Number Theory, ancient and modern

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}, \quad \mathbb{Q} = \{m/n : m, n \in \mathbb{Z}, n \neq 0\}.$$

Most basic mathematical objects. Number Theory is concerned with the study of their mysterious and hidden properties.

It is the oldest part of mathematics having its origins in Asia long before Greek mathematics.

From its earliest beginnings until today, it has been an experimental science.

Numerical experiments lead to general conjectures.

Most difficult part of number theory is to find rigorous proofs of these conjectures. This has only been possible for a small part of the interesting conjectures.

When proofs have been found, they have nearly always relied on major conceptual advances in seemingly unrelated frontiers of mathematical knowledge.

Important parts of number theory where there has been no important progress since the 18 th century.

e.g. continued fraction algorithm, which provides the most basic expansion of any real number.

for example :-

$\sqrt[3]{2}$ - are the partial quotients bounded ?

π - do we have $\left|\pi - \frac{p}{q}\right| > q^{-3}$ when q is sufficiently large

Hermite - Lindeman proved the transcendence of π in the late 19 th century, establishing the impossibility of squaring the circle.

<u>New ingredient</u> in research in number theory today, namely the ever growing links with algorithmic side of <u>Computer science</u>.

Two way process.

Number theory $\longrightarrow$ <u>algorithms</u> to computer science

Computer science - new possibilities of numerical experiments to number theory.

Also, number theory provides the basis for cryptosystems which are secure.

Aim of my lecture is to touch on four major areas of number theory :—

1. Primality testing and factorization ;
2. Diophantine equations ;
3. Distribution of prime numbers ;
4. Connexions between L-functions and arithmetic.

All are very active areas today, but have aspects which are very old.

1. PRIMALITY TESTING & FACTORIZATION

Only consider positive integers in this section.

a factorization of N is an expression

$$N = MR \quad , \; M \text{ & } R \text{ are integers.}$$

We say M & R are divisors of N.

Defn. N is prime if its only divisors are 1 & N.

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$$

Easy: There are infinitely many primes.

Largest explicitly known prime is

$$2^{32582657} - 1 \qquad (\sim 9.8 \text{ million digits}).$$

Obvious that every N has a factorization

$$N = p_1 \cdots p_t \quad > p_i \text{ primes}.$$

Fundamental theorem of arithmetic $\Rightarrow$ unique up to order.

Obvious algorithm for factoring: trial division by 2 then by all odd integers $\leq \sqrt{N}$.

Output. Either tells us N is prime or produces a factorization.

Modern cryptography : it is fast to multiply two large integers.

S & R are $\leq M$.

We can calculate $S \cdot R$ with at most $(\log_{10} M + 1)^2$ elementary operations.

General. A number theoretic algorithm is said to be polynomial if it takes at most

$$c (\log M)^w$$

elementary operations to complete it when applied to integers $\leq M$.

In particular, multiplication is polynomial.

Fundamental Problem 1. Is there a polynomial algorithm for factoring?

We do not even know if the answer should be "yes" or "no".

Primality testing. We seek an algorithm which decides in a finite number of steps whether or not N is a prime (but does not necessarily produce a factorization if N is composite).

Theorem (Agarwal, Kayal, & Saxena). There exists a polynomial algorithm for primality testing.

Proof of this, and an earlier conditional result, depend on congruence techniques.

$m > 0$

Defn. $a \equiv b \bmod m$ if m divides $a - b$.

Multiplication and exponentiation modulo m are polynomial operations.

Conditional primality test (Miller-Rabin).

$$N - 1 = 2^s t \quad (s \geq 1,\ t \text{ odd}).$$

Take w to be any integer in $\{2, \ldots, N-1\}$.

Defn. w is a *witness* for N if at least one of the following congruences does *not* hold :-

$$w^t \equiv 1 \bmod N$$

$$w^{2^i t} \equiv -1 \bmod N \quad \text{for some } i \text{ with } 0 \leqslant i \leqslant s-1.$$

Lemma. N is composite $\Leftrightarrow$ there exists a witness w for N in $\{2, \ldots, N-1\}$.

Defn. $W(N)$ = smallest witness for N in $\{2, \ldots, N-1\}$.

Theorem (Ankeny, Bach). Assume the Riemann hypothesis for all Dirichlet L-functions. Then, for all odd composite N, we have

$$W(N) < 2 \log^2 N.$$

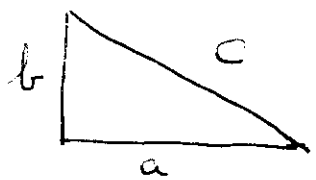
2. DIOPHANTINE EQUATIONS

Study of solutions in integers or rational numbers of polynomial equations in two or more variables.

Congruent number problem - oldest such problem and still unsolved!

