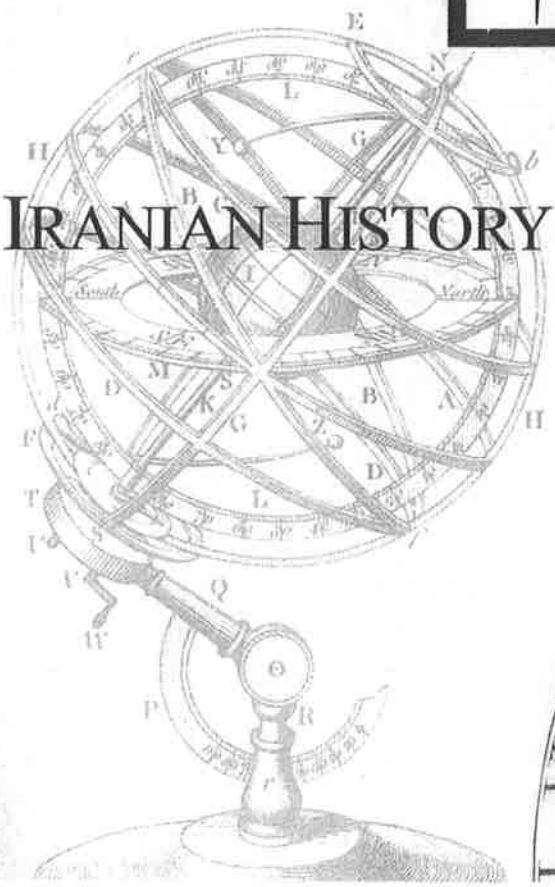
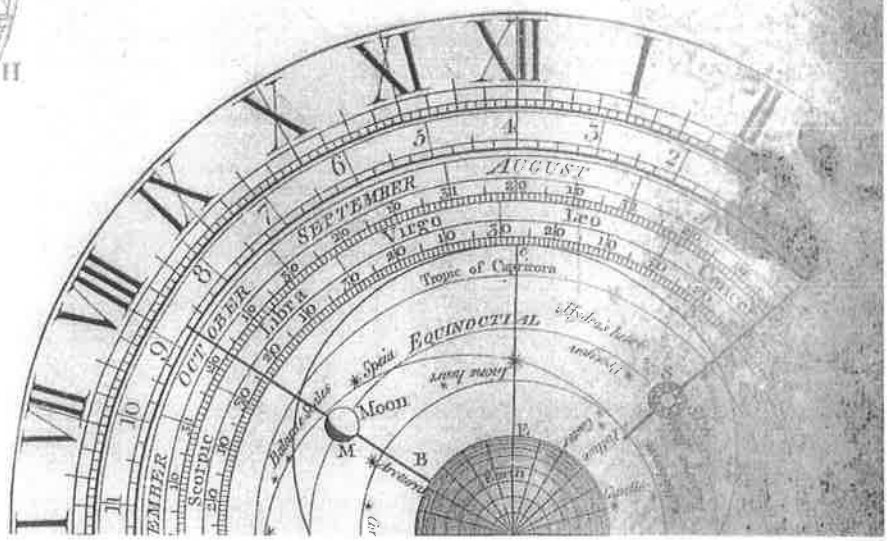
Vol. 3, No. 11/ Summer 2013

Institute for the History of Science
University of Tehran

خبرنامهٔ تاریخ علم

IRANIAN HISTORY OF SCIENCE NEWSLETTER





History of Science Newsletter
Vol. 3, No. 11, Summer 2013

Publisher: **Institute for the History of Science, University of Tehran**

Chief Editor: **Abouzar Farzpourmachiani**
Co-Editor: **Maryam Zamani**
Designer: **Farnaz Azidhak**
Editor: **Fateme Keyghobadi**

Advisory Board
Mohammad Bagheri
Hamid-Reza Giahi Yazdi
Iraj Niksereshт
Asghar Qaedan

