Proofs in Number Theory

Miliyon T.
Addis Ababa University
Ethiopia

February 24, 2014

Abstract

Number theory is one of the most elegant, abstract and the more beautiful branches of Mathematics. The Greatest mathematician Carl Friedreich Gauss once said that Mathematics is a Queen of Science and Theory of Number is the Queen of Mathematics. Although, Number Theory have been considered as non-applicable subject nowadays it is become crucial for Internet Cryptography. Here we scribe some elementary proofs in number theory.

1 Definitions

Definition 1.1. A nonempty set S of real numbers is said to be well-ordered if every nonempty subset of S has a least element.

Remark 1.2. Every nonempty finite set of real numbers is well-ordered.

Definition 1.3 (**The Well-Ordering Principle**)**.** The set $\mathbb{N}$ of positive integers is well-ordered.

2 Basic Results

Theorem 2.1. *For each integer m, the set*

$$S = \{i \in \mathbb{Z} : i \geq m\}$$

is well-ordered.

Proof. We need only show that every nonempty subset of S has a least element. So let T be a nonempty subset of S. If T is a subset of $\mathbb{N}$, then, by **the Well-Ordering Principle**, T has a least element. Hence we may assume that T is not a subset of $\mathbb{N}$. Thus $T - \mathbb{N}$ is a finite nonempty set and so contains a least element t. Since $t \leq 0$, it follows that $t \leq x$ for all $x \in T$; so t is a least element of T. $\square$

Theorem 2.2 (The Division Algorithm). *Let a be any integer and b a positive integer. Then there exist unique integers q and r such that*

$$a = qb + r \qquad \textit{where } 0 \leq r < b$$

Proof. The proof consists of two parts. First, we must establish the existence of the integers q and r, and then we must show they are indeed unique.

1. EXISTENCE

   Consider the set $S = \{a - bn | (n \in \mathbb{Z}) \text{ and } (a - bn \geq 0)\}$. Clearly, $S \subset \mathbb{W}$. We shall show that S contains a least element. To this end, first we will show that S is a non empty subset of $\mathbb{W}$:

   Case 1: Suppose $a \geq 0$. Then $a = a - b \cdot 0 \in S$, so S contains an element.

   Case 2: Suppose $a < 0$. Since $b \in \mathbb{Z}^+, b \geq 1$. Then $-ba \geq -a$; that is, $a - ba \geq 0$.

   Consequently, $a - ba \in S$. In both cases, S contains at least one element, so S is a nonempty subset of $\mathbb{W}$. Therefore, by theorem (2.1), S contains a least element r. Since $r \in S$, an integer q exists such that $r = a - bq$, where $r \geq 0$.

   To show that $r < b$: We will prove this by contradiction. Assume $r \geq b$. Then $r - b \geq 0$. But $r - b = (a - bq) - b = a - b(q + 1)$. Since $a - b(q + 1)$ is of the form $a - bn$ and is greater than 0, $a - b(q + 1) \in S$; that is, $r - b \in S$. Since $b > 0$, $r - b < r$. Thus, $r - b$ is smaller than r and is in S. This contradicts our choice of r, so $r < b$. Thus, there are integers q and r such that $a = bq + r$, where $0 \leq r < b$.

2. UNIQUENESS

   We would like to show that the integers q and r are unique. Assume there are integers q, q', r, and r' such that $a = bq + r$ and $a = bq' + r'$, where $0 \leq r < b$ and $0 \leq r' < b$.

   Assume, for convenience, that $q \geq q'$. Then $r - r' = b(q - q')$. Because $q \geq q'$, $q - q' \geq 0$ and hence $r - r' \geq 0$. But, because $r < b$ and $r' < b$, $r - r' < b$. Suppose $q > q'$; that is, $q - q' \geq 1$. Then $b(q - q') \geq b$; that is, $r - r' \geq b$. This is a contradiction because $r - r' < b$. Therefore, $q \ngtr q'$; thus, $q = q'$, and hence, $r = r'$. Thus, the integers q and r are unique, completing the uniqueness proof.

□

References

[1] Euclid's Element: The Thirteen Book of Euclid translated by Sir Thomas L. Heath Cambridge University press. 1968.

[2] [Tom Apostle] An Introduction to Analytic Number Theory California Institute of Technology. 1976.

[3] [Jeffry Stopple] A Primer of Analytic Number Theory From Pythagoras to Riemann Cambridge University Press. 2003.

[4] [William Dunham] Euler: The Master of us all. Mathematical Association of America. 1999.