October 22, 2000

Algebra and Number Theory[1]

1 The Emergence of Algebra

In 1800 Algebra still meant solving equations. However, the effects of the new subjects of analytic geometry and calculus contributed to an enlargement of algebra. The Greek idea of geometrical algebra was reversed into algebraic geometry. The study of algebraic curves led to new structures allowing unique factorizations akin to prime number factorizations.

The nagging problem of solving higher order, quintics, etc. was still present as it had dominated the 17th and 18th centuries. Many great mathematicians, notably Lagrange expended considerable efforts on it. The feeling was widespread that no solution by radicals could be achieved. Indeed, by 1803, Paulo Ruffini has published a proof to this effect, but the first rigorous proof is now attributed to the Norwegian mathematician Neils Abel in 1824,26,27. For a time the theorem was call the Abel-Ruffini theorem. Ruffini made a substantial contribution to the theory of equations, developing the theory of substitutions, a forerunner of modern group theory. His work became incorporated into the general theory of the solubility of algebraic equations developed by Galois.

New approaches were inspired by the successes of analysis and even undertaken by specialists in analysis.[2] By the beginning of the 20th century Algebra meant much more. It meant the study of mathematical structures with well defined operations. The basic units were to be **groups, fields and rings**. The concepts of algebra would unify and link many different areas of mathematics. This process continued throughout the twentieth century giving a strong algebraic flavor to much of number theory, analysis and topology.

The 19th century opened with *Disquisitiones Arithmeticae*, 1801, of **Carl Friedrich Gauss** (1777-1855). In it, Gauss discussed the basics

---

[1] ©2000, G. Donald Allen

[2] At this time, a mathematician could still be knowledgable or at least comfortable in much of mathematics.

of number theory including the law of quadratic reciprocity. He also gave early examples of groups and matrices.

This led to complex numbers $a + ib$, a, b integers which in turn led to more general number fields where unique factorizations fail to exist. Next came ideal complex numbers and by 1870 **Dedekind** defined "ideals" of rings of algebraic integers.

Gauss' study of cyclotomic equations in *Disquisitiones* together with work by **Cauchy** on permutations led to an attack on higher order polynomials. Ultimately, in 1827 **N. Abel** showed the impossibility of solutions of general equations of order five or higher in terms of radicals.

Shortly after that **Evarist Galois** (1811-1832) mapped out the relations between algebraic equations and groups of permutations of the roots. By 1854, **Arthur Cayley** defined an abstract group. Fields were defined some 20 years later by **Dedekind** and then **Weber**.

Other developments of this century were the theory of matrices, eigenvectors and eigenvalues.

2 Some Number Theory

Fascinated with diverging sequences such as the harmonic series, **Leonhard Euler** (1707-1783) was able to make the following observations in a 1737 paper. Consider, for example, the sum of the reciprocals of those numbers whose prime decompositions contain only 2, 3, and 5. Thus we have

$$s = \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{4} + \frac{1}{9} + \frac{1}{10} + \frac{1}{12} + \frac{1}{15} + \frac{1}{16} + \cdots$$

Euler noticed that he could sum this series as

$$s = \frac{1}{1 - \frac{1}{2}} \times \frac{1}{1 - \frac{1}{3}} \times \frac{1}{1 - \frac{1}{5}} = \frac{2 \cdot 3 \cdot 5}{1 \cdot 2 \cdot 4}$$

Indeed, extending to all of the primes, which will generate the entire harmonic series he obtains

$$\sum_{k=1}^{\infty} \frac{1}{k} = \prod_{p=\text{primes}} \frac{1}{1 - \frac{1}{p}}$$

where the divergent sum on the left extends over all positive integers and the (divergent) product on the right extends over the primes. There are logical problems here — equating infinite numbers. However, **Leopold Kronecker** (1823 - 1891) proved the "convergent" version of this result, namely, that

$$\sum_{k=1}^{\infty} \frac{1}{k^s} = \prod_{p=\text{primes}} \frac{1}{1 - \frac{1}{p^s}}$$

and interpretted Euler's formula as the limiting case when $s \to 1^+$. One simple consequence of Euler's formula is that there is an infinitude of primes or else $\prod \frac{1}{1-\frac{1}{p}}$ is finite. The infinitude of primes result is not new, having been discovered before the time of Euclid, but the idea of relating the divergent harmonic series to the number of primes is original.

Euler's intent in this paper was not just to demonstrate this clever argument. Rather is was directed toward determining the distribution of primes. By analogy with the formula above for just the sum of reciprocals of number with factors 2, 3, and 5, we have that

$$S = \sum_{k=1}^{\infty} \frac{1}{k} = \frac{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots}{1 \cdot 2 \cdot 4 \cdot 6 \cdot 10 \cdots}$$
$$= \frac{1}{\frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} \times \frac{6}{7} \times \frac{10}{11} \times \cdots}$$

with just a bit more manipulation. Taking logarithms (what else?)

$$\ln S = -\ln(1/2) - \ln(2/3) - \ln(4/5) - \ln(6/7) - \cdots$$
$$= -\left(\ln\left(1 - \frac{1}{2}\right) + \ln\left(1 - \frac{1}{3}\right) + \ln\left(1 - \frac{1}{5}\right) + \ln\left(1 - \frac{1}{7}\right) + \cdots \right)$$

Now use the expansion $\ln(1 - x^2) = -\left(x + \frac{x^2}{2} + \frac{x^3}{3} + \frac{x^4}{4} + \cdots\right)$ on each of the terms above. After some manipulation, one obtains

$$\ln S = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \cdots,$$

the sum of the reciprocals of the primes. Euler goes on to establish that this series diverges as one might expect. Through this entire paper, we clearly see the master at work. In fact this paper has been called the very beginning of analytic number theory.[3]

---

[3]Modern number theory is a vast subject that encompassing some topics only indirectly related to

2.1 Residues

Euler also considered residue classes:

$$a = r(\mathrm{mod}\ d)$$

means $a = m \cdot d + r$; r is called the **residue** of a modulo d.

This process divides the integers into **equivalence classes**: i.e. the set of all integers congruent to a given integer. This assignment turns out to be a ring homomorphism.

Consider the **arithmetic progression** $0, b, 2b, 3b, \ldots$. Suppose $(d, b) = 1$.[4] Then the sequence $\{kb\}$, $k = 1, 2, \ldots$, contains d different residues $(\mathrm{mod}\ d)$. More generally, we have the following result.

Theorem. If $(d, b) = g$ the sequence $\{kb\}$, $k = 1, 2, \ldots$, contains d/g residues $(\mathrm{mod}\ d)$.

Now consider the **geometric progression**, $0, b, b^2, \ldots$. The number of residues $n \leq \mu = \phi(d)$. (Recall, $\phi(d)$ is the number of integers smaller than and relatively prime to d.) Euler proved that the smallest n such that $b^n = 1(\mathrm{mod}\ d)$ divides μ. (This is now proved by a standard group theory argument.)

Example. $b = 3, d = 8$. Then $b^2 = 1(\mathrm{mod}\ 8)$. $\phi(8) = |\{1, 3, 5, 7\}| = 4$.

Example. $b = 3, d = 7$. Then $\phi(7) = 6$ (Note. $\phi(\mathrm{prime}) = \mathrm{prime} - 1$) So, $3^m = 1(\mathrm{mod}\ 7)$, yields $m|6$. In this case $m = 6$.

The Euler ϕ-function is used to generalize Fermat's "Little Theorem".

Theorem. *If b is a positive integer and if $(a, b) = 1$, then*

$$a^{\varphi(b)} = 1(\mathrm{mod}\ b).$$

numbers (i.e. integers). There are several classifications including elmentary number theory, algebraic number theory, analytic number theory, geometric number theory, and probabilistic number theory. The category reflects the methods and techniques applied. So, we see that by applying the methods of analysis as in the derivation of Euler's formula, we are with the domain of analytic number theory. Elementary number theory, which is by no means itf elementary, uses methods from no other area of mathematics and can be understood by anyone with a good background in high school algebra.

