CHAPTER 1

A brief view of number theory

1.1. Number theory in ancient time

We should have a quick review to the past (before Fermat in 17th century). Mesopotamia civilization (2000-3000 *B.C*) is the first civilization, which presents documents that indicate mathematical activities at that time. At that time there was not paper and the process of writing has been done on the tablets made of clay with a kind of hard writing called cuneiform; there are calendars which, determines that the beginning of this matter goes back to about 2000 *B.C* and it shows that Summer ions had an understanding of topologic measurements, simple and complex interest, the solution of the square equations and their uses of negative numbers. The first convincing sign which archeologist scientists found was in 1945 and it was the time that A. Negiver and A. Sakhz analyzed a table which was known to Plimpton 322 (Plimpton library from Colombia University). From the language that used in it, we can comprehend the history of it a little closer to 1600-1900 *B.C.* However there is a schedule in it including 15 answers for equation $x^2 + y^2 = z^2$ which from difficulty point, they are (3,4,5) to (12709,13500,18541).

In addition, the sequence of numbers have been written in a special way, indeed, it is requested to reduce an angle of a right triangle with (*x*, *y*, *z*) sides from 45° to 31°. Evidently, Babylonians knew not only Pythagoras theorem and eventually the sense of trigonometric functions, but they used a rule for finding the answers of Pythagoras equation. If we suppose that all of these are not extraordinary enough, we should say these people have done all of these acts without symbolic algebra and without sense of common demonstration. It does not seem that Egypt mathematics that has remained on the parchment wholly shows the proceeding of Mesopotamia in mathematics. The obtained works from *B.C.* Indo china are very scattered but the important thing is that the acts which were done in Indo china have not had any effect on the development of numbers theory. The subjects which are known as mathematics today like deduction, proof and theorem, started from Greeks. Probably conclusion has been used by Tales (548-624 *B.C*) and almost was used by the students of Pythagoras school.

Pythagoras (500-580 *B.C*) traveled to Babylon, Egypt and probably India. He was a philosopher and a Gnostic, gave importance to counting and philosophy. Probably he and his followers were depended on the senses of pictorial number (triangles numbers 1, 3, 5, 10,…; square numbers, etc), perfect numbers (for example, 28 is a perfect number because it is equal to 1+2+4+7+14, the sum of its divisors less than itself), amicable numbers (for example 220, 284 because each of them equals to sum of another real divisors). But, it is not obvious which one of them had proved theorems in these cases.

The first institute like university witch was called "museum" established in Alexandria and its first scientific member was Euclid. However, Euclid was famous mathematicians, most of the subjects that he reviewed in “principles” book, have been former’s works.

The volumes, number IX, VIII and VII of principles book have considered number theory. Unique decomposition theorem equals to theorem 14 of IX book. The existence of infinite numbers of prime number is 20th theorem of IX book.

Among three famous mathematicians that created the golden era of Greek mathematics (200-300 *B.C*). Euclid, Archimedes, Apollonius he is only Euclid Who seems to have done many researches in number theory. Most of the time, mechanics and geometricians paid more attention to it and it took time more than 3 centuries for Diophantus and Alexandrian to begin a new way with the outstanding work, "arithmetic". In his work about 13 volumes of treasure that there have been just 6 volumes of them remained started multi variables (unknown) equations, Equations with two or more unknown quantity which the answers belong to Q^+ or (today) to Z. Also, these books include some theorems like, if two integer numbers which each of them equals to the sum of two squares, the product of them also equals to the sum of two squares. According to indirect evidences, it seems that Chinese have known much mathematical subjects before finding them out in else where, which includes Pascal's triangle and simple magic squares. On the other side, probably because they had no relation to others, their portion in mathematics is considered just in "Chinese remained theorem" that belongs to some centuries ago.

In India, Brahmagopta discovered general integer answer of linear Diophantus equation" $ax+by=c$".

But Diophantus had verified only equations with higher degree, because linear equations are obvious when rational answers were considered. And always he binds himself to special and singular answers.

Some years later Bascara (1114-1185), solved equation $x^2 - dy^2 = 1$ in especial cases many years before that, samples of this equation was solved by Archimedes or one of his contemporaries and also by Diophantus.

With decreasing the influence of Greeks, and then advent of Roman imperial (that had not present a new thing in mathematics), the center of civilization was transferred to Baghdad. Probably Harmonious Knowledge of Babylonians, Egyptians, Greeks and Hindus were useful they were.

1.2. What is number theory?

This question is the motivation of primary attempts to present a definition. Number theory is the study of a set of integer numbers $0,\pm1,\pm2,...$ or some of subsets of it or sets includes it, with this thesis that integer numbers are interesting alone and in relation to each other, without paying attention to their useful role in measurement. Apparently the domain of this definition includes primary arithmetic, which in fact, it is in this manner except cases about exact and improvement aspect.

We return to 17-century, for taking an idea and knowing about the time that Pier Fermat's[1] work started a new era in mathematics. One of the most beautiful Fermat's theorems is that every positive integer number can be shown as the sum of squares of four integer numbers. For example:

$$1=1^2+0^2+0^2+0^2$$

$$2=1^2+1^2+0^2+0^2$$

$$4=1^2+1^2+1^2+1^2=2^2+0^2+0^2+0^2$$

$$7=2^2+1^2+1^2+1^2$$

$$188951=371^2+226^2+15^2+3^2$$

(According to this point, the multiplication of two representable numbers is a representable number; it is enough to prove that every prime number "*P*" is representable).

He propounded this theorem in 1636, but the first printed proof of it, presented in 1770 by Joseph Luis Lagrange. This theorem has an ideal aspect in theorems of number theory that is: beauty, fast understandability, revealing and exact and unexpected relation between integer numbers, and the best result in relation to its kind (7 cannot be shown as sum of less number than squares) and it is a proposition about infinite set of integer numbers. The last one is very important, because it determines the difference between theorems and numeral truth. This subject that 1729 is the smallest positive integer number, has two representations as the sum of two cubes $\left(12^3+1^3, 10^3+9^3\right)$is true and probably one of the most interesting facts, but we can not name this truth as a theorem. Because it can be proved by testing a finite set 1, 2,…, 1729.

On the other side, we consider that the proposition "only finite integer numbers that exist have two or more presentations of that kind" is seducer. It seems that this proposition expresses a subject about finite set, but in fact, we can not prove or reject every finite set with testing. Therefore, this proposition will be an important theorem if it is true (Of course always is not).

Another more famous subject that is attributed to Fermat and sometimes called his latest theorem, expresses that if "n" is an integer number greater than "2", the equation

[1] Fermat was a lawyer. He was expert in ancient languages and has high rank in classic culture. At that time, no scientific journal existed and he didn't like to write his demonstrations. In stead of it, he had contacted with priest M. Mersenne who had correlation with all of European scientists extensively. Fermat took the lead in analytic geometry from Decartes and in differential calculus from Newton and Leibniz, but his work didn't become famous, because he couldn't print his book in these fields. His fame is because of his work in number theory, that he was unique in this field.

$x^n + y^n = z^n$ does not answer in positive integer numbers set. Fermat claimed that he proved this but as his habit, he did not express its proof. It seems, this is only a recorded example that he claimed a result which he never proved (Although he propounded a false guess about the prime number $F_n = 2^{2^n} + 1$ that we will express below). Since there is no demonstration for this claim, modern mathematicians prefer to call it Fermat's problem instead of Fermat's theorem. This is the oldest and maybe the famous unsolved problem in mathematics. Although only a counter example is enough to discredit it, finding four numbers *x*, *y*, *z* and "*n*", if they exist, is out of the capacity of future and computers. Because, now, it is clear that this equation does not have any answers for $n < 100{,}000$ and if the answer exists, *x*, *y* or *z* must be greater than n^{2n}.

(The known worlds can contain only 10^{123} objects in proton size).

