Introduction of Number Theory

Number theory

Dr. Payman A. Rashed

Salahaddin University-Erbil College of Basic Education Department of Mathematics

Fourth Stage \ 2023-2024

Chapter one

- **Number theory Number**

theory divided in to three branches as follow:

i- Elementary number theory

ii- Algebraic number theory

iii- Analytic number theory

The theory of numbers is concerned, at least in its elementary aspects, with properties of the integers and more particularly with the positive integers 1, 2, 3, ... (also known as the natural numbers).

The origin of this misnomer harks back to the early Greeks for whom the word number meant positive integer, and nothing else. The natural numbers have been known to us for so long that the mathematician Leopold Kronecker once remarked, "God created the natural numbers, and all the rest is the work of man.

Definition1.1: Well-Ordering Principle.

Every nonempty set S of nonnegative integers contains a least element; that is, there is some integer a in S such that $a \leq b$ for all b's belonging to S.

- Because this principle plays a critical role in the proofs here and in subsequent chapters, let us use it to show that the set of positive integers has what is known as the Archimedean property.

Theorem 1.2: Archimedean property. If a and b are any positive integers, then there exists a positive integer n such that $na \geq b$.

Proof: Assume that the statement of the theorem is not true, so that for some a and b, $na < b$ for every positive integer n. Then the set $S = \{b - na \mid n \text{ a positive integer}\}$ consists entirely of positive integers. By the Well-Ordering Principle, S will possess a least element, say, $b - ma$.

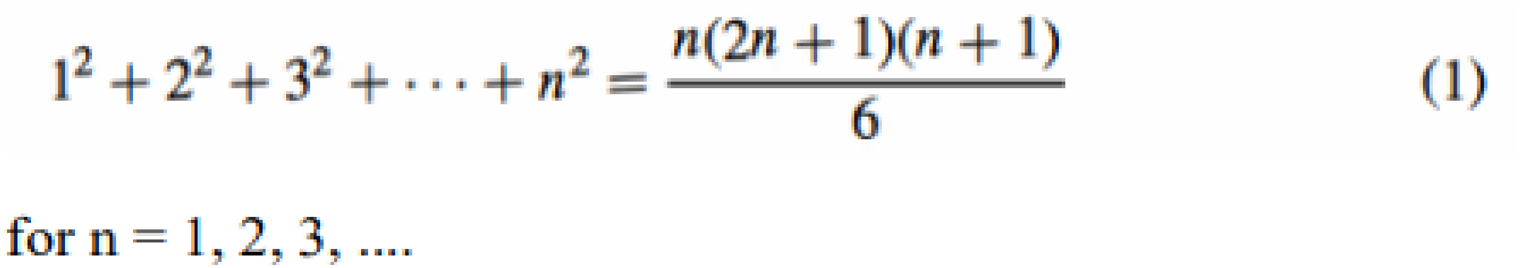
Notice that $b - (m + l)a$ also lies in S, because S contains all integers of this form. Furthermore, we have $b - (m + l)a = (b - ma) - a < b - ma$ contrary to the choice of $b - ma$ as the smallest integer in S. This contradiction arose out of our original assumption that the Archimedean property did not hold; hence, this property is proven true.

Theorem 1.3: First Principle of Finite Induction. Let S be a set of positive integers with the following properties:

(a) The integer 1 belongs to S.

(b) Whenever the integer k is in S, the next integer k + 1 must also be in S.

Then S is the set of all positive integers. Here is a typical formula that can be established by mathematical induction:



$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(2n+1)(n+1)}{6} \qquad (1)$$

for n = 1, 2, 3, ...