[4]This means d and b are relatively prime.

Corollary (Fermat). *If p is prime $\varphi(p) = p - 1$, so if $(a, p) = 1$ then $a^{p-1} = 1(\mathrm{mod}\ b)$.*

Recall, Fermat's version for $(a, p) = 1$ was $a^{p-1} = 1(\mathrm{mod}\ p)$. But Fermat supplied no proof. Euler considered this problem around 1731, quite unaware of what material was available! He first proved the simpler version $2^{p-1} = 1(\mathrm{mod}\ p)$. This very early version was proved by considering the expression $(1 + 1)^{p-1}$. The proof is not hard.

Theorem: If p is prime, then $2^{p-1} = 1(\mathrm{mod}\ p)$.
Proof. We know

$$(1 + 1)^{p-1} = 1 + \binom{p-1}{1} + \binom{p-1}{2} + \cdots + \binom{p-1}{p-1}$$

and

$$\binom{p-1}{k} = \frac{(p-1)!}{k!(p-1-k)!}$$

Now it is easy to see that

$$
\begin{aligned}
\binom{p-1}{k} + \binom{p-1}{k+1} &= \frac{(p-1)!}{k!(p-1-(k+1))!} \cdot \left[\frac{1}{(p-1)-k} + \frac{1}{k+1} \right] \\
&= \frac{(p-1)!}{k!(p-1-(k+1))!} \cdot \left[\frac{p}{(p-1-k)(k+1)} \right].
\end{aligned}
$$

The numerator of this fraction has the factor p. The proof is completed by combining the $\frac{p-1}{2}$ pairs of such binomial coefficients. This yields a multiple of p plus the first term, which is 1. ∎

Euler also introduced the **quadratic residue** problem, that is to solve

$$x^2 = r(\mathrm{mod}\ q)$$

which we will discuss in more detail shortly.

2.2 Random Numbers

Though relatively simple, a very important application of residues has become popular in the last half century for generating random numbers.

Random numbers have been found to be very useful in all sorts of situations, including simulation, sampling, numberical analysis, computer programing, decision making, and recreation. While this is not the forum to discuss these applications, the nature of the random numbers they require merit attention. In brief, what is needed is a sequence of random numbers, or as random as we can construct them. By this we mean a sequence of numbers in some range, say $[0, 1]$, which are uniformly distributed or distributed in some other way. Below we focus on uniformly distributed sequences; other distributions being possible to derive from them.

Just envoking the term 'random' leads one into a philosophical discussion of what random means anyway. In one sense, there can be no such thing as a random number. Nonetheless, scientific practitioners need this sequence of numbers that exhibit no patterns, and have a specified distribution. Our question is how mathematics entered the picture. Prior to the invention of stored program computers, researchers needing a random number sequence had to resort to a table look-up method of selecting numbers from a huge table of random numbers according to some algorithm. It was a time consuming chore that allowed for only very slow progress. For example, at first random numbers were selected by drawing numbered balls from an urn. In 1927, the first table of 40,000 random numbers, compiled from census reports, was published by L. H. C. Tippett. Eventually machines were built to produce random numbers. Yet, just as computers and stored computer programs were being employed, there came a need for random numbers generated 'on the fly' as the program executed its steps.

In 1946 the great 20th century mathematician, **John von Neumann** (1903-1957) suggested the so called "middle-square" method of generating random numbers. Basically, an n-digit number is squared to form a $2n$-digit number. Of that number the middle n digits are used as the next random number. This procedure is repeated to generate the next and the next and so on. For example, let the nth random number be $r_n = 76582934$, Then

$$\begin{aligned} r_n^2 &= 5864945780048356 \quad \text{and so} \\ r_{n+1} &= 94578004 \end{aligned}$$

Naturally, this procedure is far from random. Indeed, we can write an algorithm to express the next number, which of course means the next

so called random number is completely determined. In fact, many experiments showed that the sequence of numbers so generated possessed rather poor "random" properties. Their distributions may be sufficiently uniform, but they can have rather short cycles. (Can you convince yourself that every formula driven method of producing random numbers using finite arithmetic must eventually cycle?) [See, D. N. Knuth, *The Art of Programming*, Volume II, Addison-Wesley, Reading, 1974]

In 1951, **D. H. Lehmer** invented what is now called the *linear congruential method* for generating *pseeudo random numbers*. The term 'pseudo' is used to clarify the fact that by using arithmetical methods, numbers generated cannot be truly random. His method is this: Given a, c, and M, where M is usually taken to be very large and $(a, M) = 1$. For a given starting value $1 \leq y_0 < M$, define the sequence

$$y_{n+1} = (ay_n + c) \bmod M$$

It is not difficult to show that the sequence is periodic with period M, that is, $y_{n+M} = y_k$ and that the sequence takes on every value $0, \ldots, M - 1$ at most one time every M iterations. If c is taken to be zero, there results *multiplicative contruential method* defined by

$$y_{n+1} = ay_n \bmod M$$

Of course, the same conditions hold for its periodicity. Oftentimes it is the sequence

$$x_n = \frac{y_n}{M}$$

which is a sequence of numbers in [0,1], that is used.

In practice, M is chosen to be a rather large prime number. For example, the ANSI C library for multi-stream random number generation uses $m = 2, 147, 483, 647$. (See: http://www.cs.wm.edu/ va/software/park/park.html) Both a and M are fixed constants in the algorithm. The value y_0 is called the *seed* and is usually input by the user in some way. Changing the seed is the only way to generate differing sequences of pseudo random numbers. There are many more sophisticated methods. [See, H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Nethods*, SIAM, Philadelphia, PA, 1992.] Naturally, *pseudo* means just that. A "True" random number generator should be unbiased, unpredictable and unreproducable. The linear congruential methods are certainly none of those. As von Neumann once remarked, "Anyone who

uses arithmetical methods to generate random numbers is in a state sin." But what else can be done?

This example brings mathematics conceived for no practical value right up to the present — in a context of pure application. Few people taking advanced mathematics, statistics, or operations research today will miss seeing and using these important methods.

2.3 Perfect Numbers

We have already considered perfect numbers, those numbers whose divisors as up to itself. Euler showed that all even perfect numbers have the form
$$2^{p-1}(2^p - 1),$$
where $2^p - 1$ is prime, giving the converse of Euclid's theorem. This result is called the **Euclid-Euler** theorem; no other result bears the name of two contributors separated by such a wide span of time. Are there any odd perfect numbers? Much is known. Indeed Euler proved the following results

Theorem. If n is an odd perfect number, then

$$n = p_1^{k_1} \, p_2^{k_2} \, p_3^{k_3} \, \ldots \, p_r^{k_r}$$

where the p_i are distinct odd primes and $p_1 = k_1 = 1 \pmod 4$.

As a corollary it can be shown that if it known that n is an odd perfect number, then n must have the form $n = p^k m^2$, where p is prime, p does not divide m, and $p = k = 1 \pmod 4$. In particular, $n = 1 \pmod 4$. In 1888, James Joseph Sylvester (1814-1897) showed that $r/ge4$, and $r/ge5$ the following year.

Estimates of the minimum magnitude of an odd perfect number have been made. The classical estimate was made by Turcaninov in 1908. He proved that n must have at least five distinct prime factors and exceed $2 \cdot 10^6$. This lower bound has been improved in recent years, particularly with the help of computers. The current lower bound is that $n > 10^{300}$ and n must have at least eight distinct prime factors and 29 prime factors, not necessarily distinct.[5] All this leads one to

---

[5]This (eight factor) result is recent, having required the use of a computer.

believe that there may be no odd perfect numbers at all. To paraphrase Sylvester, to find an odd perfect number in view of the complex web of conditions would be nothing short of a miricle. Nonetheless whether a lower bound can be increased even to $(10000!)^{10000!}$, a number with so many digits as to be virtually unexpressible with all the resourses of humankind, this still does not eliminate the possibility. In the face of that, these two results amount to a theory of numbers that may not exist. This is how mathematics proceeds.

