11

The Number Theory Revival

11.1 Between Diophantus and Fermat

Some important results in number theory were discovered in the Middle Ages, though they failed to take root until they were rediscovered in the seventeenth century or later. Among these were the discovery of Pascal's triangle and the "Chinese remainder theorem" by Chinese mathematicians, and formulas for permutations and combinations by Levi ben Gershon (1321). The early development of the Chinese remainder theorem is discussed in Chapter 5, and the theorem did not reemerge until after the period we are about to discuss. A full account of its history may be found in Libbrecht (1973), Chapter 5. Pascal's triangle, on the other hand, began to flourish in the seventeenth century after a long dormancy, so it is of interest to see what was known of it in medieval times and what Pascal did to revive it.

The Chinese used Pascal's triangle as a means of generating and tabulating the binomial coefficients, that is, the coefficients occurring in the formulas

$$\begin{array}{lc}
(a+b)^1 = & a+b \\
(a+b)^2 = & a^2+2ab+b^2 \\
(a+b)^3 = & a^3+3a^2b+3ab^2+b^3 \\
(a+b)^4 = & a^4+4a^3b+6a^2b^2+4ab^3+b^4 \\
(a+b)^5 = & a^5+5a^4b+10a^3b^2+10a^2b^3+5ab^4+b^5 \\
(a+b)^6 = & a^6+6a^5b+15a^4b^2+20a^3b^3+15a^2b^4+6ab^5+b^6 \\
(a+b)^7 = & a^7+7a^6b+21a^5b^2+35a^4b^3+35a^3b^4+21a^2b^5+7ab^6+b^7
\end{array}$$

and so on. When the binomial coefficients are tabulated as follows (with a trivial row 1 added at the top, corresponding to the power 0 of $a+b$),

$$\begin{array}{ccccccccccccccc}
&&&&&&&1&&&&&&&\\
&&&&&&1&&1&&&&&&\\
&&&&&1&&2&&1&&&&&\\
&&&&1&&3&&3&&1&&&&\\
&&&1&&4&&6&&4&&1&&&\\
&&1&&5&&10&&10&&5&&1&&\\
&1&&6&&15&&20&&15&&6&&1&\\
1&&7&&21&&35&&35&&21&&7&&1
\end{array}$$

and so on, the kth element $\binom{n}{k}$ of the nth row is the sum $\binom{n-1}{k-1}+\binom{n-1}{k}$ of the two elements above it in the $(n-1)$th row, as follows from the formula (Exercise 11.1.1)

$$(a+b)^n = (a+b)^{n-1}a + (a+b)^{n-1}b.$$

The triangle appears to a depth of six in Yáng Huí (1261) and to a depth of eight in Zhū Shijié (1303) (Figure 11.1). Yáng Huí attributes the triangle to Jia Xiàn, who lived in the eleventh century.

The number $\binom{n}{k}$ appears in medieval Hebrew writings as the number of combinations of n things taken k at a time. Levi ben Gershon (1321) gives the formula

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$

together with the fact that there are $n!$ permutations of n elements. In his treatment of permutations and combinations Levi ben Gershon comes very close to using mathematical induction, if not actually inventing it. As we now formulate this method of proof, a property $P(n)$ of natural numbers n is proved to hold for all n if one can prove $P(1)$ (the base step) and, for arbitrary n, one can prove $P(n) \Rightarrow P(n+1)$ (the induction step). Rabinovitch (1970) offered an exposition of some of Levi ben Gershon's proofs that certainly seems to show a division into a base step and induction step, but the induction step needs some notational help to become a proof for truly arbitrary n. Levi ben Gershon does not say "Consider n elements $a,b,c,d,\ldots,e$," as we might, but only "Let the elements be a,b,c,d,e," since he does not have the device of ellipses.

