For example, let it be proposed to find the number of the cell ξ of the fifth perpendicular rank and of the third parallel rank.

Having taken all the numbers that precede the index of the perpendicular rank 5, that is, 1, 2, 3, 4, take as many natural numbers beginning with the index of the parallel rank 3, that is, 3, 4, 5, 6.

Now multiply the first numbers into each other, and let the product be 24. Multiply the other numbers into each other, and let the product be 360, which divided by the other product 24, gives 15 as the quotient. This quotient is the desired number.

Indeed, ξ is to the first number of its base V in composed ratio of all the ratios of the cells among themselves, that is,

$$\xi \text{ is to } V \text{ in composed ratio of } \underbrace{\xi \text{ to } \rho}_{3 \text{ to } 4} + \underbrace{\rho \text{ to } K}_{4 \text{ to } 3} + \underbrace{K \text{ to } Q}_{5 \text{ to } 2} + \underbrace{Q \text{ to } V}_{6 \text{ to } 1},$$

or by the twelfth consequence:

ξ is to V as 3 into 4 into 4 into 5 into 6 into 4 into 3 into 2 into 1,

But V is unity; hence ξ is the quotient of the division of the product of 3 into 4 into 5 into 6 by the product of 4 into 3 into 2 into 1.[8]

Note. If the generator were not unity we should have to multiply the quotient by the generator.

This paper is followed by several others, in which the Pascal triangle is applied.[9] First it is used to sum the arithmetical sequences of different orders 1, 2, 3, 4, etc.; 1, 3, 6, 10, etc., 1, 4, 10, 20, ... (these sequences are called "numbers of the first, second, etc. order" [*ordres numériques*], then to the solution of certain games of chance, to the finding of combinations, to the raising of binomials to different powers, to the summation of the squares, cubes, etc., of the terms of an arithmetical series, etc., and to the proof that (in our present notation) $\int_0^a x^p \, dx = \dfrac{a^{p+1}}{p+1}$, p a positive integer. On this integral see Selection IV.6.

6 FERMAT. TWO FERMAT THEOREMS AND FERMAT NUMBERS

Pierre de Fermat (1601–1665) was a lawyer attached as councilor to the provincial parliament (that is, law court) of Toulouse. Of his contributions to geometry and calculus we speak in Selections III.3 and IV.7, 8. He was the first to take up seriously the challenge offered in number theory by the *Arithmetica* of Diophantus, first made fully available in the original Greek of A.D. c. 250 by Claude Bachet in 1621, together with a Latin translation. Fermat communicated his results in letters to his friends or kept them to himself in notes,

[8] This means that $P_k^l = \dfrac{l(l+1)\cdots(l+k-2)}{1\cdot 2\cdots(k-1)} = C_{k-1}^{l+k-2}$; hence $C_p^n = P_{p+1}^{n-p+1}$, where

$C_p^n = \dfrac{m!}{p!(n-p)!}$, the number of combinations of n elements in groups of p.

[9] Some of this is translated in Smith, *Source book*, pp. 76–79.

---

many of them as marginal notes to his copy of Bachet. His son Samuel published a second edition of Bachet's Diophantus and added to it his father's marginal notes (Toulouse, 1670).

The extant work of Fermat has been published in the *Oeuvres de Fermat* (4 vols.; Gauthier-Villars, Paris, 1891–1912), in which the Latin texts are accompanied by a French translation (in vol. III, 1896).

We first quote the famous Latin marginal note to Diophantus' Proposition II, 8: "To divide a given square number into two squares," for which Diophantus gives the answer (in our notation) $[a(m^2 + 1)]^2 = (2am)^2 + [a(m^2 - 1)]^2$; for example, $a = \frac{16}{5}$, $m = \frac{1}{2}$; $16 = (\frac{16}{5})^2 + (\frac{12}{5})^2$; see *Oeuvres*, I, 53; French translation, III, 24. Fermat wrote:

In contrast, it is impossible to divide a cube into two cubes, or a fourth power into two fourth powers, or in general any power beyond the square into powers of the same degree; of this I have discovered a very wonderful demonstration [*demonstrationem mirabilem sane detexi*]. This margin is too narrow to contain it.