3   Gauss and Congruences

In his *Disquisitiones* Gauss begins with simple congruences. Recall that b is said to be **congruent** to c **modulo** (mod) a if a divides b with remainder c. We write

$$b = c(\mathrm{mod}\ a)$$

Gauss called b and c each a **residue** of the other.

He showed how to solve

$$ax + b \equiv c(\mathrm{mod}\ m).$$

He solved the Chinese remainder problem: Find N so that

$$N = i_j(\mathrm{mod}\ p_j) \quad j = 1, \ldots, k \quad (i_j, p_j) = 1$$

where all the i_j are relatively prime. He also showed how to compute the Euler φ-function

$$\varphi(n) = \mathrm{card}\{m < n \mid (m, n) = 1\}.$$

Gauss noted that: if p is prime and $a < p$ and m is the smallest integer such that $a^m \equiv 1(\mathrm{mod}\ p)$, then $m \mid p - 1$.

He also showed that there exists a number a such that $m = p - 1$. Such a number is called a **primitive root** modulo p.

Example. $p = 7$ has primitive root $a = 3$. $(3^6 = 7 \cdot 104 + 1)$. So $3^6 \equiv 1(\mathrm{mod}\ 7)$

Another very well known resultof this period is Wilson's Theorem. Proved in 1771 by Lagrange in 1771 In his proof, he noted that the converse also holds.

Wilson's Theorem. If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.

    This result was published in 1770 in *Meditationes Algebraicae* by the English mathematician Edward Waring (1741- 1793). Appearing without proof, it was reported to Waring by his student John Wilson. Its origin may well have been numerical experiment. Curiously enough, Waring mentioned that owing to a lack of suitable notation for prime numbers, results of this type may be very difficult to prove. Gauss disputed this claim, summing up that it is the *notion* not the *notation* that is significant. Significantly, the heavy use of new notations and symbolisms had played an extremely important role in the rapid development of analysis throughout the previous century. Mathematicians were still reeling from the newly discovered power of abstraction and of useful notations. Waring's comment, therefore, is reflective of his time. Gauss' comment came somewhat later when symbolism and abstractions were more commonplace.

3.1   Cryptography

One very important application of congruence theory is to cryptography. The encryption of messages is ancient. For example, it is known the Roman emporer Julius Caesar used a simple substitution cypher. Each letter was encrypted to the letter three places down in the alphbet, with the last three letters "cycled" back to the beginning of the alphbet. Allowing the numbers 1 - 26 denote the letters A - Z, this cypher is easily seen to be mathematically expressed by

$$C = P + 3 \pmod{26}$$

Such codes and complex variants have been used for centuries, and nowadays provide little protection for the security conscious against modern code breaking programs. However, with a little more sophisticated use of congruence theory and group theory and number theory, encryption codes now exist that are virtually unbreakable. The best known of these is the class of so-called RSA codes, named after their inventors R. Rivest, A. Shamir, and L. Adleman. Using only elementary number theory and pairs very large primes numbers, these methods achieve their power by the fact that factoring the product of such primes

is prodigiouly difficult, even with the fastest computers of the day. Remarkably, this encryption technology was first published in 1977 in the popular magazine *Scientific American*.

RSA encryption is relatively simple, but would probably be not very practical prior to the invention of computers. There is required a considerable amount of computation. Here is how it works.

We need two primes p and q, which are taken in practice to be very large. We define $m = pq$ and select v and w so that $(p-1)(q-1)|vw-1$. The two values v and w are the encryption-decryption keys. One is usually public, that is v, the other is private, that is w. Let X be your message. By this we mean that you have converted your message to a number using some simple scheme. For example, one could use the ASCII values (000-255) for each letter and number and merely encode the message as a string of numbers. We now encrypt the message as

$$X_E = X^v (\mathrm{mod}\ m)$$

To make this meanful we must have that the encoded message is less than m. We decrypt the message by the similar formula

$$X_D = X_E^w (\mathrm{mod}\ m)$$

To establish this as a valid encryption scheme we need to show that $X = X_D$. This is straight forward. First of all, note that

$$[X^v (\mathrm{mod}\ m)]^w (\mathrm{mod}\ m) = X^{vw} (\mathrm{mod}\ m)$$

To see this write $X^v = am + b$ where $b < m$. Then $X^v (\mathrm{mod}\ m) = (am + b)(\mathrm{mod}\ m) = b$ and

$$[X^v (\mathrm{mod}\ m)]^w = [am + b(\mathrm{mod}\ m)]^w = b^w$$

Therefore

$$[X^v (\ \mathrm{mod}\ m)]^w (\ \mathrm{mod}\ m) = [am + b(\ \mathrm{mod}\ m)]^w (\ \mathrm{mod}\ m) = b^w (\ \mathrm{mod}\ m)$$

Finally

$$
\begin{aligned}
X^{vw}(\mathrm{mod}\ m) \ &= \ = (X^v)^w (\mathrm{mod}\ m) \\
&= (am + b)^w (\mathrm{mod}\ m) \\
&= (cm + b^w)(\mathrm{mod}\ m) \\
&= b^w (\mathrm{mod}\ m)
\end{aligned}
$$

To complete the proof, we use Fermat's little theorem: if $(a, b) = 1$, and b is prime then $a^{b-1} = 1 \pmod{b}$. We have by the hypothesis $(p-1)(q-1)|vw - 1$ that for some value a

$$
\begin{aligned}
X_D^w(\bmod\, m) &= X^{vw}(\bmod\, m) = X^{vw-1}X(\bmod\, m) \\
&= X\, X^{a(p-1)(q-1)}(\bmod\, m) \\
&= \Big[X(\bmod\, m)\,[X^{(p-1)(q-1)}(\bmod\, m)]^a(\bmod\, m)\Big](\bmod\, m) \\
&= \Big[X\,[X^{(p-1)(q-1)}(\bmod\, m)]^a(\bmod\, m)\Big](\bmod\, m)
\end{aligned}
$$

because for any integers a and b we have

$$
ab(\bmod\, m) = [a(\bmod\, m)\,b(\bmod\, m)](\bmod\, m)
$$

Now $X^{(p-1)(q-1)}(\bmod\, m) = X^{(p-1)(q-1)}(\bmod\, pq)$. Also, $X^{(p-1)(q-1)} = 1(\bmod\, q)$ and $X^{(p-1)(q-1)} = 1(\bmod\, p)$. Thus there are integers s and t such that $X^{(p-1)(q-1)} = sq + 1$ and $X^{(p-1)(q-1)} = tp + 1$. Since p and q are prime, it follows that $s|p$ and $t|q$. It follows that $X^{(p-1)(q-1)} = \tilde{s}pq + 1$, or what is the same $X^{(p-1)(q-1)} = 1(\bmod\, m)$. Finally,

$$
\begin{aligned}
X_D^w(\bmod\, m) &= \Big[X\,[X^{(p-1)(q-1)}(\bmod\, m)]^a(\bmod\, m)\Big](\bmod\, m) \\
&= X
\end{aligned}
$$

and this completes the proof.

So, whomever possess your private key can decrypt your messages. Alternatively, you announce to the world your public key — there are ways to do this. Then anyone wishing to send you a secret message can encrypt it with that key. You alone, possessing the private key, can decrypt the message. What makes the code difficult to break is the challenge to determine computationally p and q. And when p and q are quite large, the computational demands exceed current computational capabilities.

