Miscellaneous

7/3/59.

Notes from Rademacher's & Toeplitz's book "Enjoyment of Mathematics"

relating to Chapters on the theory of numbers"

(2) I - Enjoyment of Mathematics by Rademacher & Toeplitz - Chapters on the theory of numbers.

Chap. 1 - The sequence of prime numbers - (a) Euclid's proof of the infinitude of primes by considering

$N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdots p + 1$, where p is any prime. N is either prime or composite. In the first case the theorem is proved since $N > p$. In the second case, all the prime factors of N are different from $2, 3, 5, \cdots p$ since N is not divisible by any of these, and hence all prime factors of N are greater than p, thus also proving the theorem. A particular example of this given by $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30301 = 59 \times 509$. Euclid's proof looks for some prime beyond p & not the next prime & thus does not try to do more than what is required.

(b) Existence of large gaps in the series of primes - It is shown that one can find 1000 consecutive composite numbers. The first four digit prime $p = 1009$. Form the 1000 numbers

$$2 \cdot 3 \cdot 5 \cdot 7 \cdots p + 2, \quad 2 \cdot 3 \cdots p + 3, \quad \cdots, \quad 2 \cdot 3 \cdots p + 1001$$

Each of the numbers $2, 3, 4, 5, 6, \cdots 1001$ is divisible by one of the primes $2, 3, \cdots p$ [perhaps it would be more correct to say "one of the primes in the series $2, 3, \cdots p$". In fact $p = 1009$ itself would not be necessary. At worst the prime next below $p = 1009$ viz 997 is used as for eg. in $2 \cdot 3 \cdot 5 \cdots 997 \cdot 1009 + 997$], and so is $2 \cdot 3 \cdots p$, and hence each of the numbers listed is not a prime. [The list could have been extended to give 8 more consecutive composite nos. viz $(2 \cdot 3 \cdots p) + 1002$, $(2 \cdot 3 \cdots p) + 1003$, $\cdots$ $(2 \cdot 3 \cdots p) + 1008$, and $(2 \cdot 3 \cdots p) + 1009$ ie 1008 consecutive composite numbers ie $(p-1)$ - what about 10 consecutive composite numbers? The method suggested gives $p = 11$, and hence gives the sequence

This gives only 999 consecutive non-primes

$$(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11) + 2, \quad \cdots, \quad (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11) + 11$$

ie $2312, 2313, \cdots, 2321$ - But is there no other such sequence with smaller numbers? By a mental calculation, I found that the first such sequence is given by $114, 115, 116, \cdots, 123$, and this was quite easy. But suppose I want to raise a similar question in the case 100 consecutive composite numbers. Here $p = 101$ & the method in the book gives the sequence of 100 composite nos (not more than 100 unlike the case of $p = 1009$ where we had 1008 consecutive ones) viz

There is a sequence of 19 consecutive composite numbers viz 888,889, ... 906

Bsm 9/5/75

$$(2 \cdot 3 \cdots 101) + 2, \quad \cdots, \quad (2 \cdot 3 \cdots 101) + 101$$

But to find by successive calculations such a sequence of 100 numbers smaller than the above sequence (as we did for the case 10) would be a colossal job. Anyway we have raised a problem viz. No. 1 - to find the first sequence of 10, 100, 1000, (Call it even) consecutive composite numbers or in general of n. I am reminded here of having read somewhere that any fool can raise a problem in the theory of numbers, but the greatest genius may not be able to show whether this is true or false! - Well, what about 10000 consecutive ones?

we have to find out p ie the first five digit prime, but there does not appear to be any general rule for this. we have to consider numbers 10001, 10003, .. and test divisibility by all primes from 2 to 97 (since $\sqrt{10000} = 100$); 10001 is divisible by 73; 10003 is divisible by 7 (like a fool I started divisibility from 97 downwards as in case of 10001 instead of from 3 upwards & this took 10 minutes); 10007 is prime (going from 3 upwards). To arrive at this I took nearly half an hour. Thus we can write a sequence of 10006 consecutive composite numbers viz

$(2\cdot 3 \cdots 10007) + 2$, ... $(2\cdot 3 \cdots 10007) + 10007$.

– Next, let us try a sequence of a million consecutive primes. This leads to finding the first seven digit prime, and for this we have test divisibility of 1000001, etc by all primes less than 1000 ($\sqrt{\text{million}} = 1000$) ie by 2, 3, - -, 997 which is a far bigger job than the previous one of five digit prime. It appears pointless to attempt this; anyway I have raised another Problem No. 2 viz. to find the first n^{th} digit prime & this will solve the problem of finding a sequence of $10^{(n-1)}$ or more consecutive composite numbers. Thus we have

Problem 1: To find the first sequence of 10^m, or in general of n, consecutive composite numbers.

Problem 2: To find the first n^{th} digit prime number

Problems of type (b) were not considered by the Greeks, but are results of modern investigations. These are related problems relating to gaps which are still unsolved and some are solved with great difficulty & some have led to new fields of mathematics.

(c) Existence of infinitude of primes in particular sequences of integers — Here are considered the two sequences of integers which respectively leave remainders 2 and 1 when divided by 3 (the case of remainder 0 giving 3, 6, 9, 12, .. a sequence of composite numbers) viz. 2, 5, 8, 11, 14, 17, 20, 23, 26, . . . $a(3x+2)$ $(x = 0, 1, 2, \ldots)$

and 1, 4, 7, 10, 13, 16, 19, 22, ... $a(3x+1)$ $(x = 0, 1, 2, \ldots)$

To prove that the first sequence has an infinitude of primes, two Corollaries are proved viz:

(i) The product of any two numbers in the second sequence belongs to the second sequence,

for, $(3x+1)(3y+1) = 3(3xy + x + y) + 1$

(ii) if any of the numbers in the first sequence is split up into its prime factors, at least one of the prime factors must belong to the first sequence,

for, all numbers (and hence any prime factor) are of either of the three forms $3x$, $3x+1$, $3x+2$. The first case does not give a prime factor except when $x = 1$ but then 3 is not in the first sequence. Next all the prime factors cannot be of type $3x+1$ since from (i) the number itself would be in the second sequence. Hence at least one of the prime factors must be of type $3x+2$ ie in the first sequence.

Now consider $M = (2\cdot 3\cdot 5\cdot 7\cdot 11 \cdots p) - 1$, where p is any prime in the

first sequence. ~~if we assume it had only a finite number of primes~~. M is of the form $3y-1$ which is equivalent to $3x+2$ (if ~~$x=y+1$~~ $x = y-1$) and hence belongs to the first sequence. It is either prime or composite. In the first case since $M > p$, the theorem is proved. In the second case, just as in (a), all the prime factors of M are greater than p, and from (ii) at least one prime factor belongs to the ~~second~~ first sequence, ie there is at least one prime factor of M belonging to the first sequence which is greater than p & this proves the theorem.

It is stated that it requires quite different methods to prove that the second sequence viz 1, 4, 7, 10, 13, .. also has an infinitude of primes.

In the notes & remarks at the end of the book, it is stated that the proofs concerning gaps is due to Kronecker, 1901 – Also that existence of infinitude of primes in some other sequences for eg $(4x+1)$, or $(4x-1)$ $(3, 7, \ldots)$ can be proved by elementary means – In general the theorem holds for sequences in A.P. if the first term is relatively prime to the common difference. This was proved by Dirichlet (1837) by means of higher mathematics in a famous and difficult paper.

Chapter 9 — On Waring's problem.

