UNIT 2 THE HIGHER ARITHMETIC-2

Structure

2.0 INTRODUCTION

The properties of the integers have been studied since ancient times; yet their importance to mathematical theory remains undiminished. They are the central theme of this Unit. People often have the feeling that mathematics is "serious business", that mathematicians must therefore be cold and dry and logical and rational; but we believe that mathematics is fun, and the lives of mathematicians, spent in search of proof and solution, are inspiring and instructive: hence the inclusion, in the pages that follow, of short biographical accounts of the great creators of our subject.

The "higher arithmetic" - now an obsolete term for the theory of numbers - is amongst the oldest branches of mathematics: its simple conundrums, handed down to us over the centuries, have proved to possess unsuspected depths. A typical problem runs as follows: Three sailors, shipwrecked on an island, gathered a pile of coconuts that they agreed to share equally between them the following day. But one enterprising blade woke up in the middle of the night and decided to take his third without waiting for the other two: he found that after throwing away one coconut, he could divide the remaining coconuts into three equal parts, which he did. He hid his share, and went back to sleep. Later one of his companion woke up, and had the same idea. He too discovered that after throwing away one coconut, he could divide the number remaining evenly by three. Thus he threw one into the sea, hid away a third for himself, and went back to sleep. Still later, the third seaman, not to be outdone by his companions, went through the same routine. He too threw away one coconut, after noting that the number now left was exactly divisible by three. From this he hid a third, then lay down to sleep again. The next morning the three men were able to divide the remaining coconuts into three equal shares. The question is: What is the least number of coconuts the men should have collected so that such a distribution could have resulted. Problems of this sort, which deal with integer quantities and must necessarily have integer solutions, lead to what are known as Diophantine Equations, after the Greek mathematician Diophantos of Alexandria who first studied them in about 250 AD.

Though Diophantine equations arise frequently in the solutions of puzzles, they have been of immense importance in the development of the theory of numbers: the tenth in David Hilbert's celebrated list of twenty-three unsolved problems, presented, by him at the International Congress of Mathematicians in Paris in 1900 to predict the directions in which mathematics would grow in the twentieth century, is the question: is there a mathematical procedure - or *algorithm* - for deciding whether or not a given Diophantine equation (or a system of such equations) has a solution?

Hilbert's questions had profound consequences: many have been solved, and have made the reputations of their solvers. Several remain unsolved. But the tenth problem was of great importance for the theory of computation: it led mathematicians, logicians and computer scientists

- Turing, Church, Kleene, Godel and Post - to precisely define the term "algorithm"; further, with Turing was born the idea of the algorithmic machine, the Turing machine, which can execute any given algorithm. By his pioneering techniques Turing established the existence of *a class of problems which have no algorithmic solutions whatsoever.* But Hilbert's tenth problem had still to wait for a solution: it was decided only in 1970 by the work of the Russian mathematician Y. Matiasevich, who proved that an algorithm to decide if a given set of Diophantine equations is solvable, is alas impossible.

However, take heart: the problem about the sailors and the coconuts is easy to solve: the answer is 25.

2.1 OBJECTIVES

After working through this Unit you should have learnt:

the use of reduction ad absurdum in mathematical proof

several ways to establish the infinitude of the primes

some theorems relating to prime numbers

some open questions relating to prime numbers

the Sieve of Eratosthenes method to determine prime numbers

Format's method for establishing the primality of a given number

Euler's proof of the infinitude of prime numbers

2.2 PRIME NUMBERS

The concept of primeness is simple to understand, yet it is fundamental to arithmetic. Indeed, all fundamental ideas are simple. We recall that an integer number is said to be prime if it cannot be expressed as the product of two (or more) factors each smaller than itself. Thus 15 = 5 x 3 is composite it is decomposable into prime factors- while 17 is a prime: not both its factors, 17 and 1, are smaller than itself (For a similar reason the number 1 is not considered a prime. But we will shortly see that there is a deeper reason why it is inappropriate to regard 1 as a prime.)

The first few primes are:

$$2, 3, 5, 7, 11, 13, 17, 19, \ldots$$

The distribution of primes seems to follow no law or pattern: indeed, though prime numbers have been the subject of study for thousands of years, it is in general impossible to predict the next prime after a given prime.

A composite number can be expressed as the product of primes in one and only one way, except for order of the factors. Thus:

$$48 = 2 \times 24 = 2 \times 2 \times 12 = 2 \times 2 \times 2 \times 6 = 2 \times 2 \times 2 \times 2 \times 3$$

This statement, called the Fundamental Theorem of Arithmetic, seems "obviously" true because we are so used to factoring numbers from early childhood.: our experience has been that for each integer there is a unique set of factors; but experience is no substitute for proof. The assertion is in fact provable for the integers (a proof was given by Euclid some 300 years before the beginning of the Christian era). but the theorem does not hold for other number systems. Later in this Unit we shall see an example of a system of arithmetic in which prime factorisation does not hold.

1 differs from the other integers that it does not fall within the ambit of the Fundamental Theorem. It can be factored into a product of 1's in more than one way:

$$1 = 1 \times 1 = 1 \times 1 \times 1 = 1 \times 1 \times 1 \times 1, \text{ etc.}$$

Therefore it is conventional to regard it as composite.

