a common factor of x and $x+y$. Let

$$x = f \cdot q_1 \tag{13}$$

where $q_1 \in \mathbb{N}$, and

$$x + y = f \cdot q_2 \tag{14}$$

where $q_2 \in \mathbb{N}$.

Let $y > x$. By substituting x from (13) and rearranging the terms, we get

$$y = f \cdot (q_2 - q_1) \tag{15}$$

where $(q_2 - q_1) \in \mathbb{Z}$.

From (13) and (15) it follows that $f > 1$ is a *common factor* of both x and y implying that they are *not* relatively prime. This is a contradiction since we started with the proposition that x and y are relatively prime. A similar argument can be made to prove that x and $x-y$ are relatively prime too.

□

Theorem 5. *Let $GCD(m,n)$ denote the greatest common divisor of two nonnegative integers, m and n. Prove that $GCD(m,n) = GCD(m-n,n)$.*

Proof. Without the loss of generality, let $m > n$. A *sorted sequence* of all factors of m (p factors) and n (q factors) can be written:

$$S_1 = f_{m(1)}, f_{m(2)}, \ldots, \underline{f_{m(i)}}, \ldots, f_{m(p)} \tag{16}$$

where $f_{m(i)} < f_{m(j)} \forall i < j$ and $p \in \mathbb{N}, p \geq 2$. Clearly, $f_{m(1)} = 1$, and $f_{m(p)} = m$.

$$S_2 = f_{n(1)}, f_{n(2)}, \ldots, \underline{f_{n(j)}}, \ldots, f_{n(q)} \tag{17}$$

where $f_{n(i)} < f_{n(j)} \forall i < j$ and $q \in \mathbb{N}, q \geq 2$.

Let $GCD(m,n) = f_{m(i)} = f_{n(j)}$. Then, by definition,

$$m = GCD(m,n) \cdot q_m \tag{18}$$

$$n = GCD(m,n) \cdot q_n \tag{19}$$

where $q_m, q_n \in \mathbb{N}$ are the respective multiples.

Subtracting (19) from (18),

$$m - n = GCD(m,n) \cdot (q_m - q_n) \tag{20}$$

The numbers q_m and q_n must be relatively prime, because, if they were not, $GCD(m,n)$ would be greater than $f_{m(i)}$ or $f_{n(j)}$. It then follows that q_n and $q_m - q_n$ are relatively prime too (See Theorem 4). Therefore, from (19) and (20),

$$GCD(m-n,n) = GCD(m,n)$$

□

References

[1] Bell, Eric Temple. MATHEMATICS Queen and Servant of Science. G. Bell & Sons, Ltd: London. Page 231.

[2] Peter Suber, "Mathematical Induction". On the WWW at `https://legacy.earlham.edu/~peters/courses/logsys/math-ind.htm`.