$D \geq 1$ in $\mathbb{Z}$.

Defn. D is congruent if it is the area of a right-angled triangle, all of whose sides have rational length



$a, b, c \in \mathbb{Q}$ & $\frac{1}{2}ab = D$.

5, 6, 7 are congruent $\left(\frac{40}{6}, \frac{9}{6}, \frac{41}{6}\right)$, $\left(\frac{3}{2}, 4, 5\right)$, $\left(\frac{288}{60}, \frac{175}{60}, \frac{337}{60}\right)$

Need only consider square free D.

Tables of congruent numbers made by Arab mathematicians 1000 years ago

5, 6, 7, 15, 21, 30, 34, 65, 70, ...

FUNDAMENTAL PROBLEM 2. Prove the existence of an algorithm which decides in a finite number of steps whether a given D is congruent.

Totally unlike the factorization problem. We know the conjectural algorithm! But we cannot prove that it always works.

FUNDAMENTAL PROBLEM 3. Prove that every positive integer of the form $8n+5$, $8n+6$, $8n+7$ is congruent.

Can only be explained by the connexion with L-functions.

Why is this a problem about diophantine equations?

Lemma. D is congruent $\Leftrightarrow$ there is a point (x, y) with x, y in $\mathbb{Q}$ and $y \neq 0$ on the elliptic curve

$$E_D : y^2 = x^3 - D^2 x.$$

Fermat proved 1 is not congruent. His beautiful proof started the modern theory of diophantine equations. He noted it showed that there are no integers x, y, z with $xyz \neq 0$ such that

$$x^4 + y^4 = z^4.$$

Here are two major recent results about diophantine equations: —

THEOREM (Wiles). If $n \geq 3$, there are no integers x, y, z with $xyz \neq 0$ such that

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

THEOREM (Mihaelescu). The only solutions of the equation

$$x^m - y^n = 1$$

in positive integers x, y, m, n with $m, n \geq 2$ is

$$x = 3, \; y = 2, \; m = 2, \; n = 3.$$

3. DISTRIBUTION OF PRIME NUMBERS

$x \geq 2$.

Defn $\pi(x)$ = number of primes p with $p \leq x$.

Today we can compute $\pi(x)$ for $x \leq 10^{21}$.

Gauss - late 18 th century, Gauss made the inspired guess that a good approximation to $\pi(x)$ should be given by the function

$$li(x) = \int_2^x \frac{dt}{\log t}.$$

Numerically, $\pi(x) < li(x)$ for all $x \leq 10^{21}$.

Littlewood proved that $\pi(x) - li(x)$ changes sign infinitely often

Prime Number Theorem $\lim_{x \to \infty} \frac{\pi(x)}{li(x)} = 1.$

FUNDAMENTAL PROBLEM 4. Prove that

$$|\pi(x) - li(x)| \leq x^{\frac{1}{2}} \log x \quad \text{for all } x \geq 3.$$

This turns out to be equivalent to the celebrated conjecture called the Riemann Hypothesis.

Numerical examples of finite arithmetic progressions of primes have long been noticed, e.g.

$$7, 37, 67, 97, 127, 157.$$

The following striking recent result has been proven.

THEOREM (Green and Tao). There exist arbitrarily long arithmetic progressions of prime numbers.

Here are two important open problems about primes:-

(i). Are there infinitely many prime pairs $(p, p+2)$?

(ii). Are there infinitely many primes of the form n^2+1?

4. CONNEXIONS BETWEEN L-FUNCTIONS & ARITHMETIC.

This is the most striking and original part of number theory. L-functions are analytic objects (functions of a continuous variable). When they enter an arithmetic question, they usually predict very simple phenomena that are unexpected from an elementary point of view.

First modern proof of this connexion was given by Dirichlet in 1837.

THEOREM (Dirichlet). Let a, b be relatively prime positive integers. Then there are infinitely many primes of the form $an+b$ $(n = 1, 2, \dots)$.

Curious consequence of his proof. $p > 2$ a prime

$$P = \{1, \dots, p-1\}.$$

Defn. $w \in P$ is a quadratic residue mod p if there exists an integer x with $x^2 \equiv w \bmod p$.

w is a quadratic non-residue mod p if no such x exists.

Ex $p = 19$, quadratic residues are

$$1, 4, 5, 6, 7, 9, 11, 16, 17.$$

Easy. P always has $\frac{p-1}{2}$ quadratic residues, and $\frac{p-1}{2}$ non-residues.

As p varies, we would expect the residues and non-residues to be randomly distributed in P.

Dirichlet's proof shows this is not the case.

$$\mathcal{P} = \left\{1, \cdots, \frac{p-1}{2}\right\}.$$

THEOREM (Dirichlet). For every prime p with $p \equiv 3 \bmod 4$, the set $\mathcal{P}$ contains more quadratic residues than non-residues mod p.