In anticipation of using Theorem 1.2, let S denote the set of all positive integers n for which Eq. (1) is true. We observe that when n = 1, the formula becomes

$$1^2 = \frac{1(2+1)(1+1)}{6} = 1$$

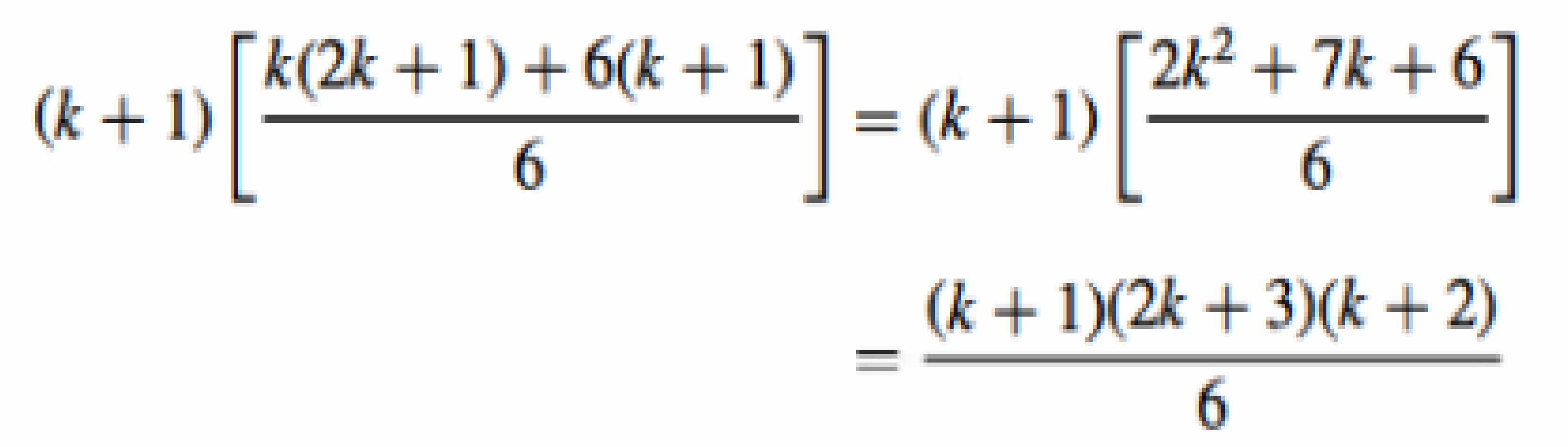
This means that 1 is in S. Next, assume that k belongs to S (where k is a fixed but unspecified integer) so that

$$1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{k(2k+1)(k+1)}{6} \qquad (2)$$

To obtain the sum of the first k + 1 squares, we merely add the next one, (k + 1)2, to both sides of Eq. (2). This gives

$$1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = \frac{k(2k+1)(k+1)}{6} + (k+1)^2$$

After some algebraic manipulation, the right-hand side becomes

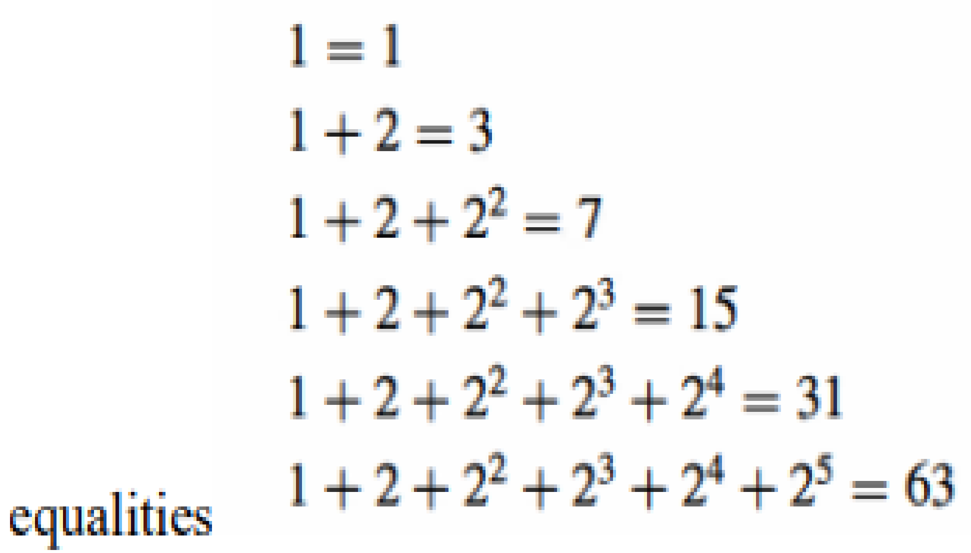


$$(k+1)\left[\frac{k(2k+1)+6(k+1)}{6}\right]=(k+1)\left[\frac{2k^2+7k+6}{6}\right]$$