One of the basic concepts of number theory is prime numbers. Integer number "*p*" is prime if $p \neq \pm 1$ and equation $p = ab$ does not have an answer with respect to integer number "*a*" and "*b*", except $a = \pm 1$ or $a = \pm p$. Therefore, we can say briefly that a prime number is an integer number that is the opposite of ± 1 and does not have any non–trivial divisor. (Before, Euclid knew that the sequence of prime numbers 2, 3, 5, 7 …does not finish and the manner of their appearance is very irregular). Fermat and Mersenne also were seeking a kind of order and both of them guessed a wrong thing. Fermat guessed that all of numbers $F_n = 2^{2^n} + 1$ are prime numbers that in fact, this conjecture is true for *n*=0, 1, 2, 3, 4. After a while, it was clarified that, it stops soon, because Leonard Euler in 1739 showed that "F_5" is a divisor of "641". In fact, for $5 \le n \le 24$ no prime value was found for F_n. Since false guesses about prime numbers are very frequent this story would not be very valuable if Fermat's prime numbers appeared "200" years later in different situation again. Carl Fredrich Guass[1] searched one of ancient Greece's problems. He proved that regular m-angle can be made by ruler and compass if and only if (IFF) "*m*" can be factorization in $m = 2^k.\ f_{n_1} \dots f_{n_r}$ form, that *k*,*n*$_1$,…n_r are non-negative integer numbers and f_{n_i} are Fermat's distinct prime numbers. So it is interesting to know whether prime numbers more than this kind exist or not?

Although portion of Mersenne in Mathematics was propagating the new results more than creating them, but he studied prime numbers among numbers in $M_n = 2^n - 1$ form.

If $n = rs$, then "M_n" is divisible by "M_r" and also by "M_s". Therefore "M_n" can be prime Just for prime values of "*n*". In 1644, Mersenne expressed that from "55" numbers of "M_p" that $p \le 257$, the ones which are prime number, are corresponding with $p = 2,3,5,7,13,17,19,31,67,127,257$. So, Mersenne committed "5" errors. Because he took into account 67 and 257 and he didn't teak into account 61, 89 and 107. It isn't attention

[1] Some people believe that Guass is the greatest mathematician till now. He guessed the theorem of prime numbers when he was 15; he determined the characteristics of construction able polygon in 18 the age of. When he way 22 years old he proved that a polynomial of "*n*" the degree has "*n*" roots, and printed his best work as Disquisitiones Arithmeticae when he was 24 years old. This book changed numbers theory from a set of singular problems to a branch related to mathematics. After 1801, he studied other fields of mathematics, mostly geometry, analysis, astronomy and physics except two essays about two quadratic reciprocities. He spent his accomplished life in Guttingen University. His collected works include 12 books.

able that he had wrong but it is important that he could gain information about numbers which have 78 digits without pocket calculator. Again we see numeral truth, not theorem, and frankly some cases must be hidden beyond these subjects, that "N is prime number if …" or "N isn't prime number if …" and such cases are useful. Always there is strong interaction effect between intuitive truth and theorems of numbers theory. Calculations give information that we can infer from them some counter examples or theorem's guesses and also subjects for useful theorems which lead to useful algorithms. (Algorithm means methods for calculation).

Fermat's numbers and Mersenne's numbers are so scattered that if all of them be prime numbers, we can infer a little information about distribution of prime numbers in them.

Other useful and prominent studying by Guass was started in 1792 by using a table of prime numbers smaller than 102,000 that some years ago printed by John Lambert. If as it is usual, $\pi(x)$ was indicator of the number of positive prime numbers not more than "x", then what Guass did, was searching the increments of $\pi(x)$ according to the increments of "x". He started by enumeration of prime numbers in intervals with constant lengths and obtained a table like below, in which:

$$\Delta(x) = [\pi(x) - \pi(x - 1000)]/1000$$

x	$\pi(x)$	$\Delta(x)$
1000	168	0.168
2000	303	0.135
3000	430	0.127
4000	550	0.120
5000	669	0.119
6000	783	0.114
7000	900	0.117
8000	1007	0.107
9000	1117	0.110
10000	1229	0.112

The average of the number of prime numbers reduces in successive interval and Guass chose inverse of $\Delta(x)$ and compared it to a different primary function. The following table is obtained about natural logarithm of "x":

X	1000	2000	3000	4000	5000	6000	7000	8000	9000	10,000
$\Delta(x)$	0.168	0.135	0.127	0.120	0.119	0.114	0.117	0.107	0.110	0.112
$\frac{1}{Lnx}$	0.145	0.132	0.125	0.121	0.117	0.115	0.113	0.111	0.110	0.109

The wonderful match of these numbers strengthen, this guess $\Delta(x)$ is almost equal to $\frac{1}{Lnx}$. Since $\Delta(x)$ is equal to slope angle of a segment on curve $y = \pi(x)$, we must integrate the approximate equation of $\Delta(x) \approx \frac{1}{Lnx}$ so that $\pi(x)$ can be calculated, therefore Guass guessed:

$$\pi(x) \approx \int_2^x \frac{dt}{Lnt}.$$

This Integral is not a primary function and usually is shown by $li(x)$. Its values are calculated easily and modern calculations present the following comparison (that $li(x)$ is given with its nearest integer number)

x	$\pi(x)$	$li(x)$	$li(x) - \pi(x)$	$\pi(x)/li(x)$
10^3	168	178	10	0.94382
10^4	1,229	1,246	17	0.98636
10^5	9,592	9,630	38	0.99605
10^6	78,498	78,628	130	0.99835
10^7	664,579	664,918	339	0.99949
10^8	5,761,455	5,762,209	754	0.99987
10^9	50,847,534	50,849,235	1701	0.99997
10^{10}	455,052,512	445,055,614	3102	0.99999

What Gauss expressed in present ion a guess that $\pi(x)$ is a good approximation of $\pi(x)$ for great "x", was not that $(li(x) - \pi(x)) \to 0$, or even $(li(x) - \pi(x))$ was limit, but this was that its relative error is little:

$$(li(x) - \pi(x))/\pi(x) \to 0$$

Or:

$$\lim_{x\to\infty} \frac{\pi(x)}{li(x)} = 1 \qquad (1)$$

He guessed this subject in 1793 when he was "15" years old. But this subject wasn’t proved, till more than a "100" years later Hadamard and Poisson proved it (independently in 1896). Its demonstration is too hard that can be expressed in this book. But it is possible to show that if the limit of (1) exists, its value will be equal to "1". It is not so difficult to show (1) result:

$$\lim_{x\to\infty}\frac{\pi(x)}{x/Lnx}=1 \qquad (2)$$

This subject and its inverse are proved. Because of the Basic situation that relation (1) or its formal form (2), have in number theory, it is known as "theorem of prime numbers".

The Reason for studying the information of latest table for great number of "*x*" which Gauss did not calculate $\pi(x)$ for them, is that he persisted on this important point that no calculations can substitute the demonstration. As the table clearly show's $li(x)$ always presents $\pi(x)$ with abundant approximate. It means that at least the value of $[\,li(x)-\pi(x)\,]$ is positive and increasing to $x=10^{10}$. But this isn't permanent, because Littlewood in 1914 showed that the sign of $[\,li(x)-\pi(x)]$ changes infinite times. No body knows that when first sign changing occurs. But Skewes in 1955 proved that this subject happens for "*x*" that $x<10^{10^{10^{34}}}$. Probably no determinate value will be found for "*x*" in future so that for it $li(x)<\pi(x)$. Many questions exist about prime numbers that all of them remain unsolved (, despite the attempts that have been done for two or more centuries,) for example, is there infinite number of twin prime numbers like 17 and 19, 4967 and 4969 so that their difference is "2", and does every even number greater than 4 equal to the sum of two odd prime numbers?