(a) Fermat proved that every positive integer can be expressed as a sum of at most four squares – Waring conjectured that a similar theorem could be proved for cubes, fourth powers and so on & raised the question as to how many cubes, fourth powers, etc. would at most be required. This set of problems is called Waring's problem – (b) For cubes, Jacobi's empirical tests of numbers up to 12000 showed that 23 and 239 required 9 cubes, some 8 and some 7 – Landau first proved by ~~suffe~~ difficult mathematical methods that from some point on 8 cubes suffice, and later Wieferich proved that from some point on 7 cubes suffice (c) For fourth powers the number ~~suggested~~ 19 suggested by $79 = 4 \times 2^4 + 15 \times 1^4$ was expected to suffice & much work done on the problem – Liouville showed that 53 would suffice and this was brought down to 47, 45, 41, 39, 38 and finally to 37 by Wieferich, but all these were far from the much hoped-for 19 – Hilbert considered in a general way the whole set of problems connected with cubes, 4^{th}-powers, 5^{th}-power etc, and was able to prove at one stroke that not only for cubes & 4^{th} powers but also for higher powers, there is a number that will suffice (like the 9 for cubes & 37 for fourth powers – Hardy & Littlewood used still different & highly complicated methods to prove that all numbers from a certain point on are sums of 19 fourth powers, and this shows the power of their method & this is just one of their far-reaching results. But the number N beyond which ~~they showed~~ all numbers, they showed, are sums of at most 19 fourth powers, is ~~so enormous~~ tremendously large & they did not bother to compute its value. In a sense their result practically settles the case of 4^{th} powers, for one need only test all numbers less than N and test whether or not 19 fourth powers will suffice for every number, but N is so tremendous that such a testing would be far beyond the ability of any computer. (d) Some idea of the methods used, specially those of Hilbert are next given –

The identity $(a^2+b^2)(c^2+d^2) \equiv (ac+bd)^2 + (ad-bc)^2$ - - - (1)

shows that if each of two numbers is a sum of two squares, then their product is also a sum of two squares.

Euler's identity

$$(a_1^2+a_2^2+a_3^2+a_4^2)(b_1^2+b_2^2+b_3^2+b_4^2) \equiv (-a_1b_1+a_2b_2+a_3b_3+a_4b_4)^2 + (a_1b_2+a_2b_1+a_3b_4-a_4b_3)^2$$
$$+ (a_1b_3+a_3b_1-a_2b_4+a_4b_2)^2 + (a_1b_4+a_4b_1+a_2b_3-a_3b_2)^2 \quad --(2)$$

shows that if each of two numbers is a sum of four squares, so is their product. (i) Liouville's proof about sufficiency of 53 fourth powers using Fermat's theorem :-

In this proof Liouville uses the identity

$$6(x_1^2+x_2^2+x_3^2+x_4^2)^2 \equiv (x_1+x_2)^4 + (x_1+x_3)^4 + (x_2+x_3)^4 + (x_1+x_4)^4 + (x_2+x_4)^4 + (x_3+x_4)^4$$
$$+ (x_1-x_2)^4 + (x_2-x_3)^4 + (x_2-x_3)^4 + (x_1-x_4)^4 + (x_2-x_4)^4 + (x_3-x_4)^4$$
$$- - \quad --- \quad (3)$$

If n be any number, it can be written as $n = 6x+y$, where $y = 0$ or 1 or 2 or 3 or 4 or 5. Using Fermat's theorem let $x = a^2+b^2+c^2+d^2$, then $n = 6a^2+6b^2+6c^2+6d^2+y$. Again using Fermat's theorem for a, b, c, d, let $a = a_1^2+a_2^2+a_3^2+a_4^2$, $b = b_1^2+\cdot$, $c = c_1^2+-$, $d = d_1^2+\cdots$; hence

$$n = 6(a_1^2+a_2^2+a_3^2+a_4^2)^2 + \cdots + \cdots + \cdots + \cdots + y$$

We now using (3) each of the first four terms is a sum of 12 fourth powers, and the first four terms give 48 fourth powers. Since y is one of 0, 1, 2, 3, 4, 5 it can be expressed as a sum of at most 5 fourth powers, each of which is 1. This gives a total of at most $48+5 = 53$ fourth powers.

(ii) Lagrange's proof of Fermat's theorem by proving the theorem (called Lagrange's theorem) that every integer $n \geq 0$ can be written as the sum of four squares :-

Steps of the proof Th(1) If A and B be each written as the sum of four squares, then so can the product AB. This is an immediate consequence of identity (2). It allows one to concentrate on prime numbers only.

Th(2) If p be a prime >2, then it is possible to find an integer m such that $1 \leq m < p$, and such that $mp = x_1^2+x_2^2+x_3^2+x_4^2$ — Proof not too simple

Th(3) If p be a prime >2, and m is the smallest positive integer such that $mp =$ sum of four squares, then $m = 1$ — Proof more complicated than that of Th(2).

Th.(4) If p be any prime number, it can be written as a sum of four squares — for $p>2$, this is Th.(3) & for $p=2$, $2 = 1^2+1^2+0^2+0^2$.

Th(5) - Lagrange's theorem - Every integer $n \geq 0$ can be written as a sum of four squares.

for $n=0$, $0 = 0^2+0^2+0^2+0^2$

$n=1$, $1 = 1^2+0^2+0^2+0^2$

So we need consider $n>2$, and consider composite numbers say $n = p_1p_2p_3\cdots p_t$. From Th.(4) both p_1 & p_2 can be expressed as sum of four squares & hence from Th(1), so can p_1p_2. Again from Th(4) p_3 can be so expressed & from Th.(1) again $p_1p_2p_3$ can be so expressed & continuing in this manner Lagrange's theorem is proved.

In the Notes & Remarks at the end, Waring's conjecture is interpreted to mean that any integer n can be represented as a sum of

$$I = 2^K + q - 2$$

k^{th}-powers, where q is the greatest integer not surpassing $(3/2)^K$ [for $K=2$, $q=2$, & $I=2$; $K=3$, $q=3$, & $I=9$; $K=4$, $q=5$, & $I=19$; $K=5$, $q=7$, & $I=37$]

for the number $n = 2^K q - 1$, I K^{th} powers are indeed needed since n would be $< 3^K$ & only summands 1^K & 2^K can be used

[Thus for $K=3$, $n = 23 = 2^3+2^3+1^3+1^3+1^3+1^3+1^3+1^3+1^3$ i.e. $I=9$ & for $K=4$, $n=79$ = sum of 19 fourth powers i.e. $I=19$]

Dickson & Pillai proved in 1936 that for $K \geq 6$, I indeed suffices for all n if (with Niven's later improvement)

$$\left(\frac{3}{2}\right)^K - q < 1 - \frac{q}{2^K} \quad \ldots (4)$$

This condition holds for $2 \leq K \leq 400$ & it is not known whether it is true for all K. However for those K for which it might not be valid, the number $g(K)$ of required K^{th} powers has also been determined viz. for the cases $K = 2,3,4,5$ (since Dickson & Pillai's theorem is valid for $K \geq 6$). For $K=2,3$, $I = 4,9$ resply also hold good. For $K=4,5$ we know at present only $19 \leq g(4) \leq 35$, and $37 \leq g(5) \leq 54$. [Thus Waring's conjecture has been proved by Dickson & Pillai for $6 \leq k \leq 400$, and ~~not~~ for $K=2,3$ but not for $K=4,5$ or $K>400$]. The work of Dickson & Pillai rests throughout on the results which Vinogradoff obtained with his functional-theoretic methods that he developed from the methods of Hardy & Littlewood.

[The methods used by Hilbert are supposed to be illustrated in this chapter, but no explicit mention of Hilbert's work is made in the explanation of the ideas].

Chapter II — Is the factorisation of a number into prime factors unique?

It is shown that this problem is not trivial by considering the system of complex numbers $a+ib\sqrt{6}$ & showing that unique factorisation does not hold in this system by setting up the example, $6 = 2 \cdot 3 = -(i\sqrt{6})(i\sqrt{6})$. The actual proof of uniqueness is done in a number of steps by a series of lemmas:-

Lemma 1: Every common multiple of two numbers is a multiple of their least common multiple.

Lemma 2: The quotient of the product of two numbers a and b divided by their L.C.M i.e. the number, $d = ab/m$ is always a common divisor of a & b.

Theorem: If a prime p divides the product xy of two numbers x and y, then p divides x or y.