Because the integers can be factored into a product of primes in a unique way, prime numbers can he regarded as the fundamental building blocks from which all positive numbers are constructed.

The early Greeks considered the question: is the sequence of primes unending, or is there a largest prime, say P, than which there is none greater? The proof, to be found in the ninth book of Elements is amongst the most beautiful in all of mathematics.

Euclid begins his argument by surrendering the game. Assume, he says, that the sequence of primes is finite. This is quite the opposite of what he wants to prove, the idea being that if the assumption is invalid its consequences must be absurd, which in turn would imply that the assumption itself was false.

Now, asserts Euclid, in any finite collection of different positive integers, there must be some largest number. Thus, in the supposedly finite sequence of primes, let the largest be P.

Next, craftily stalking his game, he invites our attention to the expression:

$$Q = 2 \times 3 \times 5 \times 7 \times 11 \times 13 \times \ldots \times P + 1$$

that is, he asks, consider the number Q formed by multiplying each of the primes up to and including and adding 1 to the result.

Euclid now moves in to the kill. Here, he asserts, is a number that is larger than P, and yet one that is not divisible by any of the primes up to P - for division by any of these numbers leaves a remainder of 1. Q is a prime! But it may be asked: "Granted that Q is not divisible by 2, 3, 5, ..., P, yet couldn't it he divisible by some prime different from all of these? After all, Q is a number vastly bigger than P!" Q may indeed have divisors, Euclid would concede: but they must be different from 2, 3, 5. ..., P.

In other words, they must be greater than P. We have only two logical alternatives: either Q is a prime. larger than P, in which case the assertion stands proved; or, Q is composite, and has prime factors other than 2, 3, 5, ..., P, and therefore greater than P. In any case, there is some prime larger than P, for any prime P; therefore there is no largest prime. Therefore the number of primes is infinite!

Note that Euclid very cleverly skirts the issue of determining the next prime after P: indeed, the distribution of primes is so random that there is no way, except by trial and error, to find it. He merely asserts that there is some prime after any that you can identify as the largest.

The method yields the following primes for P set at 3, 5 and 7:

$$2 \times 3+ 1 =7;$$
$$2 \times 3 \times 5 + 1 =31;$$
$$2 \times 3 \times 5 \times 7+ 1 =211.$$

It skips 5, 11, 13, 17, 19, etc.

Little is known of the life of Euclid, except that he was probably a Greek, that he probably lived in the fourth century before Christ, and was probably the founder of the school of mathematics at Alexandria. He collected and organised in his Elements practically the entire corpus of the mathematical knowledge of his time, in this way becoming, in the words of D. E. Smith, "the most successful textbook writer the world has ever known." This one book (though much altered by the translations and reconstructions of generations of scholars) is even today the source for much of the syllabus of geometry in schools all over the world.

Check Your Progress 1

1. Find the smallest prime P such that Q = 2 x 3 x 5 x ... x P + 1 is a composite number. What are the prime factors of Q? What are the next two such composite Q's? What are their prime factors?

   [Open questions: Are there infinitely many primes P such that Q = 2 x 3 x 5 x ... x P +1 is prime? Are there infinitely many primes P such that Q defined as above is composite?]

2. List 10 primes of the form $k^2 + 1$, where k is an even integer. Can k^2+1 be prime for odd integers k? Can $k^2 - 1$ be prime for any integers k?

3. Verify that there is at least one prime between k^2 and $(k+ 1)^2$ for all integral k satisfying 1 <= k <=20. (This is still a conjecture for all k.)

4. Verify that there is at least one prime between k and 2k for all integral k satisfying 1 < k <= 100. (Bertrand conjectured this result to be true for all k. It was first proved by Tchebychef in 1850.)

5. Verify that every even integer k such that 6 <= k <= 100 can be partitioned as the sum of two odd primes. (Christian Goldbach in a letter to Euler (1742) conjectured that every even number greater than 4 can be decomposed into two odd primes, thus:

   16 = 5 + 11;
   32 = 13 + 19;2 computers have been applied to the inquiry.)

6. In 1752 Goldbach conjectured (again in a letter to Euler) that every odd integer can be written in the form $p + 2a^2$, where p is either 1 or an odd prime, and a > 0. Verify that 5777 is a counter example.

7. de Polignac's conjecture (1848): Every odd integer is the sum of a prime and a power of 2. (For example, $19 = 2^4 + 3$, $39 = 2^5 + 7$, etc.) Verify that 509 is a counter example.

8. Another way to establish the infinitude of the primes is to consider, for some presumed largest prime P, the expression:

$$Q = 1 \times 2 \times 3 \ldots \times P + 1.$$

(The product of all the positive integers up to and including a number P is called the factorial of P, and is abbreviated P!). Now ask: is Q a prime? If it is, we have nothing to prove. If not, can it have factors smaller than P? Hence complete the argument.

