Proofs in Number Theory

Miliyon T.*
Department of Applied Mathematics
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. The proofs presented here are elementary and beautiful.

1 Basic Results

Lemma 1.1 (Bezout's lemma)**.** *For every pair of whole numbers a and b there are two integers s and t such that $as + bt = \gcd(a, b)$.*

1.1 Euclid's Lemma

Lemma 1.2. *Any composite number is divisible by a prime.*

Proof. For a composite number n, there exists an integer d satisfying the conditions $d \mid n$ and $1 < d < n$. among all such integers d, choose p to be the smallest. Then p must be a prime number. Otherwise, it too would possess a divisor q with $1 < q < p$; but $q \mid p$ and $p \mid n$ implies that $q \mid n$, which contradicts our choice of p as the smallest divisor, not equal to 1, of n. Thus, there exists a prime p with $p \mid n$. □

Theorem 1.3. *If p is a prime and $p \mid ab$, then either $p \mid a$ or $p \mid b$.*

Proof. If $p \mid a$, then we need go no further, so let us assume that $p \nmid a$. Since the only positive divisors of p (hence, the only candidates for the value of $\gcd(a, p)$) are 1 and p itself, this implies that $\gcd(a, p) = 1$. Citing Euclids lemma, it follows immediately that $p \mid b$. □

*Euclid[1], *Euler*[7]

2 Fundamental Theorem of Arithmetic

Theorem 2.1. *Every positive integer $n > 1$ is either a prime or can be expressed as a product of primes; this representation is unique, apart from the order in which the factors occur.*

Proof. Either n is a prime or it is composite. In the first case there is nothing to prove. If n is composite, then there exists a prime divisor of n, as we have shown. Thus, n may be written as $n = p_1 n_1$, where p_1 is prime and $1 < n_1 < n$. If n_1 is prime, then we have our representation. In the contrary case, the argument is repeated to produce a second prime number p_2 such that $n_1 = p_2 n_2$; that is,

$$n = p_1 p_2 n_2; 1 < n_2 < n_1 :$$

If n_2 is a prime, then it is not necessary to go further. Otherwise, write $n_2 = p_3 n_3$, with p_3 a prime; hence,

$$N = p_1 \cdot p_2 \cdot p_3 \cdot n_3; 1 < n_3 < n_2 :$$

The decreasing sequence $n > n_1 > n_2 > \cdots > 1$ Cannot continue indefinitely, so that after a finite number of steps n_k is a prime,say p_k. This leads to the prime factorization $n = p_1 p_2 p_k$: The second part of the proofthe uniqueness of the prime factorizationis more difficult. To this purpose let us suppose that the integer n can be represented as a product of primes in two ways; say, $n = p_1 p_2 \cdots p_r = q_1 q_2 q_s; r \leq s$; Where the p_i and q_j are all primes, written in increasing order, so that $p_1 p_2 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$: Because $p_1 \mid q_1 q_2 q_s$, we know that $p_1 | q_k$ for some value of k. Being a prime, q_k has only two divisors, 1 and itself. Because p_1 is greater than 1, we must conclude that $p_1 = q_k$; but then it must be that $p_1 \geq q_1$. An entirely similar argument (starting with q_1 rather than p_1) yields $q_1 \geq p_1$, so that in fact $p_1 = q_1$. We can cancel this common factor and obtain

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s :$$

Now repeat the process to get $p_2 = q_2$; cancel again, to see that

$$p_3 p_4 \cdots p_r = q_3 q_4 \cdots q_s :$$

Continue in this fashion. If the inequality $r < s$ held, we should eventually arrive at the equation $1 = q_{r+1} q_{r+2} \cdots q_s$; Which is absurd, since each $q_i > 1$. It follows that $r = s$ and that

$$p_1 = q_1; p_2 = q_2, \cdots, p_r = q_r;$$

This makes the two factorizations of n identical. □

3 Euclid Theorem

Theorem 3.1. *There are an infinite number of primes.*

Proof. Write the primes $2, 3, 5, 7, 11 \cdot \cdot\cdot$ in ascending order. For any particular prime p, consider the number $N = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p) + 1$. That is, form the product of all the primes from 2 to p, and increase this product by one. Because $N > 1$, we can use the fundamental theorem to conclude that N is divisible by some prime q. But none of the primes $2, 3, 5, ..., p$ divides N . For if q were one of these primes, then on combining the relation $q \mid 2 \cdot 3 \cdot 5 \cdots p$ with $q \mid n$, we would get $q \mid (N - 2 \cdot 3 \cdot 5 \cdots p)$, or what is the same thing,$q \mid 1$. The only positive divisor of the integer 1 is 1 itself, and since $q > 1$, the contradiction is obvious. Consequently, there exists a new prime q larger than p. □