Cor: If a prime divides a product of several numbers, then it divides at least one of the factors.

The unique factorisation theorem then follows immediately from the corollary by showing that if $N = pqrs\ldots = PQRS\ldots$, then (i) the two factorisations contain exactly the same primes, & (ii) each prime appears on both sides the same number of times.

Proofs of (i) & (ii) are very elegant. To prove (i) we note that since p divides $PQRS\ldots$, it follows

from the corollary that p divides one of $P, Q, R, S, \ldots$, but from the defn of a prime, when one prime divides another prime, the two must be equal. Hence p must occur on the R.H.S; similarly $q, r, s, \ldots$ on the left must also appear on the right. In other words the two factorisations contain exactly the same primes. To prove (ii), let if possible p appear a times on the right and A times on the right ie let $N = p^a q^b r^c \ldots = p^A q^B r^C \ldots$

Let $A > a$, then dividing by p^a, we have $M = \frac{N}{p^a} = q^b r^c \ldots = p^{A-a} q^B r^C \ldots$. Now M, like N, must contain because of (i) the same primes on both the sides, but here there is no p on the left, but there is p on the right. Hence $A = a$ in which case p will not be on the right also. In the same way $b = B$, $C = C$, etc.

In the Notes & Remarks at the end, a simple proof using mathematical induction found independently in the 20th century by Zermelo, Hassé & Lord Cherwell is given. This proof is also elegant and is as follows:- If there be a number with two different prime factorisations, there must exist a smallest among them (since the first few integers certainly have a unique prime factorisation) say N ie

$$N = p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_\ell \qquad (p\text{'s } \& \ q\text{'s being primes})$$

say with $p_1 \leq p_2 \leq \ldots \leq p_k$ and $q_1 \leq q_2 \leq \ldots \leq q_\ell$

Also no $p_i = q_j$, otherwise $\frac{N}{p_i}$ would be $< N$ and still have two different prime factorisations, contradicting that N is the smallest. Without loss of generality we can assume $p_1 < q_1$ (for if it were otherwise we need only interchange labels p & q, & k & ℓ). Now consider

$$M = p_1 \cdot q_2 \ldots q_\ell < N,$$

and further $N^* = N - M$. Since both M and N are divisible by p_1 so is N^* & thus it possesses a prime factorisation including p_1 (any number can be reduced to a prime factorisation).

But $N^* = M - N = p_1 q_2 \ldots q_\ell - q_1 q_2 \ldots q_\ell = (q_1 - p_1) q_2 \ldots q_\ell$ & in this $(q_1 - p_1)$ is not divisible by p_1 and also $q_2 \ldots q_\ell$ are all different from p_1. Thus N^* has also a prime factorisation not containing p_1 [Even if $(q_1 - p_1)$ were composite, it could be factorised] ie N^* has two different prime factorisations, but from the defn of N^*, $N^* < N$ & this is against the hypothesis that N is the smallest. This contradiction disproves existence of numbers possessing two different prime factorisations.

Chapter 14 — Pythagorean numbers and Fermat's theorem

(a) ~~Solution of the~~ Pythagorean problem of finding relatively prime integral solutions of $a^2+b^2=c^2$ is completely solved, by taking a & c odd & b even, ~~and~~ the solution being

$$a = u^2 - v^2, \quad b = 2uv, \quad c = u^2 + v^2$$

where u & v are relatively prime and of opposite parity, and $u > v$ (to ensure that a is +ve).

(b) Fermat's Last theorem is that $x^n + y^n = z^n$ has no solution in positive integers x, y, z when $n > 2$. This has so far never been proved or disproved. Euler (1707-1783) proved it for $n = 3$ and $n = 4$. Later Kummer (1810-1893) & his followers proved it for all n from 3 to 100.

(c) Proof is given for the case $n = 4$, by using (a). This is done by showing that even the equation

$$x^4 + y^4 = w^2 \quad \ldots (1)$$

has no solution in positive integers (~~or only~~ we need then only set $w = z^2$). Positive integers are considered to eliminate certain trivial solns like $x = 1, y = 0, w = 1$, and $x = -y, z = 0$ for the case $n = 3$. Using (a) soln of (1) (if it exists) is given by

$$x^2 = u^2 - v^2, \quad y^2 = 2uv, \quad w = u^2 + v^2 \quad \ldots (2, a, b, c)$$

(2,a) gives $x^2 + v^2 = u^2$ leading to the solution

$$x = u_1^2 - v_1^2, \quad v = 2u_1v_1, \quad u = u_1^2 + v_1^2$$

Since u is odd, v even and the two relatively prime, u and $2v$ are relatively prime. Thus (2,b) expresses y^2 as a product of two relatively prime factors u & $2v$ & hence u and $2v$ themselves must be squares ie

$$u = w_1^2, \quad 2v = 4t_1^2$$

inserting these in ~~$u = u_1^2 + v_1^2$, and~~ $v = 2u_1v_1$ and $u = u_1^2 + v_1^2$, we have

$$t_1^2 = u_1v_1 \; ; \; w_1^2 = u_1^2 + v_1^2$$

Now u_1 & v_1 are relatively prime & their product is t_1^2 ie a square. Hence u_1 & v_1 are themselves squares say $u_1 = x_1^2$, $v = y_1^2$ so that we have

$$x_1^4 + y_1^4 = w_1^2 \quad \ldots (1')$$

(1') is of the same form as (1), and from (2,c) & using $u = w_1^2$, we have $w = u^2 + v^2 = w_1^4 + v^2 > w_1^4$ ie $w > w_1$. Thus, from a (reduced) solution (x, y, w) of (1) we go to another (reduced) solution (x_1, y_1, w_1) with $w > w_1$. Similarly from (x_1, y_1, w_1) we can go to another (x_2, y_2, w_2) with $w_1 > w_2$. Continuing in this way we obtain a series of solns with

$$w > w_1 > w_2 > \ldots$$

Since all the w's are +ve integers, the above sequence must end say with w_K. But this leads to a contradiction for $w_K \to w_{K+1}$ by above process. Hence (1) has no soln in +ve integers since such an assumption leads to a contradiction. The basic idea of this proof was called the "principle of infinite descent" by Fermat (never-ending ~~set of descents~~ series sequence of decreasing +ve integers which is a contradiction)

(d) Notes & Remarks – Leaving aside the case $n = 4$, it suffices to prove the impossibility of $x^n + y^n = z^n$ in integers for prime numbers, $n = p$ only (?) – In the literature two cases are distinguished viz.

(i) $x \cdot y \cdot z$ is not divisible by p, (ii) one (and only one) of the numbers x, y, z is divisible by p. In Case (i) Fermat's conjecture has been proved for all prime numbers $p < 253,747,889$ by D. H. Lehmer, Emma Lehmer and Rosser. In case (ii) deeper theorems of number theory are to be used, and here Fermat's conjecture has been verified for all $p \leqq 4001$, with the use of the SWAC, an electronic digital computing machine at Los Angeles by D. H & Emma Lehmer and Vandiver – Terrible indeed,

Chapter 19 – Perfect numbers.

Euler defined a perfect number as one that is equal to the sum of all its divisors (enclosing the no. itself) – for eg. 6 is one such viz $6 = 1+2+3$, & the next one is $28 = 1+2+4+7+14$ – The theory of perfect numbers is only a minor topic, but the methods used in it by Euler specially have found a prominent place in the most important modern theory of the distribution of prime numbers.