9. For a third way to prove the same result, let the presumed finite sequence of primes be p_1, p_2, p_{n-2}, p_{n-1}, p_n, and consider the following sum:

$$S = p_2p_3p_4....p_{n-1}p_n + p_1p_3p_4...p_{n-1}p_n+p_1p_2p_4...p_{n-1}p_n+...+p_1p_2p_3...p_{n-1}$$

where the i^{th} product is formed from all the primes but the i^{th}. Is S divisible by any of the p's?
Conclusion?

10. For yet another way of scaling the peak, consider the sequence:

$$n_1 = 1;$$
$$n_2 = n_1 + 1 = 2;$$
$$n_3 = n_1 \text{ x } n_2 + 1 = 3$$
$$n_4 = n_1 \text{ x } n_2 \text{ x } n_3 + 1 = 7$$
$$n_5 = n_1 \text{ x } n_2 \text{ x } n_3 \text{ x } n_4 + 1 = 43$$
$$n_6 = n_1 \text{ x } n_2 \text{ x } n_3 \text{ x } n_4 \text{ x } n_5 + 1 = 1807$$

From n_2 onwards, no two members of the sequence share the same divisor (why?). Thus n_2 can have no factors in common with n_3, n_4, ..., n_k; n_3 can have no factors in common with n_4, n_5, ..., n_k; n_4 can have no factors in common with n_5, n_6, ..., n_k, etc. Since we can have an infinite number of terms of the type n_k, prove that that the number of primes is infinite.

Example: Find the smallest number such that if its leftmost digit is placed at its right end, the new number so formed is precisely 50% larger than the original number.

Let the n + 1 digits comprising the number - beginning from the left - be d_o, d_1, d_2,...., d_n, where d_0 is different from 0, and d_1, d_2, ..., d_n. are in [0 - 9]. Then the condition of the problem implies:

$$d_1 \, d_2 \, d_3 \text{ ...... } d_n \, d_0 = (3/2) \text{ x } d_0d_1d_2 \text{ .... } d_n$$

By explicitly stating the "weight" of each digit as determined by its position, we rewrite the above condition:

$$2 \text{ x } (d_1 \text{ x } 10^n + d_2 \text{ x } 10^{n-1}+ d_3 \text{ x } 10^{n-2} + ... + d_o =$$
$$3 \text{ x } (d_o \text{ x } 10^n + d_1 \text{ x } 10^{n-1} + d_2 \text{ x } 10^{n-2} +... + d_n)$$

Transposing the terms involving do to the right hand side of the equation, and the other terms to its let hand side, we find:

$$17 \text{ x } (d_1 \text{ x } 10^{n-1}+ d_2 \text{ x } 10^{n-2} +... +d_n)=3 \text{ x } 10^{n-2} \text{ x } d_0$$

From the Fundamental Theorem of Arithmetic it is clear that 17 must be a factor of the right hand side of the above equation. But what is d_0? Well, the problem specifies that we must find the *smallest* number with the required property. Since d_0 is the first digit of the number, and since the smallest number will have the least value of d_0, it is reasonable to set d_0 equal to 1. We must now find the least n such that 3 x 10^{n-2} is divisible by 17. Trying with n at 1, 2, 3, 4, etc. we look for the first number of the sequence 28, 298, 2998, 29998, ... that leaves no remainder on division by 17. That number is 29999999999999998. The quotient obtained on dividing this number by 17 is

176470588235294. Therefore d_l is 1, d_2 is 7, d_3 is 6, ..., d_{15} is 4, and the number we seek (with d_0 = 1 written at the appropriate place) is of 16 digits: 1176470588235294.

Check Your Progress 2

1. By choosing different values for d_0 find other numbers sharing the property of the number found in the last example.

2. A number is formed entirely of 1's. When is it divisible by 7, when by 13, and when by both?

3. is divisible by 7, as well as by 13. So is 1000000001. Show that a number of the form 1000...001 divisible by 7 and by 13 when it has 2 zeros, or 8 zeros, or 14 zeros, or 20 zeros, etc.

4. Find the smallest number n which has the following properties:

   (i) its decimal representation has 6 as the last digit;
   (ii) if the last digit 6 is erased and placed in front of the remaining digits, the resulting number is four times as great as the original number n.

5. A number of 9 digits has the following properties:

   i. The number comprising the leftmost two digits is divisible by 2, that comprising the leftmost three digits is divisible by 3, the leftmost four by 4, the leftmost five by 5, and so on for the nine digits of the number: the number formed from the first n digits is divisible by n, 2 <= n <= 9.
   ii. Each digit in the number is different, i.e. no digits are repeated.
   iii. The digit 0 does not occur in the number, i.e. it is comprised only of the digits 1 - 9 in some order. Find the number.

2.3 GAPS BETWEEN PRIMES

Earlier we remarked that the primes are distributed quite irregularly in the sequence of integers. Consecutive primes may differ by 2 (such prime pairs are called twins, and examples are (17, 19), (179, 181), etc.); or there may be arbitrarily long runs of consecutive composite integers without a single intervening prime. The ancient Greeks were apparently not aware of this result, though it is easy to prove by their methods. To demonstrate a sequence of 1000 consecutive composite integers consider the product 1001!:

P = 1001 x 1000 x 999 x 998 ... x 3 x 2 x 1;

Then, since P is divisible by 2, P + 2 is so divisible; since P is divisible by 3, P+3 is so divisible; similarly P + 4 is divisible by 4, P + 5 by 5, P + 6 by 6., and likewise every integer P + n is divisible by n, where 2 <= n <= 1001. Thus every one of the 1000 consecutive integers from P + 2 through P + 1001 is composite. (However, it is almost certain that there will be several "primeless" runs of 1000 consecutive integers well before 1001!)