Contributors to this issue
Irem Aslan
Sara Farzpourmachiani
Amir-Mohammad Gamini
Zahra Ghezelbash
Fateme Keyghobadi
Razie-Sadat Mousavi
Iraj Niksereshт
Morteza Somi
Mohammad-Hadi Tabatabayi

Address: No. 23, Behnam Alley, Ghods Street, Enghelab Avenue, Tehran 1417734491, Iran
Mailing Address: P.O. Box 13145-1836, Tehran, Iran
Tel: (+98) 21 88993016
Fax: (+98) 21 88993018
www.utihs.ut.ac.ir
tarikhelm@ut.ac.ir

History of Science Newsletter is going to reflect academic activities in history of science, such as conferences, commemorations, published books and journals, etc. Hence contributions by sending reports or news are appreciated.

News

Report

Thesis

Lecture

Introduction

Table of Farsi contents

News

Report

Introduction

Thesis

made by some historians of astronomy in recent decades. Shīrāzī and the other members of Marāgha Shool's naturalistic account of Ptolemaic models bring Hay'a in relation with Aristotelian natural philosophy. Although Ptolemy mentions some Aristotelian natural principles in his works, especially in the *Planetary Hypothesis*, astronomers of the Marāgha School, probably under influence of Ibn la-Haytham (965-1040), reaffirm these principles and believe Ptolemaic models are not in agreement with them. It motivates them to develop new astronomical models which nowadays are called non-Ptolemaic planetary models. Shīrazī, as a young member of the School, presents Ṭusī and ᶜUrḍī's models in *Nihāya* and *Ikhtiyārāt* and puts forward his critics upon them that encourage him to develop his own new models. Since his models for superior planets and Mercury were not without difficulty, his third work, *Tuḥfa*, appears 4 years later with new models for superior planets and Mercury. *Tuḥfa* includes a model for superior planets which is inspired by ᶜUrḍī's model to which is added some new models for the motion in latitude. Shīrāzī offers 8 models for Mercury in a developing process which makes it possible to see how he developed his sophisticated final model.

Mathematical instruments and their effects on the mathematics[1]

• İrem Aslan[2]

While Europe was in its dark ages, medieval Islam science was in its peak point, especially mathematics and astronomy that were the most important sciences for Islam religion. Even today most of the constellation's name has the Arabic etymologic roots: such as Denep (means tail in Arabic and it is the part of summer triangle, and also the tail and the alpha of the Cygnus (swan)), Altair (alpha of Aquila (eagle) constellation, means fly).

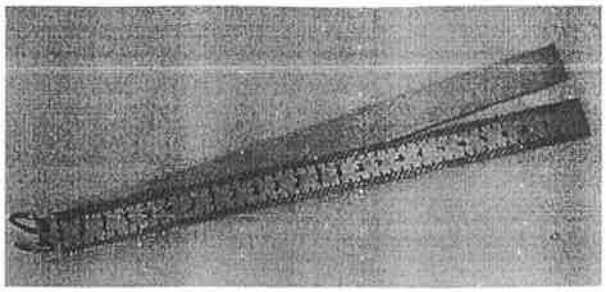
Islamic scholars had ancient Greek manuscripts and they translated them in Arabic (Arabic was the language of science). The scholars not only memorize the translations they did study them, they made considerable progress, and they lean down the problematic parts. The transmission of the problems happened under auspices of the Islamic scholars.

They interested both the applied and the theoretic part of mathematics. They made remarkable progress in the theoretic part. But applied mathematics has another meaning which is directly necessary for the Islam religion. First of all they have to determine the Namaz time, and the Qibla way (The determination of the azimuth of the Qibla) which are both still not easy estimations. Also navigation was another important problem to solve which was necessary for marine. They need astronomy, geography and especially mathematics knowledge in order to calculate those values. Those were the main stimulus of calculating time, discovering the new sundials, quadrants, astrolabes and the other mathematical instruments. Theoretical mathematics doesn't need any instruments for sure. But theoretical mathematics had also affected from those instruments.