Now, to have an extra example we express a question that is less famous and hasn't been propounded recently and it seems to be very hard. We form the following double infinite array that the first row includes prime numbers and every number of the following rows equals to absolute value of subtraction of its two upper numbers. Is it true that every row except the first row starts by "1"? This subject is true about a part of array that is written in below up to $p=53$ and it is justified up to $p=792721$. There are some branches of number theory that integer numbers exist in them less "a" the prime number theory.

```
  2     3     5     7    11    13    17    19    23    29    31    37    41    43    47    53
     1     2     2     4     2     4     2     4     6     2     6     4     2     4     6
        1     0     2     2     2     2     2     2     4     4     2     2     2     2
           1     2     0     0     0     0     0     2     0     2     0     0     0
              1     2     0     0     0     0     2     2     2     2     0     0
                 1     2     0     0     0     2     0     0     0     2     0
                    1     2     0     0     2     2     0     0     2     2
                       1     2     0     2     0     2     0     2     0
                          1     2     2     2     2     2     2     2
                             1     0     0     0     0     0     0
                                1     0     0     0     0     0
```

For example, in problems about nature of numbers like "π" and "*e*", such a situation exists. This question that whether every one of these numbers are rational or not, in fact is equivalent to whether every one of them is an answer for a linear equation like $ax+b=0$ with correct coefficient or not? Lambert[1] Switzer, a mathematician, mentioned and later

[1] Lambert's family was poor and he had to leave the school at the age of 12, and after that he had no systematic adduction. Never the less, he has a considerable role in philosophy (acquaintance and metaphysics), astronomy (nebula), physics (optics, hygrometry and thermodynamics) and drawing.
His major work in mathematics (except the number theory) is in geometry and his book about parallelism and perspective was a background of nun-Euclidian geometry that came true in 19-th century.

in 1761 proved that "π" is not a rational number. Generally, this question can be propounded that, are "*e*" and "π" algebraic or not? In other words, are any of them adapted in a polynomial like $a_0x^n + a_1x^{n-1} + ... + a_n = 0$ with integer coefficient like $a_1,...,a_n$, $a_0 \neq 0$ or not?

Again in both cases, it is proved that the answer is negative but their demonstrations are a little hard. If we verify the problem on the other side, we can study the numbers that are algebraic and therefore it seems that a strong theory can be built on it, so that it will be an interesting subject and a useful instrument to study the integer numbers.

1.3. Prime numbers

In this book, we consider the positive divisor of numbers. Therefore, we speak about "divisor", it means positive divisors unless against this mater are emphasized. For example the only divisors of 6 are 1,2,3,6.

1.3.1. Definition

Natural number " $p \neq 1$ " is a prime when its divisors are only "1" and "*p*", each natural number except "1" is compound when it is not prime. From this definition, it results that "1" is neither prime nor composite. Also natural number like "*n*" is a composite number if and only if $n = n_1n_2$ that$1 < n_2 < n$, $1 < n_1 < n$. The prime numbers less than "100" are written in Pythagorean's table:

2,3,5,7,11,13,17,19,23,29,…,97

Since the only positive divisors of prime number "*p*" are "1" and "*p*", then for each integer number like "*a*" we have (a, p)=1 or $(a, p) = p$, it means, "*a*" is coprime with "*p*" or "*p*" aliquots it. Therefore, sometimes it is correct to write $(a, p) = 1$ instead of $p \nmid a$.

Now we suppose "*p*" is prime and "*a*" and "*b*" are two integer numbers so that $p \mid ab$. If $p \nmid a$, then $(a, p) = 1$ and it results $p \mid b$. Therefore, the products of two integer numbers are divisible by prime number "*p*", if only at least one of those two numbers is divisible by "*p*". This result can be extended to multiplication of a finite number of integer numbers. (Using this product symbol $a_1a_2 ... a_k = \prod_{i=1}^{k} a_i$, we show the following General results.

1.3.2. Lemma

Imagine "*p*" is prime number and "*k*" is natural number. If $a_1, a_2, ..., a_k$ are integer numbers so that $p \mid \prod_{i=1}^{k} a_i$ then for one "*i*" and $1 \leq i \leq k$ we will have $p \mid a_i$, now we express and prove the following lemma:

He had a position comparable to Euler in Science Academy of Prussian only for the last 12 years of his life. Before that he was a teacher in his home land, Swiss.

1.3.3. Lemma

Each natural number $n > 1$ has a prime factor.

Proof. Suppose that $n > 1$ is a supposed natural number and "*S*" is a set of all divisors of "*n*" greater than "1". Since $n \in S$, then the set "*S*" is non-null and consequently "*S*" has a smaller member, namely "*p*". We prove that "*p*" is a prime number. Since each divisor of "*p*", is a divisor of "*n*", therefore if "*p*" is composite then it is necessary that "*S*" has a member which is less than "*p*" and this is impossible, therefore "*p*" is prime. The following theorem is from Ecocides and therefore this theorem is over 2000 years old.

1.3.4. Theorem

The number of prime numbers is infinite.

This theorem means that if we suppose each natural number like "*n*", the number of prime numbers is more than "*n*". We suppose $p_1, p_2, ..., p_n$ are "*n*" different prime numbers. We write $N = 1 + \prod_{i=1}^{n} p_i$. According to lemma (1.3.3)**,** "*N*" has a prime factor like "*p*". On the other hand, no value of p_i is the factor of "*N*", because in this condition it is necessary that $p_i \mid 1$. Therefore "*n*+1", prime numbers $p_1, p_2, ..., p_n, p$ are distinct. So we could prove the theorem's demonstration, by induction.

There are easy ways for classifying prime numbers. At the firs stage it seems that each natural number is either even or odd, it means that each number is in the form of "$2n$" or "$2n+1$" that "n" is a non-zero integer number.

But "2*n*" can not to be prime except for "$n = 1$". Then each prime number is odd except 2. Therefore we could deform the above theorem that the number of odd prime numbers is infinite.

In this way, because the reminder of division of each integer number by 3 is 0,1,2, then each natural number is in one of these three forms $3n, 3n+1,$ $3n+2$ and "*n*" is a natural number. Again "$3n$" can not be a prime number unless $n = 1$. Then each prime number except "3" is in form of $3n+1$ or $3n+2$. In other words, every prim number except "3" is in form of $3n \pm 1$. Therefore, the number of prime numbers is infinite to this form $3n+2, 3n+1$.

Now in the next step we remind that each natural number is in these forms $4n, 4n+1, 4n+2, 4n+3$ and "*n*" is natural number.

It is clear that "4*n*" is newer prime and $4n+2 = 2(2n+1)$ is prime only if $n = 0$. Then each odd prime number is in one of these forms $4n+1$ or $4n+3$. On the other hand, each odd prime number is in $4n \pm 1$ form. Therefore numbers of prime numbers which are in this form are infinite.

Also we can classify prime numbers according to residuals of dividing by each positive correct number and constant (as it used in 2, 3 and 4).

The following theorem is famous to Dirichlet, it is proved in some special conditions with the elementary way, but we do not know easy demonstration for the general state of this theorem. Therefore, we express the theorem without proof. Its especial state is the urgent result of theorem (1.3.4) for $a = 1$.

1.3.5. Theorem

If "a" and "b" are two natural numbers and $(a,b)=1$, then the number of prime numbers in "$an+b$" form is infinite ("n" is the natural number).