Another result easy to establish by methods similar to the foregoing is that there is an infinite number of primes of the form 4n + 3, where n is an integer. First we observe that if a number is divided by 4, the remainder can only be 0, 1, 2 or 3. Numbers which leave remainders of 0 or 2 are even, and therefore composite (with the sole exception of 2, the only even prime); thus primes may be divided into two classes, of types 4n + 1 and 4n + 3. Are there infinite numbers of primes in each class?

We will need the following lemma: If two integers a and b are each of the form 4k + 1, their product is also of the same form.

Proof: Let

$$a = 4i + 1,\ b = 4j + 1;$$

then

$$\begin{aligned} ab &= (4i + 1) \times (4j + 1) \\ &= 16ij + 4i + 4j + 1 \\ &= 4(4ij + i + j) + 1 \\ &= 4k + 1, \text{ where } k = 4ij + i + j \end{aligned}$$

Assume, in the spirit of Euclid, that there is but a finite number of primes of the type 4k + 3. Let the set of these primes be $p_1, p_2, p_3, pn.$

Now consider the product:

$$N = 4p_1p_2p_3...p_{n-1}=4(p_1p_2p_3...p_{n-1})+3$$

If N is prime, we have yet another prime of the form 4k + 3, and we have nothing to prove.

If N is composite, it must have only odd factors, (Why?)

Therefore, its factors can only be of the forms 4k + 1 or 4k + 3.

Since factors of the form 4k + 1 result in a product of the form 4k + 1 (by the lemma above), N, if composite, must have at least one factor of the form 4k + 3.

This factors must be different from p_1, p_2, p_3, ..., p_n else, because N = $4p_1p_2p_3 ... p_{n-1}$, it is indivisible by any of the p's.

Therefore regardless of whether N is prime or composite, there is yet another prime of the form 4k + 3, and so on ad *infinitum*.

Exercise: Use a similar argument to establish that there is an infinite number of primes of the form 3k+ 2.
(Hint: Prove the lemma that the product of two integers of the form 3k + 1 yields an integer of the same form.)

These theorems beg the questions: Are there infinite numbers of primes of the types 4k +1 or 3k+1 ? The answers in each case are in the affirmative, but the proofs of these assertions are extremely difficult and they require methods completely different from the foregoing. In fact, these theorems are but special cases of a powerful theorem of Dirichlet (1837):

If a and b are relatively prime positive integers, then the sequence:

$$a, a + b, a + 2b, a + 3b, ..., a + nb,$$

contains infinitely many primes.

Check Your Progress 3

1. What is the remainder left after dividing 1! + 2! + 3! + ... + 100! by 7?

2. Prove that there are an infinite number of primes of the type 6k + 5. (Hint: The product of any two integers of the form 6k +1 yields an integer of the same form.)

3. Find a prime divisor of the form 4k + 3 for the integer 4 (3 x 7 x 11 x 19) - 1.

4. For any prime p>= 5, prove that p^2 + 2 is composite.
(Hint: Recall that any prime p >= 5 can be take one of the alternative forms 6k + 1 or 6k + 5.)