The world of cryptography, from every possible viewpoint, is vast. For example, the following is a classification scheme for ciphers is given by Gary Knight (*Cryptanalysts Corner*, Cryptologia 1 (January 1978):68–74) In this and a sequence of papers he gives mathematical techniques for attacking a cypher.

```
Substitution
```

```
    Polyalphabetic
        Periodic
            Non-Interrelated Alphabets
            Interrelated Alphabets
            Pseudorandom Key
        Non-periodic
            Non-Random Key, Random Key
    Polygraphic
        Digraphic, Algebraic
    Monoalphabetic
        Standard, Mixed Alphabet, Homomorphic,
        Incomplete Mixed Alphabet, Multiplex, Double
    Fractionating
        Bifid, Trifid, Fractionated Morse, Morbit
Transposition
    Geometrical - Rail-fence, Route, Grille
    Columnar
        Complete - Cadenus, Nihilist
        Incomplete - Myskowski, Amsco
    Double - U.S. Army Transposition Cipher
```

The Caesar encryption is monoalphabetic, while the RSA encryption is polygraphic. A glossary of terms for such terms is *Ritter's Crypto Glossary and Dictionary of Technical Cryptography*, which is maintained by Terry Ritter and can be found at http://www.io.com/ ritter/GLOSSARY.HTM To take a brief 10 minute tour on ancient and modern codes, try the Website http://www.iwm.org.uk/online/enigma/eni-intro.htm

3.2   Quadratic Reciprocity

In his attempt to determine which **primes** can be written in the form $x^2 + ny^2$ or to determine their prime divisors, Euler was led to the idea of **quadratic residue**.

Let q be a prime. Euler called $p \neq 0$ a **quadratic residue** with respect to q if p has the form $p = a^2 + nq$ or $a^2 = p(\mathrm{mod}\ q)$. Put

another way

$$x^2 = p \pmod{q}$$

has a solution. He was able to establish numerous results. For example, he showed that if p is and odd prime and if $(a, p) = 1$[6], then a is a quadratic residue of p if and only if $a^{(p-1)/2} = 1 \pmod{p}$. Euler also conjectured the quadratic reciprocity theorem in 1783 but could not prove it.

Euler's work was continued by the French mathematician **Adrien Marie Legendre** (1752 - 1833) and in a landmark paper of 1785 established many results about the quadratic reciprocity law. He gave a skethc of a theory of the representation of any integer as the sum of three squares, and stated what was to become a famous result, that every arithmetic progression[7] $ax + b$ where $(a, b) = 1$ contains an infinity of primes. He assembled these results and others in his *Essai sur la Theorie des Nombres* in 1798 in a systematic way in what is regarded as the first modern treatise devloted to number theory. This work was then expanded into his *Theorie of Numbres*. In 1787 Legendre gave an imperfect proof of the quadratic reciprocity law by assuming in his argument that for any prime $p = 1 \pmod{8}$, there exists another prime $q = 3 \pmod{4}$ for which p is a quadratic residue. This result is equally difficult as the quadratic reciprocity law itself.

Gauss was up to the challenge. At the age of eighteen in 1795 he rediscoved the law and with a year of undiminished labor obtained a correct proof. Said Gauss, "It tortured me for the whole year and eluded my most strenuous efforts before, finally, I got the proof ..." All told, he eventually published five proofs!

Quadratic Reciprocity Theorem If p is a prime number of the form $4n+1$, $+p$ will be a quadratic residue of any prime q which is a quadratic residue of p. If p is a prime of the form $4n + 3$, the same is true for $-p$.

In symbols we may write this as:

---

[6]a and p are relatively prime.

[7]An arithmetic progression of numbers is as the definition indicates a subset of the integers with a constant difference between successors. Recall, a geometric progression is one with a constant quotient between successors.

(1) For $p = 4n + 1$ prime

$$
\begin{aligned}
x^2 &= p(\operatorname{mod} q) \quad \text{has a solution if} \\
y^2 &= q(\operatorname{mod} p) \quad \text{has a solution.}
\end{aligned}
$$

(2) For $p = 4n + 3$

$$
\begin{aligned}
x^2 &= -p(\operatorname{mod} q) \quad \text{has a solution if} \\
x^2 &= q(\operatorname{mod} p) \quad \text{has a solution}
\end{aligned}
$$

This theorem led to powerful prime factorization methods.

In a paper of 1832 when Gauss was trying to extend the law to **cubic** and **quartic residues** and the corresponding factorization problems he was led to what are now called the **Gaussian integers**:

$$a + ib, \quad a \text{ and } b \text{ integers.}$$

The power of Gaussian integers is felt in the area of **Algebraic Number Theory**. For example, using them one can show that the equation

$$x^2 + 1 = y^3$$

has only the *integral* solution $x = 0, y = 1$.[8] This equation was central in the analysis of Fermat's conjecture. He noted 4 units among them, $\pm 1, \pm i$. He defined the norm of $a + ib$ to be $a^2 + b^2$. He calls one **prime** if it cannot be expressed as a product of two others, neither a unit. He then determines which Gaussian integers are prime.

Because odd primes of the form $p = 4n + 1$ can be written as the sum of two squares, $p = a^2 + b^2$, we have in Gaussian integers

$$p = a^2 + b^2 = (a + ib)(a - ib).$$

Thus p is not prime. However, if $p = 4n + 3$ is prime it remains prime as a Gaussian integer.

Gauss shows $a + ib$ is a prime if and only if its norm is a real prime which can not be 2 or have the form $4n + 1$. So 2 and primes of the form $4n + 1$ split as the product of two Gaussian primes while those of the form $4n + 3$ remain prime there.

---

[8]It was proved in 1875 by Pepin but posed by Euler.

Example. Consider $3 + 5i$. The norm of $3 + 5i$ is

$$9 + 25 = 34 = 2 \cdot 17$$

. Since $17 = 1 \pmod 4$ we can write it as the sum of squares; i.e. $17 = 1^2 + 4^2$. Thus

$$17 = (4 + i)(4 - i)$$

is <u>not</u> prime. Also 2 is <u>not</u> prime as

$$2 = (1 + i)(1 - i).$$

Therefore

$$3 + 5i = (1 + i)(4 + i)$$

is the prime factorization. He finally proves *uniqueness* of factorization of Gaussian integers (up to units). A basic question is now one of the **factorization over domains**.

4   The Prime Number Theorem

Ever since the classical period of the Greeks, mathematicians had been seeking a rule for the distributions of primes. Let

$$\pi(p) := \text{number of primes less than } p$$

In 1798, on the basis of counting primes, Legendre conjectured that $\pi(p)$ should have the distribution

$$p/(\ln p - 1.08366).$$

Gauss wrote on the back page of a log(arithm) table he obtained when he was just 14 years old, the following:

$$\text{Primzahlen unter } a \ (= \infty) \ \frac{a}{\ln a}$$

This is the celebrated **Prime Number Theorem**, namely that

$$\lim_{a \to \infty} \pi(a) \Big(\frac{\ln a}{a} \Big) = 1.$$

However, Gauss was unable to prove this result. In 1851 it was proved by **P. Tchebyschev** (1821-1894), a leading mathematician of the 19th century that if the limit existed, it must be one.

In 1859 **Bernhard Riemann** attacked the problem with a new method, using a formula of Euler relating the sum of the reciprocals of the powers of the positive integers with an infinite product extended over the primes. Riemann replaced the real variable s in Euler's product formula with a complex number to define the (Riemann-)zeta function

$$\zeta(s) = \sum_{k=1}^{\infty} \frac{1}{k^s} = \prod_{p=\text{primes}} \frac{1}{1 - \frac{1}{p^s}}$$

and showed that the distribution of prime numbers is intimately related to properties of the function $\zeta(s)$ defined by the series Riemann came close to proving the prime number theorem, but not enough was known during his lifetime about the theory of functions of a complex variable to complete the proof successfully.

Thirty years later the necessary analytic tools were at hand, and in 1896, two mathematicians, **Jacques Hadamard** (1865-1943) and **C.J. de la Vallée-Poisson** (1866-1962) came up with independent proofs. The proof was one of the great achievements of analytic number theory. Subsequently, new proofs were discovered, including an elementaryproof found in 1949 by **Paul Erdos** and **Atle Selberg** that makes no use of complex function theory.[9]

5 Algebraic Structure

The origin of algebraic structure can be attributed to both factorization problems related to related to Fermat's Last Theorem, conjectured in the years 1638-1659 and to a systematic study of the solutions of general algebraic equations.