1.4. The fundamental theorem and some of its applications

In the same way, we will show, it is completely clear that each correct number is $a>1$ or prime or we can write it in a form like multiplication of prime numbers. According to lemma (1.3.3), number "a" has a prime factor like p_1 and therefore there is a natural number like a_1 in that $a = p_1 a_1$. So, there is a natural number like a_2 in that $a_1 = p_2 a_2$ or $a = p_1\ p_2\ a_2$. If $a_2 = 1$ then "a" is written as the multiplication of the primes p_1 and p_2. Now, if $a_2 > 1$ then a_2 must have had a factor like p_3 and $a = p_1\ p_2\ p_3\ a_3$ .Since $a > a_1 > a_2 > a_3 > ...$ so this sequence can't repeat to extreme infinite times and we must have $a_r = 1$ for a natural number like "r", and then $a = p_1\ p_2\ ...\ p_r$. But it is not necessary for all of prime numbers $p_1, p_2, ..., p_r$ to be different results. In this way we proved a part of the following theorem and this theorem has an important role in studying integer numbers which usually it is famous to the Arithmetic basic theorem. Before speaking about the theorem we accept that there is a multiplication even with one factor. Therefore, it is not necessary that we express different theorems for the situation that "a" is prime itself.

1.4.1. Basic theorem

We can write each natural number $a > 1$ with only one way as multiplication of prime numbers (without paying attention to the order factors). A part of the theorem proved above. Now we prove that showing each natural number is in form of multiplication of unique prime numbers. We suppose that it is possible to write "a" in two different ways as the form of multiplication of prime numbers, it means that $a = p_1\ p_2\ ...p_r$ and $a = q_1\ q_2\ ...q_s$ which "p_i" and "q_j" are prime and "p_i" is not exactly to "q_j" exactly, Then we have:

$$p_1\, p_2\ \cdots\ p_r = q_1\ q_2\ \cdots\ q_s$$

Now, if we delete equal prime numbers from both side of equality, by symbolizing the again, we will have:

$$p_1\ \ p_2\ \cdots\ p_i = q_1\ q_2\ \cdots\ q_j$$

That $i \ge 1$ and $j \ge 1$. It results $p_1 | q_1 q_2 ... q_i$ and from lemma (1.3.2) it is necessary that p_1 aliquot one of the prime numbers $q_1, q_2, ..., q_j$. Therefore p_1 must be equal to one of "q_j" that it is against omitting the equal prime numbers from the both sides of above equation. So this thesis is paradox that we can write "a" in two different methods as multiplication of prime numbers. So, the proof of theorem becomes complete.

In writing integer number $a > 1$, as multiplication of prime numbers, some times it is better to use symbol which shows all of the different prime factors of "a". Previous theorem showed that we can write each natural number $a > 1$, only in one way:

$$a = p_1^{k_1}\ p_2^{k_2} \dots p_r^{k_r} \quad (1)$$

That $p_1, p_2, \dots, p_r$ are the different prime factors of "*a*" and $k_i \geq 1 \ \ (i = 1,2,\dots,r)$. The right side of equation (1) named form of standard factorization of integer number "*a*".

Now, we suppose $d \mid a$ and (1) is a standard factorization of "*a*". We suppose $a = cd$ and $c > 1$, $d > 1$. If we express each of "*c*" or "*d*" as multiplication of prime numbers (it isn't necessary for all of them to be different) and we put it instead of "*c*" and "*d*" in $a = cd$, then "*a*" will be written as multiplication of prime numbers. If we look at equal prime numbers together in this multiplication, then according to basic theorem (1.4.6), number "*a*" exactly is written exactly as form (1). Therefore, we will have easy but important following theorem.

1.4.2. Theorem

If standard factorization of number "*a*" is in (1) form then the divisors of "*a*" will exactly be numbers like "*d*" in the following form:

$$d = p_1^{t_1} p_2^{t_2} \dots p_r^{t_r} \quad , \quad 0 \leq t_i \leq k_i (i = 1,2,\dots,r) \ (2)$$

It is clear for number "*a*" that we can give $d = 1$ with selection $t_i = 0 \ \ (i = 1,2,\dots.,r)$ in (2). Also with Selection $t_i = k_i \ (i = 1,2, \dots, r)$ we can get "*a*" itself. Remember that there is no need for (2) to be a standard factorization of "*d*", because it is possible that some or all of the powers are zero. We can get the greatest common divisor and the smallest common multiplication of two numbers $a > 1$ and $b > 1$ from the standard factorization of "*a*" and "*b*". For this, we change symbols a little. We suppose $p_1, p_2, \dots, p_t$ are different prime factors of "*a*" or "*b*". Therefore:

$$a = p_1^{m_1} p_2^{m_2} \dots p_t^{m_t} \quad , \quad b = p_1^{n_1} p_2^{n_2} \dots p_t^{n_t} \qquad (3)$$

That "m_i" and "n_i" could be zero. Nevertheless, for each $i = 1, 2, \dots, t$, at least one of "m_i" or "n_i" is greater than zero. We show the greatest and smallest number of $\{m_i, n_i\}$ respectively by $\alpha_i = Max\{m_i, n_i\}$ and $\beta_i = Min\{m_i, n_i\}$.

It is clear that when $m_i = n_i$ then $\alpha_i = \beta_i = m_i = n_i$, then with this expression, the following result is clear.

1.4.3. Theorem

If "*a*" and "*b*" are in form of (3), then:

$$(a,b) = p_1^{\beta_1} p_2^{\beta_2} \dots p_i^{\beta_i} ,$$

$$[a,b] = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} .$$

For example, we suppose that $a = 360$ and $b = 126$. Standard factorization of these integer numbers are $a = 2^3 \times 3^2 \times 5$ and $b = 2 \times 3^2 \times 7$.

By using theorem (1.4.3) we will have:

$$(360,126) = 2 \times 3^2 ,$$

$$[360,126] = 2^3 \times 3^2 \times 5 \times 7 .$$

Now, for finding the number of one positive integer number’s divisors, we obtain an easy formula. For example, according to theorem (1.4.2), divisors of $360 = 2^3 \times 3^2 \times 5$ are in $2^{t_1} \times 3^{t_2} \times 5^{t_3}$ which, t_1 is one of these four values 0,1,2,3 and t_2 is one of these three numbers 0,1,2 and t_3 is one of these two numbers 0,1. So, $2 \times 3 \times 4$ selections exist for t_1, t_2 and t_3. Therefore, the number of divisors of 360 is $4 \times 3 \times 2 = 24$.

Generally, $k_i + 1$ selections exist for t_i in (2) and so we can say:

Whenever (1) is a standard factorization of number "*a*", then the number of divisors of "*a*" is in the following form:

$$\prod_{i=1}^{r}(k_i + 1).$$

Also, we can gain a formula to calculate the sum of all of divisors of supposition integer number "*a*". Here we suppose the number $360 = 2^3 \times 3^2 \times 5$ for clear expression. We can show that multiplication:

$$(1 + 2 + 2^2 + 2^3)(1 + 3 + 3^2)(1 + 5)$$

As the sum of 24 terms in the following form:

$$2^2 \times 3^2 \times 5,\ 2 \times 1 \times 5\ ,\ 1 \times 1 \times 10$$

In fact, the above multiplication is equal to the sum of all integer numbers in form of $2^{t_1} \times 3^{t_2} \times 5^{t_3}$, so that $0 \le t_1 \le 3$, $0 \le t_2 \le 2$ and $0 \le t_3 \le 1$, namely equal to the sum of divisors of number 360, because:

$$1 + p + p^2 + \ldots + p^k = \frac{p^{k+1} - 1}{p - 1}$$

Therefore, the sum of divisors of number 360 is:

$$\frac{2^4 - 1}{2 - 1} \times \frac{3^3 - 1}{3 - 1} \times \frac{5^2 - 1}{5 - 1} = 15 \times 13 \times 6 = 1170\ .$$

1.4.4. Attention

Sometimes, it is better that we use symbol $\sum\limits_{d|a}$ for the summation, that domain of "*d*" is positive divisors of "*a*".

For example, $\sum\limits_{d|a} d$ is sum of all divisors of "*a*".