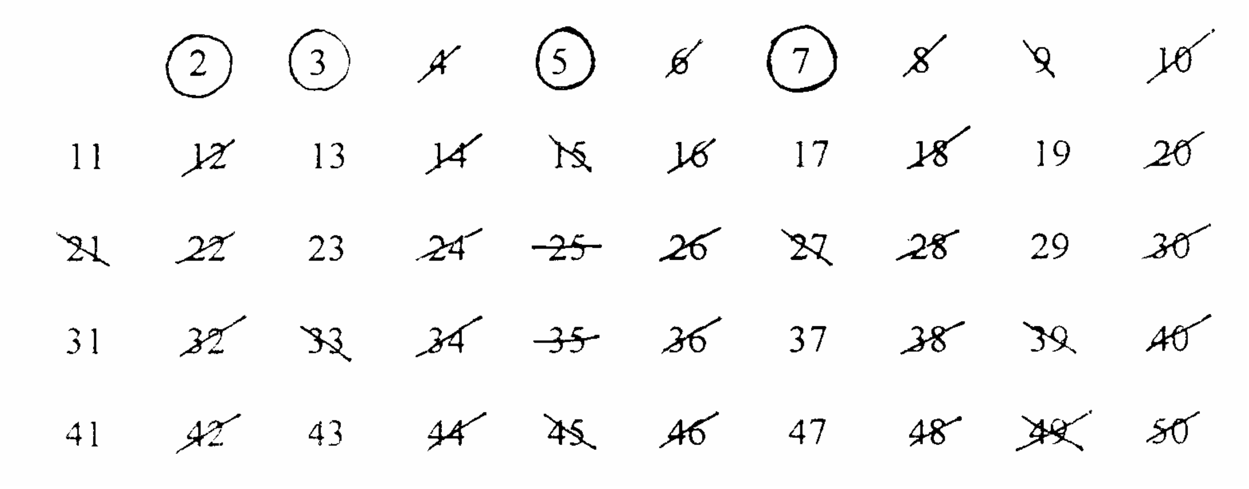
2.4 THE SIEVE OF ERATOSTHENES

Suppose that an odd integer n is given which is to be tested for primeless. In order to do this we must divide it by a succession of prime divisors. Given n, what is the largest divisor that we need try, before concluding that n was prime? The best way to answer the question is to experiment with some given n. Experimentation leads to insight, and insight may lead to proof.

Suppose that we wish to test 1367 for primeness. We divide it by the first odd prime, 3: the quotient is 455, and the remainder is 2. We see that 3 does not divide the given number; but we learn a little more: neither does 455. Nor can there be any divisor larger than 455. (Why?) We next try division by 7 (5 can obviously not be a factor): the quotient is 195, the remainder is 2. So neither 7 nor 195 can be factors of the given number, and the upper limit on a possible divisor is reduced to 195. Division by 11 yields a quotient of 124 and a remainder of 3. That rules out 124 and larger numbers as possible divisors. Continuing in this way with the primes 13, 17, 19, 23, 29 and 31 as divisors, we note that each leaves some remainder; the corresponding quotients are 105, 80, 71, 59, 47, and 44. We note that the quotients decrease as the divisors increase. We need not test 1367 for divisibility by any of these quotients, or by any larger numbers, for each will leave some remainder. By our current reckoning 1367 can have no divisor greater than 44. Finally we test for divisibility by 37. The quotient is 36, the remainder 35. The quotient has now become less than the divisor: we need test no further, for we have already tested by all the primes less than 37. The verdict is clear: 1367 is a prime. We see that it in order to test a number for primeness it is sufficient to use only those prime divisors which yield a quotient greater than or equal to the divisor itself, i.e. divisors which are less than or equal to the square root of the given number.

Eratosthenes (273 - 192 BC, b. Cyrene) used this principle to list all primes less than or equal to a given positive integer n. Suppose that it is required to list all primes up to 50: first, the integers 2 through 50 are written down as in Table 1. Then, beginning with the first prime, 2, (which is saved), all its multiples are struck off from the list. This eliminates the composite numbers 4, 6, 8, ..., 50. Of the remaining integers, the first after 2 is 3. This must be a prime, because it is divisible by no numbers from the list less than itself 3 is saved, but all its multiples that still remain: 9, 15, 21, ..., 45 are crossed off. 2 and 3 are retained, but none of their multiples. The next available prime is 5. It helps remove the composites 25 and 35. Finally the prime 7 is used as divisor: this gets rid of 49.

Further down the list is the prime 11. But 11 exceeds root of fifty no further cancellations are necessary: the remaining integers in the list are all primes.



	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~

Table 1

Eratosthenes was a multifaceted genius: at once a mathematician, poet, philologist, geographer and historian, he was nicknamed Pentathlos (an athlete of five sports). He computed the circumference of the earth by observing that the angular distance of the Sun from the zenith at Alexandria at noon on the summer solstice was about seven degrees. (The summer solstice falls about the 21 st June. The sun is then farthest from the Equator, and seems to stand a little before moving brick.). At Syene, which is believed to have been due south of Alexandria, the Sun was known to be at the zenith at the same time. This led Eratosthenes to infer that the distance between Syene and Alexandria was approximately 1/50 th the earth's circumference, yielding a value within 80 km of the presently accepted figure. Eratosthenes also invented a device to duplicate the cube. He wrote a scientific chronology of Greece, Chronographiae, and a Geography containing historical, mathematical, physical and descriptive data. He was Director of the Library at Alexandria.

Since the largest prime divisor of a given integer n may be as large as 4, it can he a fairly daunting exercise to test a large number for primeness. The first notable advance in this direction was made by Fermat (1601 - 1665, b. Beaumont-de-Lomogne), who wrote a description of the method in a letter (presumably to Father Marin Mersenne) in 1643, some 2000 years after the time of Euclid:

Assume that n is odd. If it has an integer square root x, clearly it is composite. If not, for x >square root of n compute the successive differences $x^2 - n$, $(x + 1)^2 - n$, $(x + 2)^2 - n$, ..., $((n + 1) / 2)^2 - n$. If any but the last of these differences happens to be a perfect square, n is composite. For if $x^2 - n = y^2$ for some y, then $n = x^2 - y^2 = (x - y)(x + y)$. But if x is as large as (n + 1)/2, then $x^2 - n = ((n - 1)/2)^2$, which corresponds to the trivial factorization n = n x 1, establishing that n is prime.