$$=\frac{(k+1)(2k+3)(k+2)}{6}$$

which is precisely the right-hand member of Eq. (1) when n = k + 1. Our reasoning shows that the set S contains the integer k + 1 whenever it contains the integer k. By Theorem 1.2, S must be all the positive integers; that is, the given formula is true for n = 1, 2, 3, ...

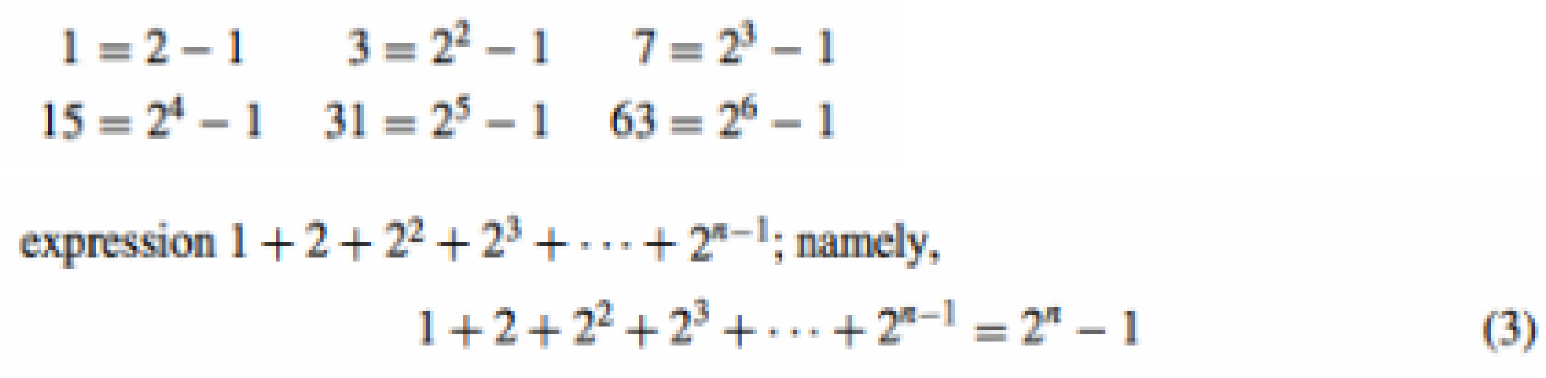
Although mathematical induction provides a standard technique for attempting to prove a statement about the positive integers, one disadvantage is that it gives no aid in formulating such statements. Of course, if we can make an "educated guess" at a property that we believe might hold in general, then its validity can often be tested by the induction principle. Consider, for instance, the list of



$$\begin{aligned}
&1 = 1\\
&1 + 2 = 3\\
&1 + 2 + 2^2 = 7\\
&1 + 2 + 2^2 + 2^3 = 15\\
&1 + 2 + 2^2 + 2^3 + 2^4 = 31\\
&1 + 2 + 2^2 + 2^3 + 2^4 + 2^5 = 63
\end{aligned}$$

equalities

We seek a rule that gives the integers on the right-hand side. After a little reflection, the reader might notice that



$$1 = 2 - 1 \qquad 3 = 2^2 - 1 \qquad 7 = 2^3 - 1$$
$$15 = 2^4 - 1 \qquad 31 = 2^5 - 1 \qquad 63 = 2^6 - 1$$

expression $1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1}$; namely,

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^{n-1} = 2^n - 1 \tag{3}$$