4 The n^{th} root of a prime number is irrational.

Proof. Suppose not. i.e suppose it is rational, thus we can write $\sqrt[n]{p} = \frac{a}{b}$ where $n \in \mathbb{Z} \geq 2$ and $a, b \in \mathbb{Z}$ and they are relatively prime. Taking a power n both side gives

$$p = \frac{a^n}{b^n} \tag{1}$$

$$pb^n = a^n$$

$$p \mid a^n \Rightarrow a \neq 1$$

From Fundamental theorem of Arithmetic

$$a = \prod_{i=1}^{k} p_i \tag{2}$$

$$a = p_1 \cdot p_2 \cdot p_3 \cdots p_k, k \geq 1$$
$$\Rightarrow p|(p_1 \cdot p_2 \cdot p_3 \cdots p_k)^n$$

This implies p divides p_i for some i between 1 and k.
Prime number divides prime number

$$\Rightarrow p = p_i$$

Thus, $p \mid a$ since $p_i \mid a$

$$\because p \mid a^n \Rightarrow p|a$$

Now we can write a as $a = pk$, where $k \in \mathbb{Z}$. Let's substitute this on (1).

$$p = \frac{(pk)^n}{b^n}$$

$$pb^n = p^n \cdot k^n$$

$$b^n = p^{n-1} \cdot k^n = p \cdot p^{n-2} k^n$$

$$b^n = p \cdot p^{n-2} k^n$$

Which implies $p \mid b^n$ then by similar argument as the above we can easily show that $p \mid b$. Now we have shown that $p \mid a$ and $p \mid b$ but this contradict the fact that a and b are relatively prime.
Hence our assumption that $\sqrt[n]{p}$ is rational is wrong.
$\therefore \sqrt[n]{p}$ is irrational. $\square$

5 Basel problem

$$\zeta(2) = 1 + \frac{1}{4} + \frac{1}{9} + \cdots = \frac{\pi^2}{6}$$

Proof. Consider the function

$$\frac{\sin{(x)}}{x}$$

which has non zero roots at $\pm\pi, \pm 2\pi, \pm 3\pi, \pm 4\pi, ...$

So we can write this function as infinite product of polynomials like this

$$\frac{\sin(x)}{x} = (1 - \frac{x}{\pi})(1 + \frac{x}{\pi})(1 - \frac{x}{2\pi})(1 + \frac{x}{2\pi})(1 - \frac{x}{3\pi})(1 + \frac{x}{3\pi})(1 - \frac{x}{4\pi})(1 + \frac{x}{4\pi}) \cdots$$

$$= (1 - \frac{x^2}{\pi^2})(1 - \frac{x^2}{4\pi^2})(1 - \frac{x^2}{9\pi^2}) \cdots$$

Expand this infinite product to get and we are only interested on the coefficient of x^2

$$= 1 + (-\frac{x^2}{\pi^2} - \frac{x^2}{(4\pi^2}) - \frac{x^2}{9\pi^2} \cdots) + \cdots$$

$$= 1 - \frac{x^2}{\pi^2}(1 + \frac{1}{4} + \frac{1}{9} + \cdots) + \cdots$$

$$\frac{\sin(x)}{x} = 1 - \frac{\zeta(2)}{\pi^2} x^2 + \cdots \tag{3}$$

But from Taylor expansion we know that

$$\sin(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7}! + \cdots$$

Divide both side by x then it becomes

$$\frac{\sin{(x)}}{x} = 1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} + \cdots \tag{4}$$

Now equate the coefficients of x^2 in (2) and (3).

$$-\frac{\zeta(2)}{\pi^2} = -\frac{1}{3!}$$

$$\zeta(2) = \frac{\pi^2}{3!}.$$

$\square$

6 O(n)=D(n)

D(n) is the number of ways of writing n as the sum of distinct whole numbers.
O(n) is the number of ways of writing n as the sum of (not necessarily distinct)odd numbers.

Proof. Introduce

$$P(x) = (1+x)(1+x^2)(1+x^3)\cdots$$

$$= 1 + x + x^2 + (x^3 + x^{2+1}) + (x^4 + x^{3+1}) + (x^5 + x^{4+1} + x^{3+2}) + \cdots$$

So

$$p(x) = 1 + \sum_{n=1}^{\infty} D(n)x^n \tag{5}$$

Introduce

$$1 + a + a^2 + a^3 + \cdots = \frac{1}{(1-a)}$$

Proof from geometric sum

$$G_n = a_1 \frac{(1-r^n)}{(1-r)}$$

But in this case $r = a$ and$a_1 = 1$. Therefore

$$G_n = 1\frac{(1-r^n)}{(1-r)}\ , G_n = \frac{1}{(1-a)} - \frac{a^n}{(1-a)}$$

For $|a| < 1$ the second term will be zero.
The equation becomes

$$G_n = \frac{1}{(1-a)}$$

Introduce

$$Q(x) = \frac{1}{(1-x)} \cdot \frac{1}{(1-x^3)} \cdot \frac{1}{(1-x^5)} \cdots$$

$$= (1 + x + x^2 + x^3 + \cdots)(1 + x^3 + x^6 + x^9 + \cdots)$$
$$(1 + x^5 + x^{10} + x^{15} + \cdots)\cdots$$

$$Q(x) = (1 + x^1 + x^{1+1} + x^{1+1+1} + \cdots)(1 + x^3 + x^{3+3} + x^{3+3+3} + \cdots)$$
$$(1 + x^5 + x^{5+5+5} + x^{5+5+5} + \cdots) \cdots$$