For an example of the method, let's work with the number chosen by Fermat himself to illustrate his idea: 2027651281. A hand calculator verifies that $45029^2 < 2027651281 < 45030^2$. We next compute the differences $x^2 - 2027651281$, for consecutive values of x beginning at 45030, until a difference is found to equal a perfect square, say y^2. As shown in Table 1, this happens when x = 45041; the difference $x^2 - 2027651281$ is 140400, which is the square of 1020. The two factors of the number are (45041 - 1020) and (45041 + 1020), i.e., 44021 and 46061.

$45030^2 - 2027651281 = 49619$	not a perfect square
$45031^2 - 2027651281 = 139680$	" " " "
$45032^2 - 2027651281 = 229743$	" " " "
$45033^2 - 2027651281 = 319808$	" " " "
$45034^2 - 2027651281 = 409875$	" " " "

$45035^2 - 2027651281 = 499944$ " " " "
$45036^2 - 2027651281 = 590015$ " " " "
$45037^2 - 2027651281 = 680088$ " " " "
$45038^2 - 2027651281 = 770163$ " " " "
$45039^2 - 2027651281 = 860240$ " " " "
$45040^2 - 2027651281 = 950319$ " " " "

Finally, $45041^2 - 2027651281 = 1040400$, of which the exact square root is 1020, so that its factors are $(45041 - 1020) \times (45041 + 1020) = 44021 \times 46061$.

Note: When searching the differences $x^2 - n$ for possible squares in Table 1, many values can be excluded by inspection of the final digits. See Exercises 1 and 2 below.

Pierre de Fermat, by profession a lawyer and a magistrate, was amongst the most gifted and perceptive arithmeticians of an age that could boast of such luminaries as Desargues, Descartes, Pascal, Wallis, Leibniz and Newton. Though he had no format mathematical training, and became interested in the subject only when he was past the age of thirty, Fermat loved the theory of numbers as only a hobbyist can. No mathematician of that time made greater discoveries, or contributed more to the subsequent flowering of the "higher arithmetic" in the hands of Euler and Gauss, than this Prince of Amateurs. But if number theory was his first love, and the field of his most remarkable theorems and conjectures, his discoveries in analytic geometry helped lay the foundations for the later development of the Calculus in the hands of Newton and Leibniz. Fermat is also remembered as being, with Blaise Pascal (1623 - 1662), one of the originators of the theory of probability. It was typical of Fermat that he would discover a theorem, state that he had a proof, but would rarely communicate it: for he pursued mathematics not for the advancement of his reputation, but for the deep and abiding love that he felt for it. He corresponded extensively with his contemporaries remember there were no mathematical journals at the time; thus our knowledge of his work derives from his letters to friends, who copied them and passed them from hand to hand.

In a letter dated October 18, 1640 Fermat communicated the following result to Bernhard Frenicle de Bessy (1605 - 1675), also a civil servant who worked for the French Mint, and a keen student of mathematics:

If p is a prime and a is any integer not divisible by p, then p divides $a^{p-1} - 1$.

Fermat wrote, "I would send you the demonstration, if I did not fear its being too long." The world had to wait a hundred years before Euler gave a proof (1736) of this statement, which has come to be known as Fermat's Little Theorem. (The requirement that p not divide a is superfluous.) For an example of the theorem, if p = 3 and a = 4, $a^{p-1} - 1 = 42-1=15$, which is divisible by 3; or if p = 19 and a = 13, then $13^{18} - 1$ is divisible by 19.

Another assertion of Fermat that succumbed to the might of Euler's intellect was the following:

Primes of the form 4k + 1 can be written as the sum of two squares in one and only one way; primes of the form 4k + 3 cannot be thus partitioned.

For example, $41 = 4^2 + 5^2$, $61 = 5^2 + 6^2$; but 47 and 67 are not decomposable into sums of two squares. It was Christian Goldbach who forced Euler's attention to Fermat's assertions. Initially Euler was not drawn to the theory of numbers. But Goldbach's persistence, and the challenge inherent in the stark simplicity of the statements melted whatever resistance Euler may have had Andre Well writes, "... a substantial part of Euler's work consisted in no more, and no less, than getting proofs for Fermats statements."

One of the conjectures of Fermat that Goldbach brought to Euler's notice was the following:

All numbers of the form $2^{2n} + 1$ are primes.

Fermat did not have a proof of this conjecture, and it was one that Euler disproved for n = 5; but numbers of this form have come to be known as Fermat numbers. It was easy to demonstrate that the first few Fermat numbers are indeed primes.

Along with Euclid's Elements one of the most influential books of the Renaissance was the Arithmetica of Diophantos of Alexandria (c. 250 A. D. ?), which was brought to Europe by Byzantine scholars after the fall of Constantinople to the Turks in 1453. But more than a hundred years were to pass before it was translated and printed (1572) by Wilhelm Holzman, who wrote under the pen name of Xylander. Some fifty years afterwards Claude Bachet published the original Greek text, together with a Latin translation and a commentary. In all probability it was the Bachet edition that drew Fermat's attention to the problems of number theory. It is believed that the Arithmetic consisted of 13 books, though none of the Greek manuscripts contains more than six. Diophantos considered a great variety of problems, leading to types of indeterminate equation known as Diophantine Equations. These equations are called indeterminate because they contain more unknowns than equations. The Diophantine problem is that of finding integer solutions to such equations. The Arithmetica also contains several propositions of number theory: for example, a number of the form $8n + 7$ cannot be the sum of three squares, and a number of the form $2n + 1$ can be the sum of two squares only if n is odd.