It is interesting to remember that we can factorize all of the numbers smaller than $\mathbf{100^2}$, it means 10000 to multiplication of prime factors with knowing the prime numbers smaller than 100. We suppose "*N*" is a non–prime number and smaller than 10000, we have in this situation $N = a.b$. In which "*a*" and "*b*" are prime or non-prime. If "*a*" and "*b*" are greater than 100, in this state, multiplication of "*ab*" will be greater than 10000 and this is against our supposition, since "*N*" is smaller than 10000. If for example "*a*" is a number smaller than 100, it means that there is a prime factor smaller than 100 (namely one of the 25 factors which are mentioned before). Therefore it is enough to know that the number "N" is divisible by which of these 25 numbers and if "N" is not divisible by any of them, it is prime number. For example we consider number 7458:

$$7458 = 3729 \times 2$$

$$3729 = 1243 \times 3$$

Number 1243 is not divisible by either 7 or 5, but we have:

$$1243 = 113 \times 11$$

And we can not continue the following action, because 113 is smaller than the square of 11 and by paying attention to these calculations that we have done, it is not divisible by any number smaller than 11, therefore it is a prime number.

Then, we can be assured by a general method that "N" is prime number, when it isn't divisible by any prime numbers smaller than "p". This method that is about primality of a simple special number is very hard when it is used for the great number of numbers and it is obvious that it is impossible for millions of numbers. There is an easy method for this case. It has been very usual since many years ago. It is related to Eratosthene and in this method, we identify the non-prime numbers among the numbers smaller than 10000 or 100000 and etc, and then we determine the least divisor of them which is prime. This way is known as Eratosthene sieve.

1.5. Sieve of Eratosthenes

Suppose that we want to determine the prime numbers smaller than 100. At first we omit even numbers, then we write the odd numbers on the consecutive rows (for example 10 numbers in each row), in this way we will have:

1	3	5	7	9	11	13	15	17	19
21	23	25	27	29	31	33	35	37	39
41	43	45	47	49	51	53	55	57	59
61	63	65	67	69	71	73	75	77	79
81	83	85	87	89	91	93	95	97	99

Then, before doing any thing, we omit the multiples of 3 and this is very easy, because these multiples are three-to-three.

When we omit the multiples of 3 there is no need to take into account the omitted even numbers, but after omitting the multiples of 3, if we want to omit the multiples of 5, we must consider the numbers five-to-five, without ignoring the multiples of 3 that have been omitted before.

For omitting the considering multiplication, it is better to adjust the above table to the following form, that in the two ends of the rows there are decimal digits and in the top of the columns, there are mono-digits.

	1	3	5	7	9	1	3	5	7	9	
0					3			3			1
2	3		5	3			3	5		3	3
4			3		7	3		5	3		5
6		3	5		3			3	7		7
8	3		5	3		7	3	5		3	9

At first, we put the number 3 in the squares which adapt numbers divisible by 3 (except the number 3 which is prime number). We will do this for number 5 and then 7. Finally the squares which are empty show the prime numbers. It is clear that the numbers 3 have a regular order in this table, along some diagonals, there is the same order for numbers 5 and 7, especially if divisors of 5 and 7 exist in equerries that also divisors of 3 exist, this situation is more obvious.

1.6. Periodic sieve for small numbers

If we note that sieve has a certain period, especially for the smaller prime divisors, then a lot of calculations can be done more easily. At first we pay attention to divisors of 2 and 3. The multiple of these two numbers is equal to 6 and it results that if a number is not divisible by 2 and 3 it will be in one of these forms:

$$6n+1 \quad , \quad 6n+5 \qquad (1)$$

It means that in any successive 6 numbers, there are two numbers that they are not divisible by 2 and 3. Now we search for the numbers which are divisible by 2, 3 or 5. We can see, among these numbers, there are only three numbers 2, 3 and 5 which are prime numbers. Nevertheless we consider them as the numbers which are divisible by 2, 3 or 5.

Among numbers of (1), which are divisible neither by 2 nor by 3, we can obtain the numbers smaller than 30 for $n = 0,1,2,3,4$ (for 5 values of "n"), in this way we will have 2×5 numbers. But among these numbers which aren’t divisible by 2 or 3, there are only two numbers which are divisible by 5. These two numbers come from the multiple of 5 by two numbers less than 6 (which are coprime with 2 and 3). Subsequently the number of numbers which aren’t divisible by any numbers 2 and 3 and 5, are equal to:

$$2\times 5-2=2\times 4=8$$

These 8 numbers are prime except "1":

$$1,7,11,13,17,19,23,29$$

Since the number 30 is divisible by 2 and 3 and 5, the numbers which are in one of the following forms:

$$\begin{cases} 30n+1 \quad , \ 30n+7 \quad , \ 30n+11 \ , \ 30n+13 \\ 30n+17 \ , \ 30n+19 \ , \ 30n+23 \ , \ 30n+29 \end{cases} \qquad (2)$$

are not divisible by 2 and 3 and 5 and these numbers aren’t necessarily prime, but, we must look for the prime numbers among them. On the other hand, for a number to be prime, the condition (2) is necessary but not enough.

Now, we consider the prime number 7. The numbers smaller than or equal to multiple of $7\times 30 = 210$, obtain from the relation (2) for seven values of "n", namely 0,1,2,3,4,5,6.

By this method we get 8×7 numbers which all of them are smaller than "210" and none of them are divisible by 2, 3 or 5.

Among these numbers, how many of these numbers are divisible by "7"? If these numbers are divisible by 7, quotient is a number between "1" to "30" and because none of these numbers are divisible by 2 and 3 or 5, Therefore their quotient by 7 is a number not divisible by 2,3 or 5, subsequently this quotient is one of eight numbers which we mentioned them before. Conversely the multiple of each of these eight numbers by 7:

$$7,49,77,91,119,133,161,203 \quad (3)$$

Will be the numbers smaller than "210" and not divisible by 2, 3 and 5, but they are divisible by 7. Finally among the first 210 numbers, the number of numbers which are not divisible by 2, 3, 5 and 7 will be:

$$8\times 7-8=8\times 6=2\times 4\times 6=48$$

These 48 numbers are numbers which are obtain from relation (2) for $n=0,1,2,3,4,5,6,$ as if we omit the mentioned numbers in relation (3).

If α is representative of every one of these 48 numbers, the numbers which are in this form:

$$210\,n+\alpha \qquad (4)$$

are not divisible by 2, 3, 5 and 7 and therefore they could be prime numbers. In fact, all 48 numbers aren't prime and among them, there are numbers which aren't prime:

$$11^2=121,\ \ 11\times 13=143,\ 13^2=169,\ 11\times 17=187$$

In this way, we can study the first 2310 numbers using the prime number "11" which is immediately after 7. $(2310=2\times 3\times 5\times 7\times 11)$.

Among these numbers, these are $2\times 4\times 6\times 10=480$ numbers[1] of β, which none of them divisible by 2, 3, 5, 7, 11 and they are written in this form[2] $2310\,n+\beta$ and we must search for the prime number only between them. Now if we consider the prime number like 13 too, then we will obtain:

$$2310\times 13=30030$$

that its appearance form is also very simple and among these 30030 primary numbers there are:

$$480\times(13-1)=480\times 12=5760$$

number which are not divisible by any prime number smaller than 17. For obtaining the prime numbers smaller than 30030, we must omit the multiples of 17, 19, … up to 173 (square root of 30030) among them. This is relatively a detailed work, but since it omits $30030-5760=24270$ numbers which are divisible by one of these numbers 2, 3, 5, 7, 11 and 13; in the first step, it facilitates the job.

[1] It can be written: 480 = (3-1) (5-1) (7-1) (11-1)

[2] Among the numbers which are in the form (4), we must omit the multiples of "11" among each of 48 numbers which are not divisible by 2,3,5,7.