It is well known that nobody has ever found this *demonstratio sane mirabilis*, but also that nobody has been able to discover a positive integer $n > 2$ for which $x^n + y^n = z^n$ can be solved in terms of positive integers x, y, z. On the enormous literature in this field see P. Bachman, *Das Fermatproblem* (De Gruyter, Berlin-Leipzig, 1919); L. J. Mordell, *Three lectures on Fermat's last theorem* (Cambridge University Press, Cambridge, England, 1921); R. Noguès, *Théorème de Fermat. Son histoire* (Vuibert, Paris, 1932); H. S. Vandiver, "Fermat's last theorem," *American Mathematical Monthly 53* (1946), 555–578. We shall show (Selection I.9) how Euler proved Fermat's theorem for $n = 3$ and $n = 4$.

Fermat communicated many of his results to the mathematician Bernard Frénicle de Bessy (1605–1675). In a letter of October 18, 1640, written in French, we find, among many observations, the following paragraphs containing another theorem of Fermat, which states that a^{p-1} is divisible by p when p is prime and a, p are relatively prime. Fermat had been interested in Euclid's theorem (*Elements*, Prop. IX, 36) that numbers of the form $2^{n-1}(2^n - 1)$ are perfect, that is, equal to the sum of their divisors including 1 (for example, $6 = 1 + 2 + 3$, $28 = 1 + 2 + 4 + 7 + 14$), if $2^n - 1$ is prime. Such prime numbers $2^n - 1$ Fermat called the *radicals* of the perfect numbers, and he had sent to Father Marin Mersenne some of his conclusions about these radicals in a letter of June 1640.[1] (If n is not prime, $2^n - 1$ cannot be prime; if n is prime, $2^n - 2$ is divisible by n; if n is prime, $2^n - 1$ is divisible only by prime numbers of the form $2kn + 1$; for example, $2047 = 2^{11} - 1 = 23 \times 89$, $2^{11} - 2 = 2046 = 11 \times 186$.) Then, in August 1640, in a letter to Frénicle, Fermat had turned to numbers of the form $2^n + 1$, writing that he was "almost convinced"

[1] These radicals $2^n - 1$, when prime, are known as Mersenne numbers M_n. It is clear that n in this case must be prime, but this is not sufficient. For example, $M_{11} = 2047 = 23 \times 89$.
Father Marin Mersenne (1588–1648), a Minorite (Franciscan), was in constant correspondence with the outstanding mathematicians of his day. His *Correspondence* has been published in 8 volumes (ed. C. de Waard; Beauchesne, Édition du Centre National de la Recherche, Paris, 1932–1963).

[*quasi persuadé*] that these numbers are prime when n is a power of 2. We now know that, though this is true for $n = 2, 4, 8, 16$, it stops being true for $n = 32$, which, as Euler showed (*Commentarii Academiae Scientiarum Petropolitanae 1* (1732/33, publ. 1738), 20–48, *Opera omnia*, ser. I, vol. 2, p. 73) is divisible by 641 ($4294967297 = 641 \times 6700417$).[2] Fermat, on October 10, 1640, after referring to earlier letters, continues:

It seems to me after this that it is important to tell you on what foundation I construct the demonstrations of all that concerns the geometrical progressions, which is as follows:

Every prime number is always a factor [*mesure infailliblement*] of one of the powers of any progression minus 1, and the exponent [*exposant*] of this power is a divisor of the prime number minus 1. After one has found the first power that satisfies the proposition, all those powers of which the exponents are multiples of the exponent of the first power also satisfy the proposition.