Fermat had the habit of writing marginal notes and comments in his copy of Bachet. Typically, he would state a result, omitting the steps that had led him to it, leaving to posterity to provide the verifications. In almost all cases his words have been vindicated, for Fermat was most circumspect in his statements: he would not claim he had a proof for a conjecture, unless he was sure he had one. The most famous of his marginalia a remark has inspired more research in mathematics than any other is the following:

"It is impossible to write a cube as a sum of two cubes, a fourth power (quadratoquadratum) as a sum of two fourth powers, and, in general, any power beyond the second as a sum of two similar powers. For this, I have discovered a truly wonderful proof, but this margin is too small to contain it."

Generations of mathematicians have been tantalized by this remark, in which Fermat simply states that the Diophantine equation:

$$x^n + y^n = z^n$$

has no solution for integral x, y, and z, when n > 2.

Solutions for the case n = 1 are trivial; solutions when n = 2 are called *Pythagorean triplets:* for they represent integer sides of right triangles, in which, as Pythagorean proved, the sum of the squares on the sides including the right angle equal the square on the hypotenuse. (Examples of Pythagorean triplets are (5, 12, 13) and (12, 35, 37), (19, 180, 181); there are infinitely many of them)

Fermat's statement is commonly called his Last Theorem. If Fermat had indeed a truly wonderful proof of it, it is still to be discovered.

Meanwhile, an immensely complex proof of Fermat's Last Theorem (FLT) has apparently been found (1993) by Andrew Wiles,. thus laying to rest a conjecture that had dogged mathematicians for more than 350 years.

Before Wiles' proof was available, the foremost mathematicians of the world had struggled to prove FLT, but their efforts produced only incomplete results and proofs for individual cases. (Fermat had himself given a separate proof for the case *n = 4.*) Enter gave the first proof for n = 3

(1770); but some gaps remained in his proof, which were filled in by Legendre. Around 1825 Dirichlet and Legendre independently settled the case for n = 5, and in 1839 Lame gave a proof for 7th powers.

As the arguments for the individual cases increased in complexity, there came the realisation that a successful resolution, of the general case would require entirely different techniques. One idea was to extend the meaning of "integer" to include a wider class of numbers, and to attack the problem within this enlarged system. The German mathematician Kummer made the major breakthrough. In 1843 he sent a what he thought was a proof to Dirichlet.

The idea was to extend the integers to include the algebraic numbers - these are solutions of polynomial equations with rational coefficients: thus, one solution of the following polynomial equation with rational coefficients of the fourth degree:

$$x^4 + x^3 - 22x^2 - 72x - 48 = 0$$
is $2 + 6^{1/2}$

But there was a major flaw in Kummer's proof, that Dirichlet was able to discover immediately: *Kummer had assumed that algebraic numbers admit of a unique factorisation,* like the integers, though this is not invariably true. (For example, $6 = 2 \times 3 = (5\ 6^{1/2} + 12) \times (5\ 6^{1/2} - 12)$.)

But Kummer was undeterred by this defeat. Building on his failure, he went on to create the theory of *ideals*, using which he was able to show that the Fermat conjecture held good for a large class of primes which he called *regular primes*. This was a magnificent achievement. Its magnitude can be appreciated if you stop to consider that *the only irregular primes less than 100 are 37, 59 and 67*. Unfortunately, it is provable that there exist infinitely many irregular primes! So the proof for FLT had to wait another 150 years!

Check Your Progress 4

1. There are some interesting results regarding Pythagorean triples which are easy to prove..
2. One member of a Pythagorean triple, wherein each member is expressed in its lowest terms, is necessarily a multiple of 3.
3. The radius of the inscribed circle of a right triangle with Pythagorean triples for its sides is always an integer.
4. It is possible for different Pythagorean triangles to have the same area: for instance the triangles (20, 21, 29) and (12, 35, 57) have the same area. Fermat proved: for any integer n > 1, there exist n Pythagorean triangles with different hypotenuses and the same area.

2.5 EULER'S PROOF OF THE INFINITUDE OF THE PRIMES

Euler gave a deeply insightful proof of the infinitude of the primes, which first brought to light the connection between the theory of numbers and real analysis. Euler's discoveries in mathematics are so numerous and so remarkable - there is scarcely a branch of the subject where he did not leave his imprint - that a few words about him are in order. Look where you will, there's an Euler's Theorem, or an Euler's Formula, an Euler's Equation or an Euler's solution to a problem then current. He was an indefatigable worker: 473 memoirs were published in his lifetime, 200 shortly after his death in 1783, while 61 had to wait. All this work was done under a severe handicap, for he had lost the sight of one eye when he was 29 years old, and became totally blind some 30 years later. His skill in manipulation was enormous, (equalled by none since his time, except possibly Srinivasa Ramanujan) and his intuitive grasp of mathematics was not less remarkable.