Recall, Fermat's Last Theorem asserts that *there are no integral solutions to*

$$x^n + y^n = z^n \qquad n > 2.$$

---

[9]It is typical of mathematicians to use such a description as "elementary." In fact, the proof is by no means easy. It is indeed a *tour de force* of classical number theory that makes no reference to complex function theory. Hence the term "elementary."

This you will note is a special algebraic equation in three unknowns.

It was resolved in a number of special cases. In the 19th century the score board of solutions was:

- $n = 3$, Euler 1753

- $n = 5$, Legendre 1825

- $n = 14$, Dirichlet 1832

- $n = 7$, Lamé 1839

- $p \mid xyz$, p a prime < 100 Germain 1820

Lamé announced a general proof in 1847. It involved a unique factorization into primes of a factorization of $x^n + y^n$ over the complex numbers. Liouville expressed doubt, and indeed Liouville was correct. Lamé's argument ultimately failed. However, the study of factorization began in earnest generating new classes of numbers.

Ernst Kummer (1810-1893) also studied higher reciprocity laws. He arrived at the **cyclotomic integers**, which are complex numbers of the form
$$f(\alpha) = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1},$$
where α is a solution to $x^n - 1 = 0$ and each a_i is an integer. Note: if $n = 2$, we get the Gaussian integers. Kummer worked on the factorization of cyclotomic integers. He used the norm

$$Nf(a) = \prod_{j=1}^{n-1} f(\alpha^j).$$

Toward this end he used the two classes: we say $f(\alpha)$ is

- **irreducible** if it cannot be factored into two other integers

- **prime:** if when it divides a product it divides one of the factors.

Theorem. *prime $\Rightarrow$ irreducible. irreducible $\nRightarrow$ prime.* Take $n = 23$ for the example.

With these ideas Kummer made progress on Fermat's theorem for certain n. He was able to show the theorem for all regular prime powers. The only primes not regular and less than 100 are 37, 59, and 67. He eventually resolved the theorem for all powers < 100. Further computations based on his ideas gave the impossibility up to $n = 25,000$. (Pollack and Selfridge, 1964). Kummer wanted to extend his cyclotomic integers to domains generated by a root of $x^n = D$, D and integer. But he failed. The next advance was made by **Richard Dedekind** (1831-1916) who defined **algebraic numbers** and the **algebraic integers** as solutions to

$$\theta^n + a_1\theta^{n-1} + \cdots + a_{n-1}\theta + a_n = 0,$$

where the a_i's are rationals or integers, respectively.

Restricting himself to a part of the domain he was able to achieve the Euclidean division algorithm. From this he went to sets he called **ideals** and then to **principle ideals** and **prime ideals**. With these tools he was able to achieve unique factorizations.

6 The Solution of Equations

The solutions of algebraic equations was a primary goal for many mathematicians from the time of Cardano and Tartaglia. Of course quadratics were well understood. With cubics, we saw the natural emergence of complex numbers. In 1637 Descartes said that for a polynomial of degree n one may imagine n zeros, but that they may not correspond to any real quantity. Yet it was Albert Girard who in 1629 claimed that there are always n solutions of the form $a + ib$. This of course was to become the Fundamental Theorem of Algebra (FTA).

This result, thought by many mathematicians as self evident, attracted a few detractors. Most notable among them was Leibnitz. In 1702 he claimed the FTA was false citing the impossibility of solving $x^4 + 1 = 0$ because one of its roots was $\sqrt{i}$. Unaware that the number $\sqrt{i}$ was expressible in the form $a + ib$, he revealed among many other things that even the best mathematicians had but a tenuous hold on complex numbers at that time. It took another forty years and a mathematician of no less the caliber of Euler to show that the Leibnitz counter example was wrong. By comparison, every modern undergraduate mathematics

major can easily express $\sqrt{i}$ in the form $a + ib$.

Among the many mathematicians that proposed proofs of the FTA were d'Alembert, Lagrange, Laplace, and Euler. All were incorrect, a testament to the difficulty of and importance of this result. d'Alembert attempted and iterative method. Euler attempted a factorization of the polynomial into lower order polynomials, where the new coefficients would be rational functions of the original coefficients. A clever idea, it was carried out in detail only for the case $n = 4$. In general, this method had flaws, observed by Lagrange. In 1799, Gauss offered a proof. Alas, this first attempt has some gaps by modern standards, but by 1816 he provided a correct and complete proof. The breakthough came from a Swiss accountant, Jean-Robert Argand (1768 - 1822). His representation of imaginary numbers rotated 90$_o$to the complex plane allowed a geometric description of the complex numbers. In his 1814 paper, *Réflexions sur la nouvelle théorie d'analyse*, he then adapted d'Alembert's idea to establish the existance of the minimum of a function. The flaw here was that there yet existed no theory to conclude that a bounded infinite set of complex numbers possessed a limit point (the location of the minimum).

A fundamental flaw was evident in many of the proposed proofs, in particular the one of Euler. It was the basic assumption asserting the existence of the roots in some form. The proofs then derived that they had the desired complex form. Gauss took great exception to this flaw, condemming it thoroughly. The Eulerian assumption indicates that mathematicians of the time believed that there was likely a hierarchy of complex-like numbers. (i.e. reals→complex numbers→???) Gauss, himself, believed this calling them shadows of shadows. Only one of these shadows was discovered. Called *quaternions* In 1831 Gauss used the term 'complex number' for the first time.

The FTA closes one door on algebraic equations, the 'existential door.' There are many doors as yet unopened. Properties of the zeros of classes of polynomials, methods for their determination, even a constructive proof of the FTA are but a few. However, what remained unknown was how to find these roots.

These studies were not performed in sequence. All questions were pursued at once. For example, In the final chapter of his *Disquisitiones* Gauss discussed solutions of $x^n - 1 = 0$, cyclotomic equations. Gauss

reduced the problem to the case when n is prime and by factoring

$$x^n - 1 = (x - 1)(x^{n-1} + \cdots \pm 1)$$

he focused on the **cyclotomic polynomials**

$$x^{n-1} + x^{n-2} + \cdots + x + 1. \qquad (*)$$

His goal was to factor $n-1$ into primes and factor $(*)$ into auxiliary equations, one for each prime. [Example: $n = 17$, gives $n-1 = 2 \cdot 2 \cdot 2 \cdot 2$. Find four equations. Example: $n = 41$, $n - 1 = 2 \cdot 2 \cdot 2 \cdot 5$. Find four equations.]

From this he shows that if $n - 1$ is a power of two the reduction of $(*)$ is into quadratics which in turn can be solved by radicals. This is how he was led to the construction of regular polygons <u>only</u> for Fermat primes, i.e. number of the form $2^{2^n} + 1$.

Among the other products of these investigations are examples of what would be called cyclic groups, cosets and subgroups.

In 1837 **Pierre Wantzel** (1814-1848) actually furnished a proof that polygons with number of sides $n = 7, 11, 13, 19, \ldots$ **could not** be constructed. Generally he showed that any construction problem that **does not** lead to an irreducible polynomial equation of degree 2 with constructable coefficients cannot be accomplished with a compass and straightedge. You can find a proof in our chapter on the Delian problem. This section also shows that the cube cannot be doubled. The two theorems are below.

Theorem. (Delian problem) The cube cannot be doubled. **Proof.** $x^3 - 2a^3 = 0$ is irreducible as above.

Theorem. (Trisection problem) An arbitrary angle cannot be trisected. **Proof.** Given the angle α, the corresponding cubic equation to be factored is equivalent to $4x^3 - 3x = a$. It is irreducible as above. (Here, $x = \sin \alpha/3$ and $a = \sin \alpha$.)