The efficacy of the mathematical instruments leads the mathematicians to use the kinematics to solve the theoretical problems. But the scholars divided in to two parts at this point. For some scholars like Thabit ibn Qurra (836-901), and Ibn al-Haytham (965-1040), using kinematics in the mathematical proofs was valid[3], so it is not a coincidence that these two scholars both used kinematics in their proofs of Euclid's fifth postulate. But the others like Omar Khayyam (1038/48-1123/4) and Nasıreddîn Tusî (1201-1274) strongly opposed the idea of the using the "movement" in the proofs of mathematical theorems. For Khayyam even Euclid didn't use the movement in his proofs. The kinematics in the Elements is only valid for one reference point such as a line which is made of from movement of a point, a surface which is made of from movement of a line, or a circle which is made of from a rotation of a line.[4] The mathematical instruments was not abolishing that rule so they were all valid. But two parallel lines which is made of from movement of a line (end points) is not valid in Euclid's geometry since there are two reference point mentioned there (That was the core of Thabit's and Haytham's proofs).

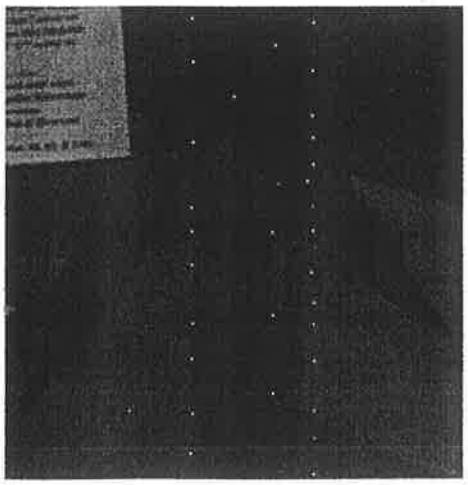
The mathematical instruments which has used in the time of Islam are now on display in the Islam Science and Technology Museumin İstanbul (in Gülhane Park). The instruments may be considered in the four groups in the section of mathematics as: Compasses,

protractors, leveling instruments, surveying tools and the others like platonic solids, dasturs, doublerulers (picture 1) (both are used for prepare perfect astrolabes), and tripods.



Pic. 1

Compasses were especially important for geometers. Trisection of an angle "teslisi zaviye" was one of the most famous problems, which was inherited from Ancient Greek (others were duplication of the cube "tazif-i mikab" and squaring the circle "terbi-i daire"). The main purpose in those problems was, the solution only considered valid if you were using compass and ruler (but the solution of those 3 problems is impossible if you just use compass and ruler). They also used "rusty compass" (fixed to an angle) and "conchoidal compasses" So the compass tradition had been taken from the Greeks and many models has produced by Islamic scholars. For example, the compass which was calculating Namaz time was also a sundial (picture 2), which is based on Musa al-Khwarizmi (780-850).