Leonard Euler was born in Basel, Switzerland, in 1707. At the age of 20 years he was invited to the St. Petersburg Academy in Russia, which he left in 1741 to take the Chair at the Prussian Academy in Berlin. He returned to St. Petersburg in 1766, remaining there until his death.

We first prove two Lemmas.

Lemma 1:

For any positive x < 1, the series:

$$1 + x + x^2 + x^3 + \ldots + x^n$$

converges to *1/(1-x)* as n tends to infinity.

Proof:

Let

$$S = 1 + x + x^2 + \ldots.. + x^n$$

Then

$$xS = x + x^2 + x^3 + \ldots..\ x^{n+1}$$

Therefore

$$S(1-x) = 1 -x^{n+1}$$

and

$$S=1 / (1-x) -x^{n+1} / (1-x)$$

where clearly the second term tends to zero with n.

In particular, for any prime *p*. since *1/p< 1*

$$1 + 1/P + 1/P^2 + 1/P^3 + \ldots. = 1/(1 - 1/p)$$

Lemma 2:

The sum:

$$1 + 1/2 + 1/3 + 1/4 + \ldots\ldots...\ l/n$$

tends to infinity with n. (This series of terms is called the harmonic series.)

Proof:

With four terms we find:

$$1 + 1/2 + 1/3 + 1/4 > 1 + 1/2 + 1/4 + 1/4 = 2,$$

while with eight terms:

$$1 + 1/2 + 1/3 + 1/4 + 1/5 + 1/6 + 1/7 + 1/8 > 2 + 1/8 + 1/8 + 1/8 + 1/8 = 5/2.$$

With sixteen terms:

$$1 + 1/2 + 1/3 +..+ 1/16 > 5/2 + 1/16 +.. 1/16 = 5/2 + 1/2 = 3.$$

Thus, with a sufficiently large number of terms, the series can be made to exceed any preassigned number, however large. In other words. the sum of the series approaches infinity, as the number of terms in it becomes infinite.

Euler's Proof :

Suppose that the number of primes is finite, say N. Let these primes be $p_1, p_2, p_3, ... p_N$.

Then the product :

$$1/(1- 1/p_1) x 1/(1-1/p_2) ... 1/(1-1/p_n)$$

must. also be finite. By Lemma 1, this product can be written:

$$(1 + 1/p_1 +1/(p_1)^2 + ...+1/(p_1)^n +...) (1 + 1/p_2 + 1/(p_2)^2 +....+1/(p_2)^n +..)..(1 + 1/p_N + 1/(p_N)^2 +..)$$

If each of the parenthetical expressions is multiplied, the set of terms obtained will be of the form

$$1/(p_1)^{i} (p_2)^{j}..(p_N)^{r}$$

where the i, j, r, are integers.

Each term in the expansion will be. different from every other term, because different values of i, j, r will occur in each denominator. A little thought will convince you that this expansion must be identical with the harmonic series:

$$1 + 1/2 + 1/3 + 1/4 + 1/5 +...$$

(Every integer, prime or composite, must occur once, and once only, in the product of the parenthetical expressions above.)

By Lemma 2 the harmonic series has an infinite sum. Therefore the number of primes cannot be finite.

Check Your Progress 5

1. Prove that the last digit of the square of any number can only be one of the following: 0, 1, 4, 5, 6, 9.
2. Prove that the last two digits of the square of any number can only be one of the 22 listed below:

00	01	04	09	16	21	24	25	29	36	41
44	49	56	61	64	69	76	81	84	89	96

Use this information to realise that the only likely candidates for perfect squares in Fermat's example are the differences 499944 and 1040400.

3. Prove that 12, 078, 521, 834 is not a square, while 1, 354, 896 is a square.

4. Find the first number after 1 which is simultaneously a 1st power, a 2nd power, a 3rd power, a 4th power, a 5th Power, a 6th power, a 7th power, an 8th power, a 9th power and a 10th power.

5. The digital root of a number is the sum of its digits; if this sum is expressed in more than one digit, add up its digits; in this way, reduce the sum of digits of the given number to a single digit. If the number started with was a perfect square, its digital root will be 1, 4, 7 or 9; if the digital root is 2, 3, 5, 6 or 8, the number could not have been a square; conversely, a digital root of 1, 4, 7 or 9 does not necessarily imply that the given number was a square. Similarly, a number cannot be a cube if its digital root is 2, 3, 4, 5, 6 or 7.

2.6 SUMMARY

Arithmetical conundrums are the earliest types of problem or puzzle known to our civilization. Because the concept of number is so fundamental to civilisation, riddles involving numbers are easy to convey to others; yet they may be enormously complicated to solve. Such an example is that of Fermat's Last Theorem, which was finally proved a only a couple of years ago, and of Goldbach's conjecture, which has withstood numberless onslaughts upon it by some of the world's best mathematical minds since it was stated some 250 years ago.

In this Unit you have seen how Euclid applied the very useful technique of reduction ad absurdum to proving the infinitude of the primes. Several different, but essentially ""Euclidean" ways of proving the same result, were also introduced. Twenty five centuries later Euler scaled that peak by a quite different route - by proving that the divergence of the harmonic series implies that the number of primes is infinite,