In a similar context, squaring the circle meant solving the quadratic $x^2 - \pi = 0$. But is π constructable? People were beginning to think it could not be so. Both the Delian problem and the trisection problem were resolved by relatively simple extentions of the rationals. This problem, on the other hand, would require a category of number beyond

the reach of any polynomial solution, that is to say beyond algebraic numbers. But before the proof could be found, such numbers had to be conceived, contructed, and categorized.

Joseph Liouville (1809-1882) in (1844) found the first nonalgebraic numbers[10] – called **transcendental**. His example:

$$\frac{1}{10} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + \frac{1}{10^{4!}} + \cdots .$$

His basic technique was continued fractions. However, he could not show that either π or e were transcendental.

The investigation of transcendental numbers continues to this day. In 1934, the great Russian mathemtician **A. O. Gelfond** and Th. Schneider (independently in 1935) proved the following result.

Theorem. If α and β are algebraic numbers with $\alpha \neq 0$, $\alpha \neq 1$ and if β is not a real rational number, then any value of α^β is transcendental.

Here β in this context need not be a real number at all. For example any complex number of the form $\beta = p + iq$, where p and q are rationals satifies the hypothesis. Thus, numbers such as 2^i and $2^{\sqrt{2}}$ must be trancendental. If you recall from complex variable theory that $\alpha^\beta = e^{\beta \ln \alpha}$ can be multiply valued, this explains the statement 'any value of' in the theorem statement. In particular, one value $i^{-2i} = e^{-2i \ln i}$ is e^π, which therefore is transcendental. Gelfond's theorem by the way resolved the seventh problem of David Hilbert.

Only recently, the English mathematician, **Alan Baker** (1939-), in 1966, extended Liouville's original proof of the existence of transcendental numbers by means of continued fractions, by obtaining a result on linear forms in the logarithms of algebraic numbers. This result, which also greatly generalized the Gelfond-Schnieder theorem, opened the way to the resolution of a wide range of Diophantine problems. For this achievement, he was awarded the Field's medal in 1970. On the Web: http://www-groups.dcs.st-and.ac.uk/˜history/Mathematicians/Baker_Alan.html

Connected with this is the order approximation of numbers by ra-

---

[10]Recall that **algebraic numbers** are those numbers which are solutions of polynomial equations with integer coefficients. Remarkably, the algebraic numbers are countable, meaning that they can be put into a one-to-one correspondence with the integers themselves.

tionals. We say the the number x is of order n if the equation

$$\left| x - \frac{p}{q} \right| < C \frac{1}{q^n}$$

has infinitely many integer solutions with $(p, q) = 1$. For example, all rationals have at most order 1, and all algebraic numbers **cannot** have order one greater than the degree of the polynomial of which they are solutions. The transcendental number $\frac{1}{10} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + \frac{1}{10^{4!}} + \cdots$. above has order ∞. However, not every transcendental number has order ∞. The interested reader should study the Liouville-Roth index for more information on this difficult subject. Two relevant books are G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed. Oxford University Press, 1985 (pp. 159-164) and A. Baker, *Transcendental Number Theory*, Cambridge University Press, 1975. A good Web site is http://mathworld.wolfram.com/TranscendentalNumber.html.

Charles Hermite (1822-1901) showed e to be transcendental in 1873 by showing that it cannot be a solution of a polynomial equation with rational coefficients.

Ferdinand Lindemann showed in (1880) that π was transcendental by showing that

$$\sum^{n} a_j e^{m_j} = 0$$

has no rational solution if the a_j and m_j are algebraic. Since $e^{ix} + 1 = 0$ has the solution $e^{i\pi} + 1 = 0$.

Lindemann's result proves that π cannot be algebraic and hence not constructable.

6.1   Permutations — solving equations

Cauchy (1789-1857) uses the word 'substitution' for a one-to-one function of a finite set to itself. He studies

- Products of permutations
- Degree = smallest $n \ni S^n = I$

- Subgroups with generator the order of which divides $n!$ ($\equiv$ # permutation)

N. Abel (1802-1829) proved that quintics cannot be solved using radicals. His proof uses permutations. He had wanted

① To find all polynomials solvable by radicals.

② To decide if a given polynomial is solvable.

algebraically. **Theorem.** (1829, Crelle's Journal) If the roots of any equation of any degree are related so that all are rationally expressible in terms of one of them (say x) and if for any two θx and $\theta_1 x$ [where θ and θ_1 are rational functions] we have $\theta_1 \theta x = \theta \theta_1 x$, then the equation is algebraically solvable. Note here the **Abelian condition**.

7   Groups and Fields

Gauss and quadratic forms: Gauss considers **quadratic forms**

$$f = ax^2 + 2bxy + cy^2, \qquad a, b, c \text{ integers.}$$

He shows two such forms equivalent,

$$f' = a'x^2 + 2b'xy + c'y^2$$

if there exists $x = \alpha x' + \beta y'$ and y: $\gamma x' + \delta y'$ such that $f \to f'$. He proves that $f' \equiv f \Rightarrow b^2 - ac = b'^2 - a'c'$, but the converse is false.

Gauss defined rules of composition: $f + f'$. Basically he forms an **Abelian group**.

In 1870, **Leopold Kronecker** (1823-1891) developed abstract group theory, first using $f(\theta, \theta') = \theta''$, later using $\theta \cdot \theta' = \theta''$.

Theorem. (Fundamental Theorem of Abelian Groups).*Let G be a finite Abelian group. Then G is the direct product of a finite number of finite cyclic subgroups.*

$$G = \prod_{i=1}^{m} D_i, \quad \text{order } D_i \mid \text{ order } D_{i+1} \qquad i = 1 \ldots m - 1.$$

With this selection the orders D_i are uniquely determined.

In 1854 **Arthur Cayley** (1821-1895) defines group, but not necessarily a commutative one. Both Cayley and Kronecker recognized the importance of abstraction as opposed to specific concrete realizations.

In 1893 **Heinrich Weber** (1842 - 1913) abstracted the concept of field based on the work of Galois, Dedekind and Kronecker. For example, Weber proved Kronecker 's theorem that the absolute Abelian fields are cyclotomic; that is to say, they are derived from the rational numbers by the adjunction of roots of unity. He also established the most general form of Abel's theorem.

7.1   Axiomization of the Group Concept

Walther von Dyck (1856-1934) published a study on groups as abstract **objects** with a multiplication operations.

He constructed the **free group** on m generators. He then restricts the definition by assuming various relations of the form $F(A_1, A_2, \ldots, A_m) = 1$.

Example. Form the group $\overline{G}$ from $\bar{A}_1, \ldots, \bar{A}_m$ which satisfy the given relation. Then all the elements of G which are equal to the identity in $\overline{G}$, form a subgroup H and this commutes with all operations of the group G.

Theorem. $A \to A_i$ is an **isomorphism** (he called) G onto G'. (Modern) H is a normal subgroup of G and $\overline{G}$ is isomorphic to G/H.

Heinrich Weber (1842-1913) defined the abstract finite group. It properties are:

- Closure under $\cdot$,

- Associativity,

- $\theta\theta_r = \theta\theta_s$ and $\theta_r\theta = \theta_s\theta \Rightarrow \theta_r = \theta_s$.

He shows there must be a unit and formally defines the concept of the **Abelian group**, namely a group whose elements commute.

8   The Mathematicians

Marie-Sophie Germain (1776 - 1831) was born in Paris and lived there her entire life. She was the middle daughter of Ambroise-Francois, a prosperous silk-merchant, and Marie-Madelaine Gruguelin. At the age of thirteen, Sophie read an account of the death of Archimedes at the hands of a Roman soldier. She was moved by this story and decided that she too must become a mathematician. Sophie pursued her studies, teaching herself Latin and Greek. She read Newton and Euler at night, wrapped in blankets, as her parents slept. Not at all encouraging her talent and in an effort to turn her away from books, they had taken away her fire, her light and her clothes. Sophie obtained lecture notes for many courses from Ecole Polytechnique. At the end of Lagrange's lecture course on analysis, using the pseudonym M. LeBlanc, Sophie submitted a paper whose originality and insight made Lagrange look for its author. When he discovered "M. LeBlanc" was a woman, his respect for her work remained and he became her sponsor and mathematical counselors. Sophie's education was, however, disorganized and haphazard and she never received the professional training which she wanted.