(1) A prime number cannot be perfect. (2) No power of a prime can be a perfect number, for considering p^α, $1 + p + p^2 + \cdots + p^{\alpha-1} = \frac{p^\alpha - 1}{p-1} \neq p^\alpha - 1$ since $p \geqq 2$ is sum of divisors $\leqq p^\alpha - 1 < p^\alpha$ and hence p^α is not perfect. (3) For any number $N = p^a q^b r^c \cdots$, the sum of divisors D is given by $D = (1 + p + p^2 + \cdots + p^a)(1 + q + q^2 + \cdots + q^b)(\cdots)\cdots$

$$= \frac{p^{a+1} - 1}{p-1} \cdot \frac{q^{b+1} - 1}{q-1} \cdot \frac{r^{c+1} - 1}{r-1} \cdots \quad \text{---} \quad \cdots (1)$$

where, however, the number N is also included

(4) If $N = p \cdot 2^b$, we have $D = \frac{2^{b+1} - 1}{2-1} \cdot \frac{p^2 - 1}{p-1}$, and if N be a perfect number, $D = 2N$

and hence $2p \cdot 2^b = (2^{b+1} - 1)(p^2 - 1)/(p-1) = (2^{b+1} - 1)(p+1)$

$$p \cdot 2^{b+1} = (p+1)(2^{b+1} - 1) \quad \text{or} \quad p = 2^{b+1} - 1 \quad \cdots (2)$$

Hence if we have Euclid's theorem viz: The number $N = (2^{n+1} - 1) \cdot 2^n$ is a perfect number for all numbers n for which $2^{n+1} - 1$ is prime.

The latter is true for $n = 1, 2, 4, 6, \cdots$

(5) Euclid's theorem gives rise to a new problem viz: For what values of n is $2^{n+1} - 1$ a prime?

Now if $(n+1)$ be composite $= uv$, say, then $2^{uv} - 1 = (2^u)^v - 1$ contains $2^u - 1$ as a factor & hence is not prime. Therefore $(n+1)$ must be prime. This is only a necessary condition but not sufficient, for taking $n = 10$, $n+1 = 11$ is prime, but $2^{11} - 1 = 2047 = 23 \cdot 89$ & hence not prime.

Several further perfect numbers of Euclid's type have been found, but no complete rule for finding them all has so far been devised. Another unanswered question is whether there is an infinite number of these perfect numbers or whether there is a last one.

(6) In Euclid's time it was stated without proof that there are no even perfect numbers other

than those given of the Euclid type. Euler later gave a proof of this as follows: —

Let N be any even number so that $N = 2^n u$, where u is odd. Using eqn (1) for D, we get

$$D = \frac{2^{n+1}-1}{2-1} U, \quad \text{where } U \text{ is the sum of the divisors of } u$$

$$= (2^{n+1}-1) U$$

Hence if N be perfect, $(2^{n+1}-1) U = 2N = 2^{n+1} u$, which can be written as

$$(2^{n+1}-1)(U-u) = u$$

$U-u$ is sum of divisors of u not including u (since U included u), & above eqn shows that $U-u$ is a divisor of u. Both these imply that $U-u = 1$ and u is prime. Hence $u = 2^{n+1}-1$, and $N = 2^n(2^{n+1}-1)$ with $2^{n+1}-1$ prime ie a Euclid type of perfect number.

(7) Another unsolved problem is whether there are any odd perfect numbers or not. No one has so far found one, and it appears unlikely but no proof is given.

(8) The number of divisors of $N = p^a q^b r^c \ldots$, is given, using first line of (1), by

$$P = (a+1)(b+1)(c+1)\cdots - 1, \text{ with } N \text{ itself not being included.}$$

Plato must have known this formula for in his Republic he recommends that in a new-founded city, the number of plots of land and of landowners be chosen so that it will have as many divisors as possible, and mentions "perhaps 5040 with 60-1 divisors". The formula formula for P with $N = 5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$ is $P = 60-1$. Plato's use of "60-1" instead of 59 suggests that the formula was known at the time.

(9) Let S be the sum of the divisors of the s^{th} powers of the divisors of a number N. For $s = 1$, $S = D$, and for $s = 0$, $S = P$. Thus is a generalisation which contains both P and D. For each value of s, a formula & analogous to (1) can be found by the same argument viz $S = (1+p^s+p^{2s}+\cdots+p^{as})(1+q^s+\cdots)\cdots$.

Using $s = -1$, the sum of the reciprocals of the divisors of N is given by

$$R = \left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots+\frac{1}{p^a}\right)\left(1+\frac{1}{q}+\cdots+\frac{1}{q^b}\right)\left(1+\frac{1}{r}+\cdots+\frac{1}{r^c}\right)\cdots$$

(10) Notes & Remarks – The primes of the form 2^p-1, where p is prime (which appear in the formula for perfect nos of Euclid type) are called Mersenne numbers. Thus an Euclid perfect number is of the form $(2^p-1)2^{p-1}$, where 2^p-1 is a Mersenne prime (Père Mersenne was a correspondent of Fermat & Descartes). The Mersenne numbers known at present belong to

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281$$

of which the last five were found in 1952–53 by means of the digital computer SWAC at Los Angeles.

Chapter 20 — Euler's proof of the infinitude of the prime numbers.

This proof uses the ideas that are basic in the theory of perfect numbers treated in the previous chapter.

Lemma 1. If p be any prime, and n a positive integer

$$1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^n} < \frac{1}{1-\frac{1}{p}} = \frac{p}{p-1} \quad \text{- - - - - - - (1)}$$

Since $p > 1$, $\frac{1}{p} < 1$ & the L·H·S. is part of a geometric series which converges to $\frac{1}{1-1/p}$.

Lemma 2. If $A_m = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \cdots + \frac{1}{2^m}$ (ie part of harmonic series $\sum \frac{1}{n}$ with $n = 2^m$)

then $A_m > 1 + \frac{m}{2}$.

for $A_m = A_{m-1} + \left(\frac{1}{2^{m-1}+1} + \frac{1}{2^{m-1}+2} + \cdots + \frac{1}{2^m}\right)$ (these being $2^m - 2^{m-1} = 2^{m-1}$ terms inside the bracket)

$$> A_{m-1} + \left(\frac{1}{2^m} + \frac{1}{2^m} + \cdots + \frac{1}{2^m}\right)$$

$$> A_{m-1} + \frac{1}{2}$$

and since $A_2 = 1 + \frac{1}{2}$, this leads by successive steps to

$$A_m > 1 + \frac{m}{2} \quad \text{- - - - - - - - - - (2)}$$

ie A_m can be made as large as we please by taking m large enough.

Lemma 3. Using Lemma 1, with $p = 2, 3, 5, 7, \cdots p$ (ie all primes) respectively, and multiplying all the inequalities of that Lemma thus obtained, we have

$$R_p < M_p = \frac{2}{1} \cdot \frac{3}{2} \cdot \frac{5}{4} \cdot \frac{7}{6} \cdots \frac{p}{p-1} \quad \text{- - - (2')}$$

where R_p is the sum of the reciprocals of all the divisors of

$$N = 2^n \cdot 3^n \cdot 5^n \cdot 7^n \cdots p^n$$

Proof: Consider the series

$$1, 2, 3, 4, \cdots, 2^m \quad \text{- - - - - - - (3)}$$

and let q be the largest ~~prime~~ of all the primes that divide all the numbers of the series (3). Then all the numbers (3) are ~~the~~ products involving only the prime factors $2, 3, 5, 7, \cdots q$. Further none of these primes can appear in a power higher than m since the last largest number of the series is the m^{th} power of the lowest prime 2. Therefore the numbers (3) are all included among the divisors of $2^m \cdot 3^m \cdot 5^m \cdots q^m$. Forming the product R of Lemma 3 with q in place of p and m in place of n ~~in~~, this instantly leads to the ~~factors~~ fact that R_q includes all the terms of A_m. Hence $A_m < R_q$. Further from (2'), $R_q < M_q$ and from (2) $1 + \frac{m}{2} < A_m$.

Combining these, we find

$$1 + \frac{m}{2} < M_q = \frac{2}{1} \cdot \frac{3}{2} \cdot \frac{5}{4} \cdots \frac{q}{q-1} \quad \text{- - - (4)}$$

m on the L·H·S. of (4) is arbitrary & choosing m as large as possible, the L·H·S. can be made as large as possible. If there were only a finite number of primes, the right hand side would increase to a certain value and would then remain constant, and this would contradict the fact that the L·H·S. can be made as large as possible.