1.7. The infinity of prime numbers

From what is said up to now, we can get to this conclusion easily that the prime numbers sequence is infinity, or in other words the last prime number does not exist. In fact, by an easy calculation which has been done before , it is resulted that if we consider only the prime numbers 2, 3, 5, 7, among the first 210 numbers greater than "1", there are 48 numbers which we can not obtain them by multiplication of one of these four prime factors by the others. If we consider more prime numbers, but restricted, there we will find more numbers which are not resulted from multiplication of these few prime numbers. For example if we consider the prime numbers 2, 3, 5, 7, 11, 13 among the first integer 30030 numbers, there are $2\times4\times6\times10\times12=5760$ numbers which will not be obtained as the multiple of one of these prime numbers by the others.

There is another reason to prove the infinity of prime numbers which is old and it is easier in some features, but it can not show clearly that how enormous the number of prime numbers is. This reasoning is as follow:

We prove there is at least a number which is greater than an arbitrary integer number "n". If we show the multiplication of first "n" integer numbers by "$n!$" and identify "N" by the following relation:

$$N=n!+1 \qquad (1)$$

then if "N" is not a prime number, it must have at least one prime divisor "p". This divisor "p" can not be smaller or equal to "n", because according to the relation (1), if we divide "N" by a number like "a" which is between 2 and "n" then the residual of division will be equal to unit. It means that "N" is not divisible by "a", therefore, there is a number like "p" which is greater than "n". Since the number of prime numbers is infinite, the distance between two consecutive prime numbers can be arbitrary great. We will show how we can use the decomposition into the positive prime factors in calculating the number of divisors and the sum of them.

1.8. Functions τ,σ and φ

1.8.1. Definition

If "n" be integer and positive, and then we will show the number of positive divisors of "n" by $\tau(n)$ and the sum of all of the positive divisors by $\sigma(n)$.

In the following theorem, we obtain a formula for calculation $\sigma(n)$ and $\tau(n)$ by using the decomposition into the prime factors.

1.8.2. Theorem

Suppose $n = p_1^{n_1}. \dots .p_r^{n_r}$, $n>1$, therefore:

$$\tau(n)=(n_1+1)(n_2+1)...(n_r+1)$$

And also:

$$\sigma(n)=\frac{p_1^{n_1+1}-1}{p_1-1}.\frac{p_2^{n_2+1}-1}{p_2-1}. \dots .\frac{p_r^{n_r+1}-1}{p_r-1}$$

Proof: suppose "$d = p_1^{d_1} p_2^{d_2} ...... p_r^{d_r}$" is a positive divisor of "n". For each "i" we have"$d_i \le n_i$", then, for all "d_i", there are "$n_i + 1$" different selections. (Indeed $d_i = 0,1,...,n_i$). Therefore, we can select the powers of "$d_1, d_2, ..., d_r$" in "$(n_1+1)(n_2+1)...(n_r+1)$" different ways. Then:

$$\tau(n) = (n_1+1)(n_2+1)...(n_r+1).$$

For calculating $\sigma(n)$, at first, note the following product:

$$P = (1 + p_1 + p_1{}^2 + ... + p_1{}^{n_1})(1 + p_2 + ... + p_2{}^{n_2})...(1 + p + ... + p_r{}^{n_r})$$

This multiplication is equal to the sum of all possible products of $p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ so that"$i = 1,2,...,r$" $(0 \le \alpha_i \le n_i)$.

But family of all of these products is exactly equal to the sum of all of the positive divisors of "n" therefore $\sigma(n) = p$. To complete the proof, at first we consider:

$$1 + p + p^2 + ... + p^k = \frac{p^{k+1} - 1}{p - 1}$$

(For prowling, it is enough to multiply $1 + p + ... + p^k$ by $p - 1$)

Therefore, we have:

$$\sigma(n) = \frac{p_1^{n_1+1} - 1}{p_1 - 1} . .... . \frac{p_r^{n_r+1} - 1}{p_r - 1}$$

1.8.3. Remark

The function σ and τ are examples of number theory functions. They have common and very important qualities. Both σ and τ are multiplicative, it means for both two coprime numbers "m" and "n", we have:

$$\sigma(mn) = \sigma(m)\sigma(n) \quad ; \quad \tau(mn) = \tau(m)\ \tau(n)$$

Generally, the function "f ", which is defined on set of positive integer numbers, is called multiplication if and only if for all "n" and "m" that $(m,n) = 1$:

$$f(m.n) = f(m)\ f(n)$$

To prove multiplicative forms of σ and τ, we can gain some results directly and with some calculations and by using some formulas.

Function φ-Euler is another important multiplicative function that we acquaint it here.

1.8.4. Conclusion

If "P" is a prime number:

$$\varphi(P^k) = P^k(1 - \frac{1}{P}) \quad (\varphi: \text{Euler's Function})$$

Proof. This assertion is clear for "k=1". Because if "P" be prime, then:

$$\varphi(P) = P - 1.$$

If "$k>1$", since "P" is prime, then the numbers which are not coprimes with "P^k" are as follow:

$$P, 2P, 3P, ..., P^{k-1}.P$$

Therefore, the number of numbers is not coprime when "$P^{k\text{” is}}$ equal to "P^{k-1}" and the other numbers are coprime with to "P^k". The number of them is equal to "$P^k - P^{k-1}$ "or $P^k(1-\frac{1}{P})$ that here, assertion is proved.

1.8.5. Result

We know that if $(a, b, c,\dots)$ =1, then:

$$\varphi\,(a.b.c....) = \varphi\,(a).\varphi\,(b).\varphi(c)....$$

Therefore, we can write for $N = p^k.q^s.r^t...$ ($p, q, r, \dots$ are prime factors):

$$\begin{aligned}\varphi\,(n) &= \varphi\,(p^k.q^s.r^t....) = \varphi\,(p^k).\varphi\,(q^s).\varphi\,(r^t)....\\ &= p^k(1-\frac{1}{p}).q^s(1-\frac{1}{q}).r^t(1-\frac{1}{r})......\\ &= (\underbrace{p^k.q^s.r^t.}_{N}.)(1-\frac{1}{p})(1-\frac{1}{q})(1-\frac{1}{r})...\end{aligned}$$

So:

$$\varphi(n) = N(1-\frac{1}{p})(1-\frac{1}{q})(1-\frac{1}{r})...$$

For example, the number of numbers smaller than 100 that are coprime with it, it is calculated by the following method:

$$N = 100 = 2^2 \times 5^2 \quad : \quad \begin{aligned}\varphi(N) &= \varphi(100)\\ &= \varphi(2^2 \times 5^2)\\ &= 100(1-\frac{1}{2})(1-\frac{1}{5})\\ &= 100 \times \frac{1}{2} \times \frac{4}{5} = 40\end{aligned}$$

1.9. Perfect numbers

1.9.1. Definition

We call integer number $n > 0$ as perfect, if it equals the sum of divisors smaller than itself. Therefore, "n" is perfect if and only if $\sigma(n) = 2n$ that $\sigma(n)$ is the sum of divisor of "n" (with itself). Mental principle of perfect numbers roots back to ancient Greece's times and we must search it in history. Greeks had a lot of secret properties for these numbers. Greek mathematicians had a lot of tendency to these numbers. Although they knew only 4 perfect numbers in Euclid themes that are: 6, 28, 496 and 8128.

In spite of this little and deficit information, they guessed even perfect numbers finish with 6 or 8 that 5th and 6th number of perfect numbers are 33550336 and 8589869056 that both of them finish to "6". Of course this result is correct that perfect number finishes with 6 or 8. Euclid mentioned the following method for calculating perfect numbers in his book "preliminaries".

1.9.2. Theorem’s Euclid

Suppose $2^n - 1$ is prime, then $2^{n-1}(2^n - 1)$ is a perfect number.

Proof. Suppose $N = 2^{n-1}.p$ then $p = 2^n - 1$. Since "p" is prime, then divisors of $(2^{n-1}.p)$ are in 2^i or $(2^i.p)$ form clearly $0 \le i \le n-1$.