Germain wrote to Legendre about problems suggested by his 1798 *Essai sur le Thorie des Nombres.* However, Germain's most famous correspondence was with Gauss. She had developed a thorough understanding of the methods presented in his 1801 *Disquisitiones Arithmeticae* . Between 1804 and 1809 she wrote a dozen letters to him, initially adopting again the pseudonym "M. LeBlanc" because she feared being ignored because she was a women. During their correspondence, Gauss gave her number theory proofs high praise.

Among her work done during this period is work on Fermat's Last Theorem It was to remain the most important result related to Fermat's Last Theorem from 1738 until the contributions of Kummer in 1840.

Germain continued to work in mathematics and philosophy until

her death. Before her death, she outlined a philosophical essay which was published posthumously as *Considérations génerale sur l'etat des sciences et des lettres* in the Oeuvres philosophiques . Her paper was highly praised by August Comte. She was stricken with breast cancer in 1829 but, undeterred by that and the fighting of the 1830 revolution, she completed papers on number theory and on the curvature of surfaces (1831).

Germain died in June 1831, and her death certificate listed her not as mathematician or scientist, but rentier (property holder).

The portrait above is taken from a commemorative medal.

Gabriel Lamé (1795 - 1870) was a student at the École Polytechnique and later a professor there. Between these times (1820-1831) he lived in Russia. He worked on a wide variety of different topics. His work on differential geometry and contributions to Fermat's Last Theorem are important. Here he proved the theorem for n=7 in 1839. In number theory he showed that the number of divisions in the Euclidean algorithm never exceeds five times the number of digits in the smaller number. On the applied side he worked on engineering mathematics and elasticity where two elastic constants are named after him. He studied diffusion in crystalline material.

Lamé worked on the Ellipse, on the Hyperbola and on the Lamé Curves

Evariste Galois (1811 - 1832) lived
a life that was dominated by politics
and mathematics. He entered the Ecole
Normale Supérieure 1829. By then,
however, he had already mastered the
most recent work on the theory of equa-
tions, number theory, and elliptic func-
tions. He submitted his papers to Cauchy,
the only mathematician capable of un-
derstanding it. To his misfortune Cauchy
was a fervent republican while he was
an ardent republican. This caused some
delay. In 1829 he published his first
paper on continued fractions, followed
by a paper that dealt with the impos-
sibility of solving the general quintic
equation by radicals. This led to
Galois theory, a branch of mathematics dealing with the general solution
of equations.

Famous for his contributions to group theory, he produced a method
of determining when a general equation could be solved by radicals.
This theory solved many long-standing unanswered questions including
the impossibility of trisecting the angle and squaring the circle.

He introduced the term 'group' when he considered the group of
permutations of the roots of an equation. Group theory made possible
the unification of geometry and algebra. In 1830 he solved $f(x) = 0$
(mod p) for an irreducible polynomial $f(x)$ by introducing a symbol j
as a 'solution' to $f(x) = 0$ as for complex numbers. This gives the
Galois field GF(p). Galois's work made an important contribution to
the transition from classical to modern algebra.

In 1830 he joined the revolutionary movement. The following year
he was arrested twice, and served a nine month prison sentence for
participating in a republican rally. Shortly after his release, he was
killed in a duel at the age of 21 shortly after his release. Dramatically,
the night before, he had hurriedly written out his discoveries on group
theory. The resulting paper on what is now Galois theory involved
groups formed from the arrangements of the roots of equations and
their subgroups, which he embedded into each other rather like Chinese

boxes.

Ernst Eduard Kummer (1810 - 1893) was born in Sorau (now Zary, Poland) and studied at Halle. Kummer taught for one year (1833) at Sorau and then for ten years at Liegnitz. He was professor at Breslau 1842 - 55. In 1855 Dirichlet's chair at the University of Berlin became vacant and Kummer was appointed, with a dual appointment at the Berlin War College. His main achievement was the extension of results about the integers to other integral domains by introducing the concept of an ideal. In 1843 Kummer, realizing that attempts to prove Fermat's Last Theorem broke down because the unique factorization of integers did not extend to other rings of complex numbers, he attempted to restore the uniqueness of factorization by introducing 'ideal' numbers.
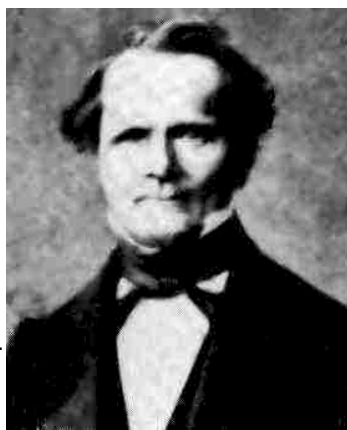
Kummer studied the surface, now named after him, based on the singular surface of the quadratic line complex. He also worked on extending Gauss's work on hypergeometric series, giving developments that are useful in the theory of differential equations.

Julius Wilhelm Richard Dedekind (1831 - 1916) was another mathematician of the brilliant German school of the 19th century. His major contribution was a redefinition of irrational numbers in terms of Dedekind cuts. He introduced the notion of an ideal which is fundamental to ring theory. Dedekind received his doctorate from Göttingen in 1852. He was the last pupil of Gauss. His major contribution was a major redefinition of irrational numbers in terms of Dedekind cuts. He published this in *Stetigkeit und Irrationale Zahlen* in 1872.

His analysis of the nature of number and mathematical induction,

including the definition of finite and infinite sets and his work in number theory, particularly in algebraic number fields, is of major importance.

In 1879 Dedekind published *die Theorie der ganzen algebraischen Zahlen* in which he introduced the notion of an ideal which is fundamental to ring theory. Dedekind formulated his theory in the ring of integers of an algebraic number field. The general term 'ring' was introduced by Hilbert. Dedekind's notion was extended by Hilbert and Emmy Noether to allow the unique factorization of integers into prime powers to be generalized to other rings.

Dedekind's brilliance consisted not only of the theorems and concepts that he studied but, because of his ability to formulate and express his ideas so clearly, he introduced a whole new style of mathematics that been a major influence on mathematicians ever since.

Joseph Liouville (1809 - 1881) was born in St Omer, Pas - de - Calais, and studied in Paris at the Ecole Polytechnique and the Ecole des Ponts et Chauss é es. He became professor at the École Polytechnique in Paris in 1833. In 1836 he founded a mathematics journal *Journal de Mathématiques Pures et Appliques*. Liouville investigated criteria for integrals of algebraic functions to be analytic during the period 1832-33. This led on to his proof of the existence of a transcendental number in 1844 when he constructed an infinite class of such numbers. In collaboration with **Jacques Charles - François Sturm** (1803 - 1855), Liouville published papers in 1836 on vibration, thereby laying the foundations of the theory of linear differential equations — Sturm-Liouville theory. It has major importance in mathematical physics. Liouville contributed to differential geometry studying conformal transformations. He proved a major theorem concerning the measure preserving property of Hamiltonian dynamics. The result is of fundamental importance in statistical mechanics and measure theory.

He wrote over 400 papers in total and was a major influence in bringing Galois' work to general notice when he published this work

in 1846 in his Journal.