(This proof is quite beautiful) but far more complicated than Euclid's, but its importance lies in the fact that the same methods can be applied to a great many similar problems but far more difficult. These methods form the basis for the theory of distribution of primes (a few mentioned in Chap I), one of the ~~most~~ extensive and difficult fields of modern mathematics.

Chapter 23 – Periodic decimal fractions.

(a) Fractions in which the denominator is a prime other than 2 and 5 lead to periodic decimal expansions. The length of the period of $\frac{a}{b}$ may be $(b-1)$ { forex $\frac{1}{7}$ & $\frac{1}{17}$ } or less than $(b-1)$ { eg. $\frac{3}{41}$ with length five only }.

(b) The period of $\frac{a}{b}$ (taken as a reduced fraction ie a & b relatively prime) can be no longer than the number of remainders that are prime to b. ie at most $\varphi(b)$ places if b is prime to 10

(c) [$\varphi(b)$ = no. of numbers less than b & prime to it]

Theorem: (c) The length λ of the period of $\frac{a}{b}$ is the smallest number λ for which $10^\lambda - 1$ is divisible by b

(d) The length $\lambda(b)$ of the period is a divisor of $\varphi(b)$.

(e) If b is prime to 10, then $10^{\varphi(b)} - 1$ is divisible by b

(f) If p is a prime that does not divide 10, then $10^{p-1} - 1$ is divisible by p

Theorem: (g) If b is prime to g, then $g^{\varphi(b)} - 1$ is divisible by b

Theorem: (h) If p is a prime that does not divide g, then $g^{p-1} - 1$ is divisible by p.

(i) If the period has an even number of digits ~~2~~ $2l$ & if the two halves of the period be A and B (each of length l), then $A + B = 10^l - 1$. = number of l digits $99\ldots9$.

(forex in $\frac{1}{7}$ period is 142857 & $142 + 857 = 999$. In $\frac{1}{17}$ period is ~~058823~~ 0588235294117647 and $05882352 + 94117647 = 99999999$.)

This happens when the period belongs to a fraction $\frac{a}{p}$ whose denominator is a prime provided period has an even number of digits [for eg. $\frac{3}{41} = 0.\overline{07317}$ ie period has an odd number of digits]

Chapter 27 – A property of the number 30.

The property that all the numbers less than ~~equal~~ the concerned number, and relatively prime to it are prime numbers is shared by

3, 4, 6, 8, 12, 18, 12, 18, 24, 30.

It is shown in this chapter that 30 is the largest number having this property.

[for 30, numbers < 30 & rel. prime to it are 7, 11, 13, 17, 19, 23, 29 & these are all primes]

The proof of this theorem is equivalent to proving that

$$p_{n+1}^2 < p_1 p_2 p_3 \cdots p_n$$ ~~for~~ is true for all n from 4 onwards

($p_1, p_2, \ldots$ are the prime numbers 2, 3, ---)

for the above ~~inequality Bonse's~~ inequality discovered an ingenious proof ~~of~~ while a student, avoiding all the analytical methods & ε-processes used by Tschebyscheff.

Bonse proved further that

$$p_{n+1}^3 < p_1 p_2 \cdots p_n \quad \text{for } n \geq 5.$$

Chapter 28 – An improved inequality.

Bonse's inequalities of previous chapter are further generalised in one direction with a loss in another direction – Take the primes $q_1, q_2, q_3 \ldots$ where $q_1 = 2$, $q_2 = 3$ and the remaining primes are all of the form $6x-1$ ie the series 2, 3, 5, 11, . . instead of the p's viz 2, 3, 5, 7, . .

It is first proved that if

$$n - i + 1 < q_i \quad \text{---(1)}$$

then $$q_{n+1} < q_1 \cdots q_i \quad \text{---(2)}$$

& next $$(q_1 \cdots q_i)^6 < q_{i+1} \cdots q_n \quad \text{---(3)} \quad (n \neq 6)$$

leading to $$q_1 \cdots q_i < \sqrt[7]{q_1 q_2 \cdots q_n} \quad \text{---(4)} \quad \text{if } n \geq 114.$$

& finally to $$q_{n+1} < \sqrt[7]{q_1 \cdots q_n}, \quad n \geq 114 \quad \text{---(5)}$$

Transferring this to the p's, the inequality becomes

$$p_{r+1} < \sqrt[7]{p_1 \cdots p_r} \quad \text{---(6)} \quad \underline{\text{only}} \text{ for } p_r \geq q_n \text{ ie } p_r \geq q_{114}$$

(6) is an improvement of Bonse's inequality about cube root with this difference that while Bonse's is true for all $n \geq 5$ (for square root ≥ 4), here the seventh-root inequality (6) is true only for a large r viz for an $\underline{r}$ for which $p_r \geq q_{114}$ and thus $\underline{r}$ can be found by checking through a list of prime numbers. (6) may be true for ~~smaller~~ values of $\underline{r}$ smaller than this, but the main interest of (6) is that as $\underline{r}$ passes a certain value it is always true, just like Bonse's inequality. The exact value of this $\underline{r}$ is of less interest – The loss is that (6) is true only for large $\underline{r}$.

[Has anybody generalised this for powers higher than the 7th ?]

Scripta Mathematica – July, 1960, p. 125 – on some unsolved problems of arithmetics by Sierpinski

(1) There are still problems left easy to formulate but still unsolved. There are still problems left for which we don't know which way to follow in order to obtain a solⁿ no matter how long this way & how much time is req^d to perform the necessary computations.

(2) W. Mnich's problem – Are there three rationals the sum as well as the product of which is equal to 1?

ie existence of u, v, w such that $u+v+w = uvw = 1$ – For integers this is equivalent to existence of three integers x, y, z $(\neq 0)$ such that $(x+y+z)^3 = xyz$. ie cube of sum = product. Nobody knows how to answer it – Again Mnich has shown that this is equivalent to existence of three integers a, b, c such that $\frac{a}{b} + \frac{b}{c} + \frac{c}{a} = 1$. – Again equivalent to existence of a rational number $\underline{a}$ with the property that all the roots of the eqⁿ $x^3 - x^2 + ax - 1 = 0$ are rational

For two rationals u, v, the problem is solved & answer is in the negative, for if $u+v = uv = 1$ then $u + \frac{1}{u} = 1$ ie $u^2 + 1 = u$ ie $u > 0$, and $(u-1)^2 = u^2 - 2u + 1 = -u < 0$

For four rationals u, v, w, t, the problem has a positive answer. Mnich has proved that there are ∞ of solns of $u+v+w+t = uvwt = 1$ given by $u = \frac{n^2}{n^2-1}$, $v = -\frac{1}{n^2-1}$, $w = \frac{n^2-1}{n}$, $t = -\frac{n^2-1}{n}$ where n is an integer > 1 – Schinzel has proved that for k-tuples ($k > 3$), there exist ∞ of solns of the problem of sum & product both being equal to 1.

For each k, Schinzel has proved existence of at least one soln of $x_1 + x_2 + \cdots + x_k = x_1 x_2 \cdots x_k$. To get a soln for $k > 2$, put $x_1 = x_2 = \cdots = x_{k-2} = 1$, $x_{k-1} = 2$, $x_k = k$. Nobody even knows how, for sufficiently large k, to show that the no. of such solns is always > 1, let alone this number $\to \infty$.

Thus we are not in a position to decide whether $(x+y+z)^3 = xyz$, an eqⁿ of 3rd order has even one soln in integers that are different from zero – Cannot even find other cubics

(3) The eqⁿ $x^3 + y^3 + z^3 = 3$ & other cubics – the cannot still find all solns in integers. Four solns are known $x = y = z = 1$, $x = y = 4$, $z = -5$ & the other two obtained by cyclic permutation. But we don't know whether there are some other solns, or even whether the no. of such solns is finite, nor do we know any method that may

lead to a soln of the problem.

If we had $x^3+y^3=m$ in view, the object could be attained, for we should only have to perform all the necessary calculations.