Therefore:

$$\begin{aligned}\sigma(N) &= 1 + 2 + ... + 2^{n-1} + p + 2p + ... + 2^{n-1}p \\ &= (1+p)\,(1 + 2 + ... + 2^{n-1}) \\ &= (1+p)\,(2^n - 1) = 2^n(2^n - 1) = 2N\end{aligned}$$

Therefore "N" is a perfect number.

The natural question that propounded is that:

Is the inverse of this Euclid theorem established? Are all of perfect numbers, in mentioned form in (1.9.2)?

Almost, 2000 years after that, Euler answered it.

1.9.3. Remark

Euclid algorithm is not an organized method to calculate the highest common divisor of two numbers. Euclid expressed and proved this algorithm in his book "Preliminaries". Of course, may be this algorithm was known before Euclid, below lemma is the key of understanding Euclid algorithm.

1.9.4. Lemma

Suppose "m" and "n" are integer numbers that both of them are not "o" together. So, for every correct number:

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

1.9.5. Theorem’s Euler

All of the even perfect numbers are in $2^{n-1}(2^n-1)$ form which 2^n-1 is a prime number.

Proof. Suppose "*N*" is an even perfect number. At that rate $\sigma(N)=2N$

Put $N=2^{n-1}m$, which $n\geq 2$ and "*m*" is a prime number.

Since $(2^{n-1},m)=1$ and σ is a multiplicative function, we will have:

$$2^n m=2N=\sigma(N)=\sigma(2^{n-1})\sigma(m)=(2^n-1)\sigma(m)$$

By solving the equivalence $2^n m=(2^n-1)\sigma(m)$, with respect to $\sigma(m)$ we will have:

$$\sigma(m)=m+\frac{m}{2^n-1} \qquad (2)$$

Therefore, $m/(2^n-1)$ is a integer number. Then both "m" and $m/(2^n-1)$ are divisors of "*m*". Because, $\sigma(m)=m+m/(2^n-1)$, from this we know that "*m*" and $m/(2^n-1)$ are only the positive divisors of "*m*". So, $m/(2^n-1)=1$ means $m=2^n-1$ and in the result "*m*" is a prime number.

Here, we remember two problems about perfect numbers.

The first of them is this odd perfect number. So, we know if there is an odd perfect number, it must be greater than 10^{300} and therefore it has 8 distinctive prime factors at least.

With these descriptions, we can result that there isn’t odd perfect number.

The second problem is none response until now that, Are the number of perfect numbers infinite? In the primary ages they have known four perfect numbers which had been considered before.

But the fifth of these numbers hasn’t been discovered until 15th century, till now; we know 42 even perfect numbers (2005). The first 21 of them have been discovered up to the year 1900.

For example, the known perfect number 2^{859432} $(2^{859433}$-1) is an ogre of mathematics with 517430 Digit almost. Then existing infinite perfect numbers, has been remained an open problem till now. Now after determining the highest prime number of 21st century, in fact the highest perfect number also calculates the:

Highest known perfect = $2^{25964950}(2^{25964951}$-1) number of the year 2005.

We finish this section By mentioning some important theorems about prime numbers like Bertrand’s principle. We know that Bertrand’s principle propounds existing prime numbers between numbers "*n*" and "2*n*".

Joseph Bertrand propounded his guess in 1845 and searched it for numbers between "1" and "3,000,000". But Russian mathematician Chebyshev solved it logically. Although its proof is easier than prime numbers "1", remember only its stronger results.

1.10. Bertrand's principle and theorems of Chebyshev, Dirichlet and Poisson

1.10.1. Bertrand's principle

For every $n > 1$, a prime number exists between "n" and "$2n$".A stronger result of Bertrand's principle is:

1.10.2. Result

If "n>5", then at least two different prime numbers exist between "n" and "$2n$". Another obvious result is that inequality " $p_{n+2} < 2p_n$ " results

$$p_{n+2} < p_n + p_{n+1}$$

1.10.3. Generalization

In 1892 Bertrand's principle way extended by James Joseph Sylvester in the following from:

If "m" and "n" are two positive integer numbers and $m > n$, then at least, one of numbers $m+1, m+2, ..., m+n$ has a prime divisor greater than "n". (With thesis that $m = n+1$, Bertrand's principle is resulted)

Another important theorem about prime numbers is Dirichlet's theorem that if "a" and "b" ($a \neq 0$) are coprime, then infinite prime numbers exist in "$ak+b$" form that $k \in n$. It is obvious that if "a" and "b" have common factors greater than "1", then for every integer number "k","$ak+b$" is a compound number.

For example, existing infinite prime numbers in "4k +3" and "4k +1" form is obvious.

1.10.4. Dirichlet's theorem

Suppose "$a > 0$", "$b > 0$" and $(a,b) = 1$. Therefore infinite integer number "k" exists. So that "$ak+b$"is "a" prime number.

Dirichlet's theorem is the first important application of analytic methods in number theory. In fact, Dirichlet's theorem and prime numbers theorem are two important theorems of primary theory of numbers that are solved by analytic methods. For both of these two theorems, primary proofs exist that it doesn't use deep theorems of functions theory. But expressing their proof is so hard that it is not in the frame of this book.

Now, we propound a combination of prime numbers theorem and Dirichlet's theorem:

1.10.5. Poisson's theorem

Suppose "a" is a positive number and (a, b) =1 and it defines $\pi_{a,b}(x)$ is the number of prime numbers in $ak+b$ form and smaller than "x". Then we can approach quotient of $\pi_{a,b}(x)/(x/Ln\,x)$ sufficiently to $1/\varphi(a)$, if "x" is great sufficiently.

1.10.6. Remark

Limit of $1/\varphi(a)$ does not depend on choosing "*b*" until "*a*" and "*b*" are coprime. Quotient tends to a limit that only depends on "*a*".

1.10.7. Result of theorem (1.10.5)

If "$d_1,...d_n$" and "$e_1,...,e_n$" are sets of digits so that e_n are odd and "$e_n \neq 5$", then there will be infinite prime numbers so that start with digits "$d_1,...,d_n$" and finish with "$e_1,...,e_n$". Theorem (1.10.5) has very beautiful interpolation that probably it doesn't see obviously from above propositions.

Fore example, if "$a = 4$", then it is resulted from theorem (1.10.5) that (since "$\varphi(4) = 2$") half of prime numbers are in "$4k+1$" form and another half is in "$4k+3$" form. (Exactly, we can approach the ratio of "$\pi_{4,1}(x)/\pi(x)$" to ½ for "*x*" that is sufficiently great). Therefore, we can find out from theorem (1.10.5) that if "$a = 8$", then a quarter of all prime numbers are in "$8k+5$" form and the last quarter in "$8k+7$" form. Generally, By supposing "$a \neq 0$", if "$b' \equiv b$" (mod *a*) then "*n*" is in $ak + b'$ form if and only if "*n*" is in "$ak + b$" form.

So, we can only calculate $\varphi(a)$ different values for "*n*" So that "*a*" and "*b*" are coprime. Therefore, it is resulted from theorem (1.10.5), that for every permissible value of "*b*", sequence of the numbers "$a, a+b, a+2b$ ..." includes the equal ratio of prime numbers; it means that the ratio of prime numbers is $1/\varphi(a)$.

1.11. Lagrange’s theorem

Suppose "*p*" is a prime number and "*n*" a natural number then the greatest power of prime number "*p*" in "*n*!" is equal to:

$$t=\left\lfloor \frac{n}{p}\right\rfloor+\left\lfloor \frac{n}{p^2}\right\rfloor+\left\lfloor \frac{n}{p^3}\right\rfloor+....$$

($\lfloor\ \rfloor$: Number integer part).

Proof. We want to count the number of prime factors of "*p*" in "*n*!".