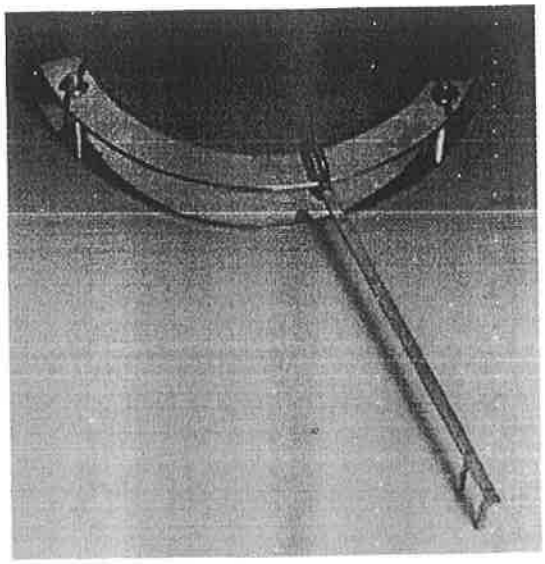
Pic. 2

Each position of the sun has recorded on the arms of the compass. It is used by embedding the sharp sides to the ground and by the help of the proportions the calculations has easily made. There were also conic sections compasses (are invented by Ebû Sehl al-Kûhî in second half of the 10th century) (Picture 3 and 4), compasses for drawing large semicircles and segments of circles of Ibn al-Haytham (Picture 5). The other instrument which has used commonly in the Islamic word was leveling instruments. Ibn Sina's leveling instrument (Picture 6) for the leveling of astronomical observation instrument using water (not usual pure water but colored water to avoid from reflections). It is used for to calculate the height of the stars.

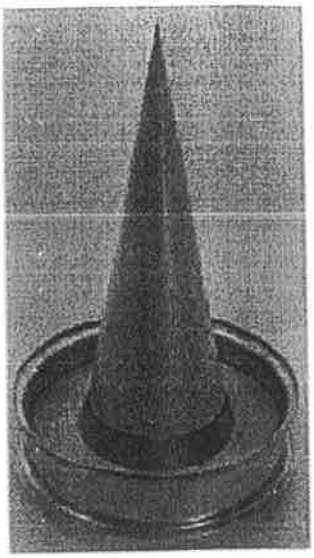
All those instruments and more, have lots of contributions to the mathematics and astronomy. They are not only helped to the improvement of the sciences, but they also gave another aspect to the mathematicians as "kinematics". They had been the display of the application of the pure mathematics, to the nature.

Pic. 3

Pic. 4



Pic. 5



Pic. 6

[1]Lecture that presented in the Second International Summer School at the Istanbul Museum of the History of Science and Technology. Author's Turkish intonation of Arabic phrases isn't changed in this text by editor.
[2]PhD Student in Ankara University, History of Science Department. iremaslan8@yahoo.com
[3]Sabra, A. I., "Thabit ibn Qurra: on Euclid's parallels postulate".
[4]Amir- Moez, Ali Riza, "A Paper of Omar Khayyâm"

A Modern Application of Kindi's Cryptanalytic Techniques[1]

Wiet van Lanschot, Edzard Scherpbier, Koen van Woerden

Abstract

Kindi was a Muslim polymath who wrote a large number of scientific works on a wide range of subjects. Raised in Basra, he went to Baghdad to complete his studies, where he drew the attention of Caliph Ma'mun, who appointed him to his House of Wisdom. In 70 years he wrote more than 290 scientific works, language being a recurring object of study.

Recently discovered [1] is his treatise on cryptanalysis, called "Risalah fi Is-tikhraj Mu'amma", which is the oldest known record of cryptanalysis today. In this manuscript, the oldest known description of the use of frequency analysis for deciphering encrypted messages is found. Kindi first provides a classification of the cryptographic methods known to him, and then gives a systematic way to attack these various methods, in which frequency analysis plays a prominent role.

In the course of our analysis of Kindi's work, we will apply frequency analysis ourselves to an encrypted text, with Kindi as our guide, showing that today his treatise is not only of historical interest, but also of practical value.

Introduction

Cryptography, the art of encoding messages, has been widely used throughout history. As writing became an often used method to communicate, the desire to make one's writing less readable to others emerged as well. The earliest use of cryptography was in Ancient Egypt around 1900 B.C., where a message, chiseled in the wall, contained multiple unconventional symbols.

As the Ancient Egyptian civilization grew, this form of encryption became widely used. It was mostly used to make hymns and blessings harder to read. In order to read the encrypted messages, often displayed in plain sight, one had to concentrate and puzzle before the true nature of the message could be understood (Kahn [1969]).

A more conventional form of cryptography is mentioned in Kama Sutra, around 300 B.C., 1000 B.H., as a method that lovers could use to communicate in a safe way (Vatsyayana, Doniger, and Kakar [2009, p1, h3, art. 45]). This method required