On the other hand there are cubic eqns in two unknowns for which we don't know how to find solns in integers for eg. $x^3-y^2=7$. It was even proved that the no. of all solns is finite, but we don't know how many it is

(4) Classification of unsolved problems.

1st Kind: problems for which we know the way to follow to obtain complete solns, and the only difficulty is that we are not in a position to perform all the necessary calculations even with the help of the biggest calculating machines. ie difficulty is purely technical.

2nd Kind – All other unsolved problems.

(5) Examples of problems of the first kind.

(i) To find all the natural divisors of $2^{101}-1$ which is of 31 decimal digits – To this aim test divisibly 1, 2, 3, ... not greater than $\sqrt{2^{101}-1}$. Each natural divisor of $2^{101}-1$ is of the form $202K+1$, where K is an integer ≥ 0. Even then the calculation exceeds our actual possibilities. The existence of some ~~other~~ factors other than 1 & $2^{101}-1$ has been proved viz that there are at least two non-trivial distinct factors. Yet none of them has been calculated so far & so no factorisation of $2^{101}-1$ is so far known, even though we know such factors exist – Of with 2^{101}

(ii) To find out a prime with exactly 500 decimal digits – In virtue of Bertrand's postulate, it follows at once that there are at least three primes with exactly 500 digits. No such number has, however, been found so far, although we know primes having more than 500 digits; for eg (2^n-1) where $n = 2203, 2281$ & 3217 which have 664, 687 and 969 digits. Yet we don't know any such prime having a thousand or more than thousand digits

(iii) Fermat's number $F_{13} = 2^{2^{13}}+1$ of 2467 digits being a prime or not. It is the least Fermat F_n

of which we don't know whether it is prime or not – Fermat supposed that all F_n are prime; it is true only for $n = 1, 2, 3, 4$, but it was later proved that all F_n for $5 \le n \le 12$ are composite. The largest is F_{1945} which has a prime factor $5 \cdot 2^{1947} + 1$ having 587 digits

(iv) To find a decomposition of the number 100 in a sum of a finite sum of different fractions of the form $\frac{1}{n}$. We know a method, but it cannot be done because it is too long.

(v) F_{10} & F_{16} – Later found composite & least prime factor has been found, but complete factorisation is still unknown.

(vi) Cullen's numbers $n \cdot 2^n + 1$ (really problem of second kind) – To find n for which they are prime. Recently the least of such a prime number was found for $n = 141$.

(6) Problems of 2nd kind becoming problems of first kind.

(i) Problem whether each odd number > 7 is a sum of three odd primes – After Vinogradov proved that each odd number $n > a = 3^{3^{16}}$ is a sum of three odd primes, the problem became 1st kind

(ii) Problem whether it is true that whenever $2^n - 1$ is prime, then $2^{2^n} - 1$ is also prime has been of 2nd kind, but when D. J. Wheeler proved in 1953, that the number $2^{2^{13}} - 1 = (m)$ which has 12366 digits is composite even though $2^{13} - 1 = 8191$ is prime. This was done by help of electronic machines. But up to now no factor of m (other than 1 & m) has been found. On the other hand, though $2^{17} - 1$ and $2^{19} - 1$ are prime, it was shown in 1957 that $2^{2^{17}} - 1$ & $2^{2^{19}} - 1$ are composite, and even that the former is divisible by $1768(2^{17} - 1) + 1$ and the latter by $120(2^{19} - 1) + 1$.

(7) Problems of the second kind.

(i) Existence of an A.P. consisting exactly of a hundred distinct primes – The largest such A.P. known so far is the one consisting of 12 terms with initial term 23143 and the difference 30030 – discovered by Gorbutiev – It is proved that there is an ~~any~~ ∞ of increasing A.P's that consist of three primes, but we don't know whether the same is true of 3 consecutive primes (e.g. 47, 53, 59)

(ii) Are there primes except 2, 5 and 257 of the form $n^n + 1$? It can be proved that among all the numbers that have at most 300,000 digits no such number exists.

1.2.3.4.5.6.7.8

5040
40320
362880
3628800
39916800
600

- Again except 2 and 17, we don't know if primes of the form $n^{n^n}+1$ exists. It can be proved if any such prime exists, it has at least millard of millards digits. Even then, we cannot resist the opinion that no such numbers exist, for if we did, it can be shown that the consequence is the proof of the existence of an infinitude of composite Fermat numbers $F_n = K^{K^K}+1$ where $K \geq 2^{2^m}$ $K = 2^{2^m}$.

(3) Does there exist ∞ of primes that have all digits equal to 1?

(4) Is there ∞ of primes of the form x^2+1 (x = integer)?

(5) " among the numbers of the form $n!+1$? We don't know whether $27!+1$ is prime, but this ∞ is of the 1st kind; however it is easy to prove that there is an ∞ of composite $(n!+1)$

(6) Does there exist at very least one even number >2, which is not a sum of two primes? - In 1742 Goldbach conjectured that the answer is negative; a stronger conjecture was stated that each even number >6 is a sum of two different primes.

(7) Is it possible to express an arbitrary even number as a difference of two primes in an ∞ of distinct ways? We even don't know whether each even number is a difference of two primes. We don't know, either whether 2 can be expressed thus in an ∞ of ways ie whether there is an ∞ of twin primes.

(8) Is there an $\infty\infty$ of $\underline{n}$ for which 2^n-2 is divisible by n^2?

(9) Is there any odd $\underline{n}$ for which the sum of all its divisors is $2n$?

(10) Are there any $\underline{n}$ " $2n+1$?

(11) Is there an ∞ of amicable pairs of natural numbers? - Two numbers $\underline{m}$ & $\underline{n}$ are amicable if for either of them the sum of all natural divisors are $m+n$; for eg. 220 & 284 are amicable.

(12) Does there exist any pair of amicable numbers, one even & the other odd?

(13) Is there a composite $\underline{n}$, such that $1^{n-1}+2^{n-1}+\cdots+(n-1)^{n-1}+1$ is divisible by $\underline{n}$? - In 1950 · G. Guiga made the conjecture that the answer is negative. He checked for all $n \leq 10^{1000}$.

(14) Is there any natural $\underline{n}>7$ for which $n!+1$ is a square number? - 4, 5 & 7 (≤ 7) have this property.

(B) Problems of second kind in terms of solvability of equations.

(1) Does there exist a soln of $x^3+y^3+z^3=30$ in integers x, y, z?

(2) Is there any solns in naturals $x_1, x_2, \ldots x_7$ for the system of four equations: $x_1^2+x_2^2=x_4^2$; $x_1^2+x_3^2=x_5^2$ $x_2^2+x_3^2=x_6^2$, $x_1^2+x_2^2+x_3^2=x_7^2$ - This means geometrically the finding of a rect. $\square^d$ such that

the length of all its edges, its diagonal, and diagonals of its faces are all natural numbers.

(3) Is Euler's conjecture that there are no naturals with $x^4 + y^4 + z^4 = t^4$ true?

(4) Is it true that each natural number is a sum of four cubes? – It is easy to prove that for each integer there is an ∞ of ways of expressing it as the sum of five cubes.

(5) Is it possible to express each natural number in the form $x^3 + y^3 + 2z^3$, where x, y, z are integers? – The least number that we don't know if it is of this form is 76 & the next such is 99.

(6) Does there exist natural numbers n, x, y, z such that $x^n + y^n = z^n$ where $n > 2$? Fermat stated the theorem that there are no such numbers, but he did it without proof (mention of proof being in a slip of paper which was lost) – up to now this has been proved for all n where $2 < n \leq 4002$ & for an ∞ number of others. Even the proof for $n = 3$ is difficult, but for $n = 4$ it is much simpler.

(4) Other types of 2nd kind:

(1) If $1, 2, 3, \ldots n^2$ be arranged in n rows, each row consisting of n consecutive numbers, is it true that there is at least one prime in each row? – This conjecture has been verified by Schinzel for all $n \leq 3000$. If true it follows that: (a) there are at least two primes between each two successive squares of naturals, and (b) between each pair of two successive cubes of naturals there are at least two distinct primes, and (c) in the triangular scheme

1
2, 3
4, 5, 6
7, 8, 9, 10
11, 12, 13, 14, 15
– – – – – –

starting from the second, in each row there is at least one prime.