The number of integer numbers among the numbers "1, 2, …, *n*" that "*p*"

aliquot them, is equal to $\left\lfloor \frac{n}{p}\right\rfloor$.But some of these numbers are also divisible by "p^2". Especially in the sequence 1, 2,..., *n*, the number of numbers which is divisible by "p^2" is exactly equal to $\left\lfloor \frac{n}{p^2}\right\rfloor$ and etc.

Therefore the sum of $\left\lfloor \frac{n}{p}\right\rfloor+\left\lfloor \frac{n}{p^2}\right\rfloor+...$ is equal to the number of prime factors of "*p*" that exists in *n*! ; It is necessary to mention that this summation has always a finite number of non-zero terms. Because for supposed "*n*", there is "*k*", so that $\frac{n}{p^k}<1$, therefore, $\left\lfloor \frac{n}{p^k}\right\rfloor=0$.

On the other word:

We suppose numbers "*n*" and "k" as natural number and $p\le n$ as a prime number. It is clear that numbers of $\{n\}$ sequence are divisible by "p^k" must be in "sp^k" form that "s" is a natural number and adapted in condition "$sp^k\le n$" in which $s\le\frac{n}{p^k}$. It is obvious that the number of "s" values is $\left\lfloor \frac{n}{p^k}\right\rfloor$. On the other hand "*t*" ("*p*" power) that appear in factorization of "*n*!" to prime factors *n* is obtained from sum of numbers which are the number of $\{n\}$ sequence’s terms divisible by "p" or "p^2"or "p^3"or ... "p^k".Therefore justification of relation (1) is verified.

1.11.1. Example

Calculate the greatest power of "$m=15$"that aliquot "62!".

Solution. According to "$15=3\times5$"and considering this point that greatest power of "5" is smaller than the greatest power of "3" which aliquot "62!", it is enough to determine the greatest power of "5" which aliquot "62!":

$$\begin{aligned} t &= \left\lfloor \frac{62}{5} \right\rfloor + \left\lfloor \frac{62}{5^2} \right\rfloor + \left\lfloor \frac{62}{5^3} \right\rfloor + \dots \\ &= \left\lfloor \frac{62}{5} \right\rfloor + \left\lfloor \frac{62}{25} \right\rfloor + 0 = 12 + 2 = 14 \end{aligned}$$

It is obvious that the greatest power of "3" which aliquot 62! is the least "14". So the greatest power of "15" which aliquot "62!" is "14" (number 15^{14}).

1.11.2. Example

How many zeros the number 100! is ended to?

Solution. In fact, we must calculate he greatest power of "$10 = 2 \times 5$" in "100!". Since the greatest power of "5" is smaller that the greatest power of "2" which aliquots "100!". We determine only the greatest power of "5" that aliquots 100! :

$$t = \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{5^2} \right\rfloor + \left\lfloor \frac{100}{5^3} \right\rfloor + \dots = 20 + 4 + 0 = 24$$

Therefore, 100! is ended to "24" zero.

1.11.3. Example

How many zeros the number $\frac{340!}{170!}$ is ended to?

Solution. The greatest power of "10" that aliquots "340!" is:

$$t = \left\lfloor \frac{340}{5} \right\rfloor + \left\lfloor \frac{340}{5^2} \right\rfloor + \left\lfloor \frac{340}{5^3} \right\rfloor + \dots = 68 + 13 + 2 = 83$$

And also, the greatest power of "10" that aliquots "170!" is:

$$t' = \left\lfloor \frac{170}{5} \right\rfloor + \left\lfloor \frac{170}{5^2} \right\rfloor + \left\lfloor \frac{170}{5^3} \right\rfloor + \dots = 34 + 6 + 1 = 41$$

Therefore, number $\frac{340!}{170!}$ is ended to "83-41=42" zero.

1.11.4. Example

Find natural number "*n*" in which "n!" is ended to "20" number of zero.

Solution. It is clear that number "n!" is ended to "20" number of zero if and only if the greatest power of "5" that aliquots "*n*!" is equal to "5^{20}". On the other hand we want to find "*n*" that

$$t = \left\lfloor \frac{n}{5} \right\rfloor + \left\lfloor \frac{n}{5^2} \right\rfloor + \left\lfloor \frac{n}{5^3} \right\rfloor + \dots = 20$$

If "$n = 125$", then "$t = 31$" and if "$n = 75$", then "$t = 18$", therefore, it is clear that $75 < n < 125$.

If "$n = 75 + 5k + s$", then, we can write $(k, s \in IN)$:

$$t=\left\lfloor \frac{75+5k+s}{5}\right\rfloor+\left\lfloor \frac{75+5k+s}{25}\right\rfloor$$
$$=15+k+\left\lfloor \frac{s}{5}\right\rfloor+3+\left\lfloor \frac{k}{5}\right\rfloor+\left\lfloor \frac{s}{25}\right\rfloor=20$$

If "$0\le k\le 4$" and "$0\le s\le 4$", then:

$$t=15+k+3=20 \quad ; \quad k=20-18=2$$

Therefore, values of "n" will be determined for "$k=2$" and "$0\le s\le 4$":

$$(k=2): n=75+5k+s=75+5(2)+s=85+s\ ;$$
$$0\le s\le 4: n=85,86,87,88,89$$

1.11.5. Example

If we suppose that "$n!$" finishes to "t_k" the number of zero, shows that "t_k" is close to $\frac{n}{4}$ for great number of "n".

Solution. It is clear that "t_k" is equal to the greatest power of "5" which aliquots "n!" (According to theorem 1.11):

$$t_k=\left\lfloor \frac{n}{5}\right\rfloor+\left\lfloor \frac{n}{5^2}\right\rfloor+\left\lfloor \frac{n}{5^3}\right\rfloor+\ldots+\left\lfloor \frac{n}{5^k}\right\rfloor+\ldots \qquad (1)$$

It is obvious that if "$0<\frac{n}{5^k}\le 1$", then "$k\ge \log_5^n$" and it means that there is not more than "$\lfloor \log_5^n \rfloor+1$" nonzero terms in "$t_k$". Here, we consider the following geometric progression:

$$s_k=\frac{n}{5}+\frac{n}{5^2}+\frac{n}{5^3}+\ldots+\frac{n}{5^k}+\ldots \qquad (2)$$

By comparing every term of (1) series with every term of (2) series:

In special case:

$$(n=5^k : s_k-t_k=0) \qquad 0\le s_k-t_k<k$$
$$k=\lfloor \log_5^n \rfloor+1\ :\ 0\le s_k-t_k<1+\lfloor \log_5^n \rfloor \qquad (3)$$

The limit of infinite terms of geometric progression (2) is equal to $s=\frac{n}{4}$, so, we have the following relation by substituting this value instead of s_k:

(In fact, if "n" be great infinitely, "k" is great infinitely)

$$\frac{1}{4}-\frac{1+\lfloor \log_5^n \rfloor}{n}<\frac{t_k}{n}\le\frac{1}{4} \qquad (4)$$

Since the rate of changing of logarithmic function is slower than "n", then if we choose "n" great enough, we can approach the quotient of $\frac{t_k}{n}$ to $\frac{1}{4}$ so that "t_k" is equal to "n/4" approximately.

1.11.6. Example

Whether number "$n!$" can finish to 48 number of zero?

Solution. It is clear that for solving this problem, it is enough to determine the greatest power of "5" which aliquots "$n!$" . For"$n = 200$", we calculate:

$$t = \left\lfloor \frac{200}{5} \right\rfloor + \left\lfloor \frac{200}{5^2} \right\rfloor + \left\lfloor \frac{200}{5^3} \right\rfloor + ... + \left\lfloor \frac{200}{5^k} \right\rfloor = 40 + 8 + 1 = 49$$

On the other hand, this summation is equal to "47"for"$n = 199$". Therefore, "$n!$" can not finish to "48" number of zero fore no natural "n".

1.11.7. Paractice. How many zero the number $\binom{2n}{n}$ is ended to?