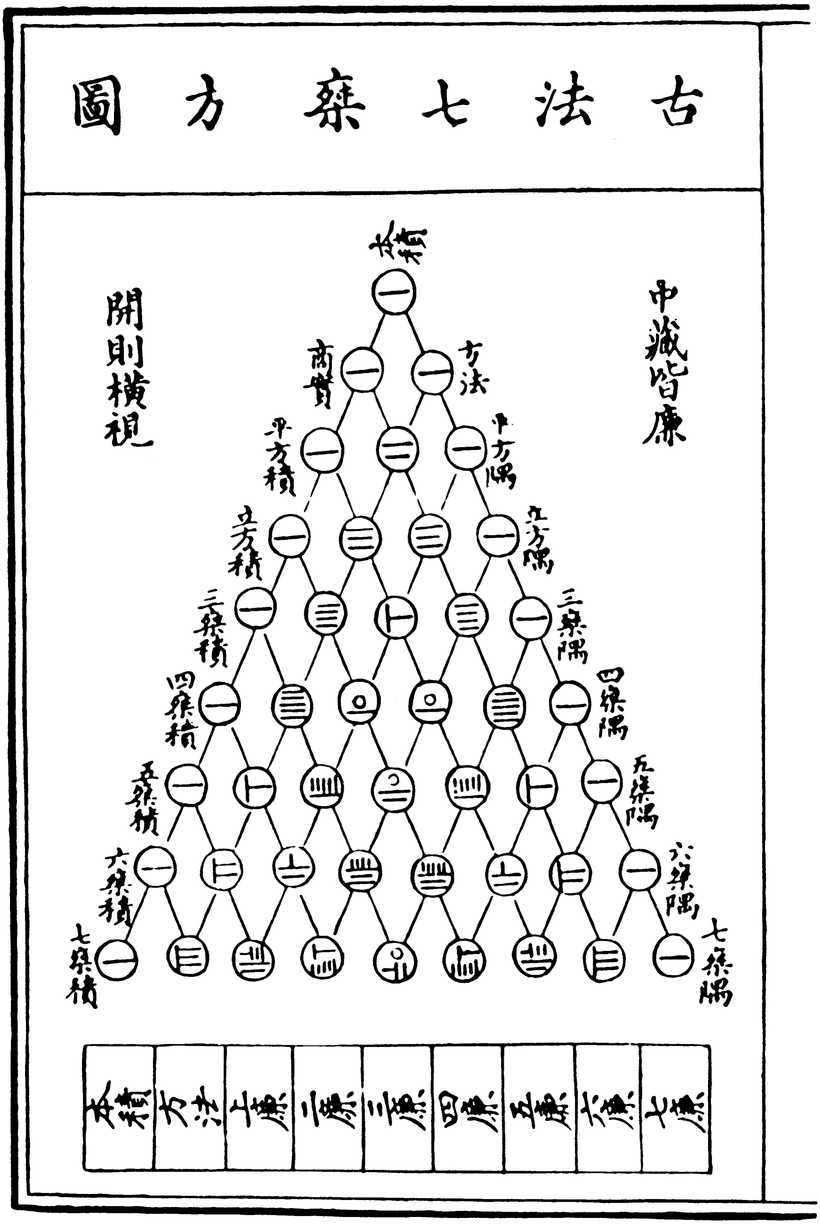

Figure 11.1: Chinese Pascal's triangle

In view of these excellent results, why do we call the table of binomial coefficients "Pascal's triangle"? It is of course not the only instance of a mathematical concept being named after a rediscoverer rather than a discoverer, but in any case Pascal deserves credit for more than just rediscovery. In his *Traité du triangle arithmétique* [Pascal (1654)], Pascal united the algebraic and combinatorial theories by showing that the elements of the arithmetic triangle could be interpreted in two ways: as the coefficients of $a^{n-k}b^k$ in $(a+b)^n$ and as the number of combinations of n things taken k at a time. In effect, he showed that $(a+b)^n$ is a *generating function* for the numbers of combinations. As an application, he founded the mathematical theory of probability by solving the problem of division of stakes (Exercise 11.1.2), and as a method of proof he used mathematical induction for the first time in a really conscious and unequivocal way. Altogether, quite some progress!

In going to Pascal's work in 1654 we have overshot the end of the pre-Fermat period in number theory, since Fermat was already active in this field in the 1630s. However, it is convenient to have some background of binomial coefficients established, since Fermat's early work appears in this setting.

EXERCISES

The basic properties of the binomial coefficients, for example the fact that each is the sum of the two above it in Pascal's triangle, follow easily from their interpretation as the coefficients in the expansion of $(a+b)^n$.

11.1.1 Use the identity

$$(a+b)^n = (a+b)^{n-1}a + (a+b)^{n-1}b$$

to prove the sum property of binomial coefficients:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

This property gives an easy way to calculate Pascal's triangle to any depth, and hence compute a fair division of stakes in a game that has to be called off with n plays remaining. We suppose that players I and II have an equal chance of winning each play, and that I needs to win k of the remaining n plays to carry off the stakes.

11.1.2 Show that the ratio of I's winning the stakes to that of II's winning is

$$\binom{n}{n} + \binom{n}{n-1} + \cdots + \binom{n}{k} : \binom{n}{k-1} + \binom{n}{k-2} + \cdots + \binom{n}{0}.$$