(2) Are there successive naturals, except $8 = 2^3$ and $9 = 3^2$, such that each of them is a power of a natural number with natural exponent (> 1)? – Catalan made a negative conjecture

(3) Is it true that in the decimal expansion of $\sqrt{2}$, the digit 1 occurs an infinite number of times?

(4) Is it true that in the decimal expansion of π, the sum which consists of the nine digits 123456789 consecutively, as they are in their natural order, occurs at least once?

There is a lot more of unsolved problems of arithmetic. Their number continually increases with time. This is because the new problems arise more rapidly than those already established are being proved, and plenty of them have remained unsolved for centuries. But the progress of our knowledge of numbers is advanced not only by what we know already about them, but also by realising what we don't know of them yet.

Mordell's article in the same Issue, p. 93

In no other parts of maths is there evidence of eternal youth as in number theory. In many subjects discovered about the time of Fermat's results in number theory, possibilities have long been exhausted. But in number theory old questions often suggest new problems, new proofs & new associations with other branches of mathematics. Five topics dealt with in the paper:—

(1) If $a_1, a_2, \ldots a_n$ are non-negative integers, then

$$Q = (a_1 + a_2 + \cdots + a_n)! \,/\, a_1! a_2! \cdots a_n!$$

is an integer. This is a classical result known for several centuries — Mordell gives a simple proof.

(2) Pell's eqn $y^2 - Dx^2 = 1$ whose history dates from the time of Fermat & which is known to be solvable in integers x, y with $x \neq 0$ if D is a +ve non-square integer. Consider the eqn $y^2 - Dx^2 = -4$, which, of course, need not have solns for the integers D above. If however D is a prime $p \equiv 1 \pmod 4$, there are always integer solns. Denote by $(x, y) = (u, t)$ the fundamental soln i.e. that one in which x has its least positive value, and $y > 0$, then all integral solns with $x > 0$, $y > 0$ are given by

$$y + x\sqrt{p} = \left(\frac{t + u\sqrt{p}}{2} \right)^n \text{ for integer } n > 0$$

In 1952, Ankeny, Artin & Chowla published the conjecture that when $p \equiv 1 \pmod 4$, then $u \not\equiv 0 \pmod p$. Prof. Taussky-Todd has had this verified for $p < 100,000$ — Here Mordell proves the conjecture under special conds in the form of two theorems using Cyclotomic fields & Bernoulli numbers — Mordell mentions a further extension by Chowla of his two theorems

(3) Rational quadrilaterals — quads called rational if sides & diagonals are rational numbers. It has been known for at least 14 centuries eg. Brahmagupta (born 598 A.D) & to Bhaskara (1114 A.D) — Mordell gives some results towards finding such quadrilaterals, rather complicated — I am reminded of my earlier Calcutta work on cubics.

(4) & (5) are quite complicated problems of a non-elementary character.

—— 0 ——

$(2^2)^{2^2}$

$(a^m)^n = a^{mn}$

(1) Numbers rules the Universe – Pythagoras

(2) Maths is the Queen of the Sciences & Arithmetic is the Queen of Maths – Gauss

(3) Addition, Subtraction, Multiplication & Division

(4) God made the integers, all else is the work of man. – Kronecker

(5) God ever arithmetizes – Jacobi

$2^{2^{2^2}} = 2^{2^4} = 2^{16} =$

$a^{a^{a^a}} = \boxed{2} \quad 2^{2^{2^2}}$

$\triangle = a^{a^{a^a}} \quad 2^{2^4} = 2^{16}$

$\square = a^{a^{a^{a^a}}}$

$256^{256^{256}} = \textcircled{A} = a^{a^{a^{a^a}}} = \text{mega}$

---

not intimately in advance the subject of the talk – not the slightest notion of what to talk about when in a weak moment, I agreed to Prof. Kulkarni's request – officially even afterwards to fix a topic – Supposed to be an appl. mathematician – no meaning in appl. math – Covers all branches of learning – Universality of maths – Russell's definition of maths as a kind of logic – usual meaning of appl. maths – have given addresses on several such topics & wanted not to repeat addresses as President, Ind. Math. Soc, but give something new – struggling how the idea struck me while watching motor car nos. & attempts to factorise them & examine for prime nos – curious phenomena observed of all even numbers & mostly odd & even nos. in equal ::s in one hour's watching, not finding a single prime number – So decided to talk about arithmetic or number theory.

Four branches of maths – Remarks about Arithmetic – Quotation from Alice in Wonderland – Last remark about – re numbers prompting the – re Cocoanut solution of Sc. American article.

Coming back to number theory & watching motor car numbers mention of highly composite nos and Ramanujan's work on same – Short accts. of Ramanujan & his work – Work. re. round numbers – His work on prime number theorem & remarks on prime number theorem – Skewes number, Chess, protons etc – Δ, $\square$, $\textcircled{A}$ mega & megistan

Mention of other problems from Arithmetic ~~Hardy's account~~ – Recent problem of Mnich re. rationals 2, 3, 4 & > 3 –

Problem of placing 36 officers proved impossible by Fisher & Yates; possible for 5^2 and n^2 $(n \neq 6)$ Officers – ~~two kinds of problems, 1st & 2nd kind~~ Problems leading to eqns: Mnich's to $(x+y+z)^3 = xyz$; $x^3+y^3+z^3 = 3$, $x^3+y^3 = n$, $x^3 - y^2 = 7$, ~~$x^3+y^3+z^3=30$~~; $x_1^2+x_2^2 = x_4^2$, $x_1^2+x_3^2 = x_5^2$, $x_2^2+x_3^2 = x_6^2$, $x_1^2+x_2^2+x_3^2 = x_7^2$ & its geometrical meaning; Brahmagupta (598 AD) & Bhaskara (1114) (author of Leelavathi)'s problem of finding rational

Quadrilaterals, recent soln by Mordell; Pellian eqn $y^2 - Dx^2 = \pm 1$ or -4 (Chowla's work); $x^4+y^4+z^4 = t^4$; sum of 4 cubes, sum of five cubes; ~~$x^2+y^2+z^2$~~, Fermat's problem $x^n+y^n = z^n$ $(n > 2)$

Division into problems of two kinds – Examples of problems of 1st kind:

(1) $2^{101}-1$, (2) prime with exactly 500 digits (3) Fermat's numbers (4) $100 = \sum \frac{1}{n}$ (5) Cullen's numbers.

Examples of problems of 2nd kind :- (1) Primes of the form n^n+1 and $n^{n^n}+1$, (2) Existence of ∞ of primes that have all digits 1, (3) primes of the form $n!+1$, (4) Goldbach's conjecture, (5) even no = diff of 2 primes, twin primes, ~~(6) Amicable numbers~~, (6) $n!+1$ is a square number, (7) Successive naturals which are powers (8) In decimal expansion of $\sqrt{2}$, digit 1 occurring ∞ many, (9) In decimal for π, does the sequence 1 2 3 4 5 6 7 8 9 occur at least once?

Second kind $\rightarrow$ first kind :- Ex (1) Vinogradov's problem (2) 2^n-1 & $2^{2^n}-1$ being prime.

Lots more - no. increasing with time & reason for same - But progress of knowledge in theory of nos. is advances not only by ~~how~~ solving but also by unsolved problems.

In the mock-turtle's story.

"I ... ." said the Mock-turtle with a sigh "I only took the regular course"

"What was that?" enquired Alice.

"Reeling and Writhing, of course, to begin with" the Mock-turtle replied "and then the different branches of Arithmetic – Ambition. Distraction, Uglification, and Derision"

"I never heard of "Uglification'" Alice ventured to say "What is it?"