Charles Hermite (1822 - 1901) was born in Lorraine, France (though some sources indicate the place of birth to be Dieuze). Even though he had distinguished himself as an original mathematician by the age of twenty, not been a good performing student on examinations, he had to spend five years working for his B.Sc. which he received in 1848. He first held a monor post at the École Polytechnique. Later he held posts at the Collége de France, École Normale Supérieure and the Sorbonne. His work in the theory of functions includes the application of elliptic functions to the general equation of the fifth degree, the quintic equation. In 1873 he published the first proof that e is a transcendental number.

Hermite applied elliptic functions to the quintic equation. He published the first proof that e is a transcendental number.

Hermite was also a major figure in the development of the theory of algebraic forms and the arithmetical theory of quadratic forms. He studied the representation of integers, now called Hermitian forms. His solution of the general quintic equation appeared in Sur la résolution de léquation du cinquième degré (1858; "On the Solution of the Equation of the Fifth Degree"). An encouraging mathematician, many late 19th-century mathematicians first gained recognition for their work largely through his efforts.
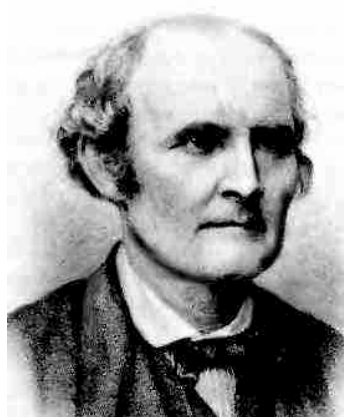
Using method's similar to those of Hermite, Lindemann established in 1882 that π was also transcendental. Hermite is known also for a number of mathematical entities that bear his name, Hermite polynomials, Hermite's differential equation, Hermite's formula of interpolation and Hermitian matrices. Henri Poincaré is the best known of Hermite's students.

Carl Louis Ferdinand von Lindemann (1852 - 1939) was the first to prove that π is transcendental. He studied under Klein at Erlangen and, under Klein's direction, wrote a thesis on non-Euclidean line

geometry and its connection with non-Euclidean kinematics and statics.

Lindemann became professor at the University of Königsberg in 1883. Hurwitz and Hilbert both joined the staff at Königsberg while he was there. In 1893 Lindemann accepted a chair at the University of Munich where he was to remain for the rest of his career. Lindemann's main work was in geometry and analysis. He is famed for his proof that π is transcendental, discussed in an earlier chapter.

Arthur Cayley (1821 - 1895), one of the most prolific mathematicians of his era and of all time, born in Richmond, Surrey, and studied mathematics at Cambridge. For four years he taught at Cambridge having won a Fellowship and, during this period, he published 28 papers in the Cambridge Mathematical Journal. A Cambridge fellowship had a limited tenure so Cayley had to find a profession. He chose law and was admitted to the bar in 1849. He spent 14 years as a lawyer, but Cayley always considered it as a means to make money so that he could pursue mathematics. During these 14 years as a lawyer Cayley published about 250 mathematical papers! Part of that time he worked in collaboration with **James Joseph Sylvester**[11] (1814-1897), another lawyer. Together, but not in collaboration, they founded the algebraic theory of invariants 1843.

In 1863 Cayley was appointed Sadleirian professor of Pure Mathematics at Cambridge. This involved a very large decrease in income. However Cayley was very happy to devote himself entirely to mathematics. He published over 900 papers and notes covering nearly every aspect of modern mathematics.

The most important of his work is in developing the algebra of matrices, work in non-euclidean geometry and n-dimensional geometry.

---

[11] In 1841 he went to the United States to become professor at the University of Virginia, but just four years later resigned and returned to England. He took to teaching private pupils and had among them Florence Nightengale. By 1850 he bacame a barrister, and by 1855 returned to an academic life at the Royal Military Academy in Woolwich, London. He returned to the US again in 1877 to become professor at the new Johns Hopkins University, but returned to England once again in 1877. Sylvester coined the term 'matrix' in 1850.

Importantly, he also clarified many of the theorems of algebraic geometry that had previously been only hinted at, and he was among the first to realize how many different areas of mathematics were linked together by group theory.

As early as 1849 Cayley a paper linking his ideas on permutations with Cauchy's. In 1854 Cayley wrote two papers which are remarkable for the insight they have of abstract groups. At that time the only known groups were groups of permutations and even this was a radically new area, yet Cayley defines an abstract group and gives a table to display the group multiplication.

Cayley developed the theory of algebraic invariance, and his development of n-dimensional geometry has been applied in physics to the study of the space-time continuum. His work on matrices served as a foundation for quantum mechanics, which was developed by Werner Heisenberg in 1925. Cayley also suggested that euclidean and non-euclidean geometry are special types of geometry. He united projective geometry and metrical geometry which is dependent on sizes of angles and lengths of lines.

Heinrich Weber (1842 - 1913) was born was born and educated in Heidelberg, where he became professor 1869.[12] He then taught at a number of institutions in Germany and Switzerland. His main work was in algebra and number theory. He is best known for his outstanding text *Lehrbuch der Algebra* published in 1895.

Weber worked hard to connect the various theories even fundamental concepts such as a field and a group, which were seen as tools and not properly developed as theories in their contained in his *Die partiellen Differentialgleichungen der mathematischen Physik* 1900 - 01, which was essentially a reworking of a book of the same title based on lectures given by Bernhard Riemann and written by Karl Hattendorff.

Algebra and Number Theory[13]

9 Exercises

1. Consider the **arithmetic progression** 0, b, $2b$, $3b$, ... Suppose $(d, b) = 1$.[14] Prove that the series $\{kb \pmod{d}\}$, $k = 1, 2, \ldots$, contains d different residues. (Hint. Prove that the series $\{kb(\bmod d)\}$, $k = 1, 2, \ldots, d$ contains d different residues.

2. For any integers a, b, and m show that $ab(\bmod m) = [a(\bmod m)\, b(\bmod m)](\bmod m)$.

3. Given an argument that when constrained to a fixed mantissa arithmetic, that every mathematical formula proposed to generate random numbers must cycle.

4. The **floor** function takes any non-integer number to the next smaller interger, while leaving intergers unchanged. For example, $\lfloor 3 \rfloor = 3$, $\lfloor -3.19 \rfloor = -4$, $\lfloor 7.939 \rfloor = 7$. Using the floor function, give a formula for the middle-square algorithm.

5. Write a short biographical essay on the professional life of John von Neumann.

6. How can you utilize random numbers in the classroom to illustrate some mathematical concept?

7. Let $s = \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{4} + \frac{1}{9} + \frac{1}{10} + \frac{1}{12} + \frac{1}{15} + \frac{1}{16} + \cdots$ be the sum of the reciprocals of all numbers with primes factors 2, 3, and 5. Prove Euler's formula in the special case, that $\prod_{p=2,3,5} \frac{1}{1-\frac{1}{p}}$

8. Compute $\varphi(25)$, $\varphi(32)$, and $\varphi(100)$.

9. Show that $\varphi(2n) = \varphi(n)$, for every odd integer n.

10. Prove that if the integer n has r distinct primes, the $2^2 | \varphi(n)$.

---

[14]This means d and b are relatively prime.

11. Prove that the Euler φ-function is multiplicative. That is, $\varphi(mn) = \varphi(m)\varphi(n)$. (This may prove difficult.)

12. Show that there is no odd perfect number which is the product of just two odd numbers ($\dot{\iota}1$).

13. Prove the formula $\ln(1 - x^2) = -\left(x + \frac{x^2}{2} + \frac{x^3}{3} + \frac{x^4}{4} + \cdots\right)$

14. Express $\sqrt{i}$ in the form $a + ib$.

15. Classify which numbers of the form $\sqrt{p}^{\sqrt{q}}$ are transcendental.

16. Use the classical result $e^{i\pi} = -1$ and Gelfond's theorem to establish that e cannot be algebraic.

17. Note two example of aspects of number theory that required further algebraic development ot solve.

18. Explain the development of algebra as a consequence of symbolism. (Hint. What aspects of 19th century developments would have been impossible without symbolism?)

19. Write a short essay on the impact of number theory on the development of algebra.