Example: Let the given progression be

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 9 & 27 & 81 & 243 & 729 \end{array} \text{ etc.}$$

with its exponents written on top.

Now take, for instance, the prime number 13. It is a factor of the third power minus 1, of which 3 is the exponent and a divisor of 12, which is one less than the number 13, and because the exponent of 729, which is 6, is a multiple of the first exponent, which is 3, it follows that 13 is also a factor of this power 729 minus 1.

And this proposition is generally true for all progressions and for all prime numbers, of which I would send you the proof if I were not afraid to be too long.

But it is true that every prime number is a factor of a power plus 1 in any kind of progression; for, if the first power minus 1 of which the said prime number is a factor has for exponent an odd number, then in this case there exists no power plus 1 in the whole progression of which this prime number is a factor.

Example: Because in the progression of 2 the number 23 is a factor of the power minus 1 which has 11 for exponent, the said number 23 will not be a factor of any power plus 1 of the said progression to infinity.

If the first power minus 1 of which the given prime number is a factor has an even number for exponent, then in this case the power plus 1 which has an exponent equal to half this first exponent will have the given prime as a factor.

The whole difficulty consists in finding the prime numbers which are not factors of any power plus 1 in a given progression, for this, for instance, is useful for finding which of the prime numbers are factors of the radicals of the perfect numbers, and to find a thousand other things as, for example, why it is that the 37th power minus 1 in the progression of 2 has the factor 223. In one word,

---

[2] These numbers $2^n + 1$, $n = 2^t$, when prime, are known as Fermat numbers. See O. Ore, *Number theory and its history* (McGraw-Hill, New York, 1948).

we must determine which are the prime numbers that factor their first power minus 1 in such a way that the exponent of the said power be an odd number—which I think very difficult [*fort malaisé*].

Fermat then continues with other striking properties of powers, also of numbers of the form $2^n + 1$, which, he believed, are all prime if n is a power of 2.[3]

7 FERMAT. THE "PELL" EQUATION

In a letter of February 1657 (*Oeuvres*, II, 333–335; III, 312–313) Fermat challenged all mathematicians (thinking probably in the first place of John Wallis in England) to find an infinity of integer solutions of the equation $x^2 - Ay^2 = 1$, where A is any nonsquare integer. He may have been led to this by his study of Diophantus, who set the problem of finding, for example, a number x such that both $10x + 9$ and $5x + 4$ are squares. If these squares are called u^2 and v^2 respectively, then $u^2 - 2v^2 = 1$, and a solution is $x = 28$. The problem was taken up by De Billy (see below) and later by Euler, who in his "De solutione problematum Diophanteorum per numeros integros," *Commentarii Academiae Scientiarum Petropolitanae 6* (1732/33, publ. 1738), 175–188, *Opera omnia*, ser. I, vol. 2, 6–17, referred to the problem as that of Pell and Fermat. John Pell (1611–1685), an English mathematician, had little to do with the problem, but the problem of Fermat has since been known as that of the Pell equation. It had already been studied by Indian mathematicians, and even in the *Cattle Problem*, attributed to Archimedes, which leads to a "Pell" equation with $A = 4729494 = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 29 \cdot 353$; see T. L. Heath, *A manual of Greek mathematics* (Clarendon Press, Oxford, 1931), 337.

Fermat, after observing that "Arithmetic has a domain of its own, the theory of integral numbers," defines his problem as follows:

Given any number not a square, then there are an infinite number of squares which, when multiplied by the given number, make a square when unity is added.

Example.—Given 3, a nonsquare number; this number multiplied by the square number 1, and 1 being added, produces 4, which is a square.

Moreover, the same 3 multiplied by the square 16, with 1 added makes 49, which is a square.

And instead of 1 and 16, an infinite number of squares may be found showing the same property; I demand, however, a general rule, any number being given which is not a square.

It is sought, for example, to find a square which when multiplied into 149, 109, 433, etc., becomes a square when unity is added.

---

[3] See note 2.