– question about 'beauty' & 'ugly' being its opposite –

Mystery ancient and modern, with Seaography; then Drawling – "The Drawling master taught us Drawling, Stretching, and Fainting in Coils"

"Went to the Classical master, an old crab, who taught us Laughing and Grief"

"Ten hours first day, nine the next and so on, and that's the reason they are called lessons, because they lessen from day to day"

"The eleventh must be a holiday"

"of course, it was"

"And how did you manage on the twelfth?"

"That's enough about lessons"

~~N = 5A + 1~~

(1) five Sailors, monkey & pile of cocoanuts – $N = 5A+1$, $4A = 5B+1$, ..., $4E = 5F+1$. Leads to

$$1024N = 15625F + 11529.$$

If N be a soln so is $N + K\cdot 5^6$ and the guess of $N=-4$, $F=-1$ being a soln – description of soln each sailor getting -2 & the monkey $+6$. Req^d no is $N = -4 + K\cdot 5^6$ & for $K=1$, $N = 15621$ – My soln $1024 = 2^{10}$, $15625 = 5^6$, $11529 = 5^6 - 2^{12}$ so that eqn is $2^{10}(N+4) = 5^6(F+1)$ giving –ve cocoanut soln & since 2^{10} & 5^6 have no common divisors, final soln is $N+4 = K\cdot 5^6$, $F+1 = K\cdot 2^{10}$ & least value is $K=1$.

Suggestion of n sailors, monkey getting m cocoanuts, if nothing better to do.

---

(2) Ramanujan – Born 1887 & married 1909 died 1920, first Indian F.R.S – went to England in 1914, fell ill in 1917 – Tragedy of his early death – Mathematician comparable in power to Euler & Jacobi, Gauss old at 30, Abel dying at 26

Round numbers ; almost all numbers n have $\log\log n$ prime factors.

Prime number theorem – $\pi(x) \sim \frac{x}{\log x}$ · (large x) & better one is ~~$\pi(x) \sim$ li x~~ $\pi(x) \sim$ li x.

$$\text{li } x = \int_0^x \frac{dt}{\log t}.$$

conjecture about $\pi(x) <$ li x – Even Gauss thought so – Ramanujan thinking conjecture false & stating that x must be very very large for the conjecture to be false – Has been verified for x up to 1,000,000,000 – Littlewood's proof of conjecture being false by showing that there is such an x, Skewes found this $10^{10^{10^{34}}}$; largest no. serving any definite purpose in Maths no. of protons in Universe 10^{80}, no. of possible games of chess $10^{10^{50}}$. If Universe be chessboard & protons the chessmen & a move = interchange in posⁿ of two protons, total no. of possible games of chess = Skewes's number

(3) Giant numbers △, □ & ⓜ – mega & megiston – ~~long~~ mega = ⓜ.

(4) Mroick's problem for two rationals $u + v = uv = 1 \to v = \frac{1}{u}$ i.e. $u + \frac{1}{u} = 1$, $u^2 + 1 = u$ i.e. ~~$u > 0$, but~~ $u > 1$, but $(u-1)^2 = u^2 - 2u + 1 = -u < 0$. Hence contradiction i.e. no soln – for case of 4 rationals ex is: $\frac{4}{3}, -\frac{1}{3}, \frac{3}{2}, -\frac{3}{2}$ & for $k \geq 3$, ∞ of solns exist.

(5) $x^3+y^3+z^3=3$ (Solns 1, 1, 1 & $x=y=4$, $z=-5$ & others obtained by cyclic permutation, we don't know whether there are other solns, whether finite, nor do we know any method leading to a soln)

(6) $x^3+y^3=m$, of 1st kind (7) $x^3-y^2=7$ - we don't know how to find solns, proved that solns exist & are finite but we don't know how many.

(8) Pellian eqn - $y^2-Dx^2=1$ (Soln exists if D be a +ve non-square integer)

(9) Euler's conjecture that $x^4+y^4+z^4=t^4$ has no integral solns - unproved

(10) Each n = sum of 4 cubes, not answered, but as sum of 5 cubes, answer is yes & ∞ - no gaps.

(11) Fermat's problem $x^n+y^n=z^n$ - up to now proved for all n, $2<n<4002$ & for an ∞ no. of other numbers. Proof for $n=3$ difficult & $n=4$ easy

Problems of 1st kind - (1) $2^{101}-1$ has 31 digits - Existence of factors other than 1 & $2^{101}-1$ has been proved ie there are at least 2 non-trivial arithmetic factors, yet none often has been calculated

(2) Prime with 500 digits exactly - Proved that there at least ~~2 primes with~~ 3 such primes, but no such has so far been found - we know primes of > 500 digits for eg. 2^n-1 where $n = 2203, 2281, 3217$ having 664, 687 & 969 digits - till 1959, $n=2281$ was largest prime known, in 1960, $n=3217$ was discovered - So far no. prime with 1000 or more digits is known.

(3) Fermat numbers $2^{2^n}+1 = F_n$; F_{13} of 2467 digits is the least F_n of which we don't whether it is prime or not - Fermat supposed all F_n are prime, later proved false. Prime for $n=1, 2, 3, 4$ and for $5 \leqq n \leqq 12$, composite - The largest F_{1945} so far known has a prime factor $5 \cdot 2^{1947}+1$ having 537 digits - F_{16} later found composite & least prime factor found, but complete factorisation not found.

(4) $100 = \sum \frac{1}{n_i}$ - Method is known, but it cannot be done because it is too long.

Problems of the second kind :-

(1) n^n+1 - Except 2, 5, 257 no primes of this form have been found, ~~upto~~ Proved that up to nos. having 300,000 digits no such prime exists. - for $n^{n^n}+1$, we know none except 2 & 17, proved up to nos. with millions of a million digits, but answer cannot be reached

(2) 11, & 11111 are prime.

(3) Primes of form $n! + 1$ – Can be proved ∞ of them exist, but not one known – $27! + 1$ tried (1^{st} kind) but no results.

(4) Goldbach's conjecture – there is no even number > 2 which is not a sum of two primes – not proved. Hardy's remark

(5) Even no = diffce of 2 primes – nothing known in genral – If even no = 2 we have twin primes (eg. 19, 17) & we don't know if we have ∞ of twin primes

~~(5) Amicable nos – If for either of them (m & n), the sum of all natural divisors = $m + n$, eg 220 & 284 – Is there an ∞ of amicable nos.~~

(6) $n! + 1$ is a square for $n = 4, 5, 7$ – Is there a $n > 7$ having this property ? not known.

(7) $8 = 2^3$, $9 = 3^2$ is the only known pair – Catalan's negative conjecture

(8) – –

(9) – –

Second kind → 1^{st} kind – (1) Vinogradov's problem – whether each odd no > 7 = sum of three odd primes – Ver V. proved that each odd number $n > a = 3^{3^{16}}$ is such a sum – After this problem became of 1^{st} kind. ie ~~first $n <$~~ examine $n < a$

(2) If $2^n - 1$ is prime is $2^{2^n} - 1$ also prime – Wheeler D. J. proved in 1953 that $m = 2^{2^{13}} - 1$ is composite (12366 digits) even though $2^{13} - 1 = 8191$ is prime. This done by help of electronic machines, but no factors of m have been found – on the other hand $2^{2^{17}} - 1$ & $2^{2^{19}} - 1$ were shown composite & factors found for each $1768\,(2^{17} - 1)$ & $120\,(2^{19} - 1) + 1$ respy [$2^{19} - 1$, $2^{17} - 1$ are both primes)

Gen. Remarks –

4. 16 + 81 = 97 ; 194 + 25 = 169 ; 13 ; 5 ; 25 + 100 = 250.

6 ; 36 + 121 = 157 ; 314 + 21 = 289 ; 49 + 144 = 193 ; 68 + 386 + 21 = 289

(15) 5 ; (17) 6 ; 64 + 169 = 233 ; 466 + 25 = 441 ; (19) 7 ; (21) 8 ; 81 + 196 = 277 ; 100 + 225 = 325 ; 225 ; 725 ; (23) 9.