No proof without L-functions has ever been found.

Example of a Dirichlet L-function.

$p > 2$ a prime.

Defn $\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{if } p \mid n \\ +1 & \text{if } (n,p)=1 \text{ and } n \text{ is a quadratic residue mod } p. \\ -1 & \text{if } (n,p)=1 \text{ — } n \text{ is a quadratic non-residue mod } p. \end{cases}$

Defn $L\left(s, \left(\frac{\cdot}{p}\right)\right) = \sum_{n=1}^{\infty} \left(\frac{n}{p}\right) \cdot \frac{1}{n^s} \qquad \mathrm{Re}(s) > 1.$

Dirichlet proved that $L\left(s, \left(\frac{\cdot}{p}\right)\right)$ has a holomorphic continuation to the whole complex plane, and found a simple closed formula for $L\left(1, \left(\frac{\cdot}{p}\right)\right)$.

Generalized Riemann Hypothesis. all zeroes of $L\left(s, \left(\frac{\cdot}{p}\right)\right)$ with $R(s) > 0$ lie on the line $R(s) = \frac{1}{2}$.

Proof seems far away.

In 20 th century, number theorists began to attach L-functions to other arithmetic objects, including the elliptic curve

$$E_D : y^2 = x^3 - D^2 x.$$

How do we define such L-functions? Not obvious! However, the idea comes from noting the identity

$$L\left(s, \left(\frac{\cdot}{p}\right)\right) = \prod_{q \neq p} \left(1 - \frac{\left(\frac{q}{p}\right)}{q^s}\right)^{-1} \qquad (\mathrm{Re}(s) > 1)$$

where the product is taken over all primes $q \neq p$. The RHS is called an Euler product. This Euler product can be vastly generalized. We only give the generalization for the elliptic curve E_D.

Assume D square free. $(q, 2D) = 1$

Defn. N_q denotes number of pairs of integers (x, y) (x and y mod q) satisfying

$$y^2 \equiv x^3 - D^2 x \bmod q.$$

Defn. $a_q = q - N_q$.

Defn. $L(E_D, s) = \prod_{(q, 2D)=1} \left(1 - a_q q^{-s} + q^{1-2s}\right)^{-1}$.

Product is taken over all primes q which do not divide $2D$.
This Euler product only converges for $\mathrm{Re}(s) > \frac{3}{2}$.

THEOREM (Deuring, Weil). $L(E_D, s)$ can be analytically continued to a function which is holomorphic in the whole complex plane.

Birch and Swinnerton-Dyer discovered about 50 years ago an astonishing new arithmetic phenomena in connexion with the function $L(E_D, s)$. Here is a special case of their conjecture.

FUNDAMENTAL PROBLEM 5. Prove that there exists a point (x, y) on E_D with $x, y \in \mathbb{Q}$ & $y \neq 0 \iff L(E_D, s)$ vanishes at $s = 1$.

One direction is proven: if there is a point (x, y), $x, y \in \mathbb{Q}$ & $y \neq 0 \Rightarrow L(E_D, 1) = 0$.

Converse is unknown: we know that

$L(E_D, 1) = 0 \Rightarrow$ there exists a phantom point!

In fact a solution of Problem 5 $\Rightarrow$ solution of Problems 2 & 3.

Remark. There is a functional equation linking $L(E_D, s)$ and $L(E_D, 2-s)$.

Consequence. $L(E_D, s)$ has a zero at $s=1$ of odd order $\Leftrightarrow D \equiv 5, 6, 7 \bmod 8$.

Hence Problem 5 $\Rightarrow$ Problem 3.

In general, there are some interesting closed formulae for $L(E_D, 1)$. We explain one due to Tunnell.

$$g(T) = T \prod_{n=1}^{\infty} (1-T^{8n})(1-T^{16n})$$

$$\theta_k(T) = 1 + 2 \sum_{n=1}^{\infty} T^{2kn^2}.$$

Define $a(n)$, $b(n)$ in $\mathbb{Z}$ by the expansions

$$g(T)\theta_1(T) = \sum_{n=1}^{\infty} a(n) T^n$$

$$g(T)\theta_2(T) = \sum_{n=1}^{\infty} b(n) T^n.$$

Tunnell proved that, for each odd positive square free integer N, we have

$$L(E_N, 1) = u(N)\, a(N)^2 \qquad u(N) \neq 0$$

$$L(E_{2N}, 1) = v(N)\, b(N)^2 \qquad v(N) \neq 0.$$

Hence $L(E_N, 1) = 0 \iff a(N) = 0$

$$L(E_{2N}, 1) = 0 \iff b(N) = 0.$$

There is an obvious algorithm for computing $a(N)$ and $b(N)$.