So

$$Q(x) = 1 + \sum_{n=1}^{\infty} O(n)x^n \tag{6}$$

What we have done so far is we introduce two function $P(x)$ and $Q(x)$.Additionally we have proved that they are actually equal to the following infinite sums.

$$P(x) = (1 + x)(1 + x^2)(1 + x^3) \cdots = 1 + \sum_{n=1}^{\infty} D(n)x^n$$

$$Q(x) = \frac{1}{(1 - x)} \cdot \frac{1}{(1 - x^3)} \cdot \frac{1}{(1 - x^5)} \cdots = 1 + \sum_{n=1}^{\infty} O(n)x^n$$

Our aim is to show $D(n) = O(n)$. WLOG suppose our generating functions $P(x)$ and $Q(x)$ are equal.

$$P(x) = Q(x)$$

$$1 + \sum_{n=1}^{\infty} D(n)x^n = 1 + \sum_{n=1}^{\infty} O(n)x^n$$

$$\Rightarrow D(n) = O(n)$$

Now, we are only expected to show our assumption $P(x) = Q(x)$ is true.

Let's pick $P(x)$ and do some trick

$$P(x) = (1 + x)(1)(1 + x^2)(1)(1 + x^3) \cdots$$

$$P(x) = (1 + x)(\frac{1 - x}{1 - x})(1 + x^2)(\frac{1 - x^2}{1 - x^2})(1 + x^3) \cdots$$

$$= \frac{\cancel{(1 + x)(1 - x)}\cancel{(1 + x^2)(1 - x^2)}(1 + x^3)(1 - x^3)(1 + x^4)(1 - x^4)}{(1 - x) \qquad \cancel{(1 - x^2)} \qquad (1 - x^3) \qquad \cancel{(1 - x^4)}} \cdots$$

If we keep multiplying by this pattern the entire numerator will cancel out and becomes 1. All the expressions with even power will cancel out and the odds left in the de-numerator. Like this

$$= \frac{1}{(1 - x)} \cdot \frac{1}{(1 - x^3)} \cdot \frac{1}{(1 - x^5)} \cdots$$

which is $= Q(x)$.

Hence we can conclude that

$$D(n) = O(n).$$

$\square$

7 Chinese Remainder Theorem

The Chinese Remainder Theorem is a result from elementary number theory about the solution of systems of simultaneous congruences. The Chinese mathematician Sun-tsï wrote about the theorem in the first century A.D. This theorem has some interesting consequences in the design of software for parallel processors.

Lemma 7.1. *Let m and n be positive integers such that $\gcd(m,n) = 1$. Then for $a, b \in \mathbb{Z}$ the system*

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

has a solution. If x_1 and x_2 are two solutions of the system, then $x_1 \equiv x_2 \pmod{mn}$.

Proof. The equation $x \equiv a \pmod{m}$ has a solution since $a + km$ satisfies the equation for all $k \in \mathbb{Z}$. We must show that there exists an integer k_1 such that

$$a + k_1 m \equiv b \pmod{n}.$$

This is equivalent to showing that

$$k_1 m \equiv (b - a) \pmod{n}$$

has a solution for k_1. Since m and n are relatively prime, there exist integers s and t such that $ms + nt = 1$. Consequently,

$$(b - a)ms = (b - a) - (b - a)nt,$$

or

$$[(b - a)s]m \equiv (b - a) \pmod{n}.$$

Now let $k_1 = (b - a)s$.

To show that any two solutions are congruent modulo mn, let c_1 and c_2 be two solutions of the system. That is,

$$\begin{aligned} c_i &\equiv a \pmod{m} \\ c_i &\equiv b \pmod{n} \end{aligned}$$

for $i = 1, 2$. Then

$$\begin{aligned} c_2 &\equiv c_1 \pmod{m} \\ c_2 &\equiv c_1 \pmod{n}. \end{aligned}$$

Therefore, both m and n divide $c_1 - c_2$. Consequently, $c_2 \equiv c_1 \pmod{mn}$. $\square$

Theorem 7.2 (Chinese Remainder Theorem). *Let $n_1, n_2, \ldots, n_k$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then for any integers $a_1, \ldots, a_k$, the system*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has a solution. Furthermore, any two solutions of the system are congruent modulo $n_1 n_2 \cdots n_k$.

Proof. We will use mathematical induction on the number of equations in the system. If there are $k = 2$ equations, then the theorem is true by Lemma 7.1. Now suppose that the result is true for a system of k equations or less and that we wish to find a solution of

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_{k+1} \pmod{n_{k+1}}. \end{aligned}$$

Considering the first k equations, there exists a solution that is unique modulo $n_1 \cdots n_k$, say a. Since $n_1 \cdots n_k$ and n_{k+1} are relatively prime, the system

$$\begin{aligned} x &\equiv a \pmod{n_1 \cdots n_k} \\ x &\equiv a_{k+1} \pmod{n_{k+1}} \end{aligned}$$

has a solution that is unique modulo $n_1 \ldots n_{k+1}$ by the lemma. □

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.