CHAPTER I

Number theory

1.1. Introduction.

Ladder algebra, which is described in [Ad14] is developed and includes a discussion of the uncountable continuum hypothesis, UCH, proving its incompatibility with the countability of the rational numbers, $\mathbb{Q}$, and a rule of induction for sets. We introduce real numbers with a transfinite number of terms. A comparison of our account with that of P. J. Cohen is given in chapter III. Complex numbers are applied to ladder analysis where we give examples employing the standard protocol, which defines ordinal infinity, and the strict transfer principle.

Fourier series, the complex Cauchy integral formula and the hyperintricate Cauchy-Riemann equations are represented in volume I, chapter VII and are extended here to the l-adic case.

1.2. Finite arithmetic.

1.3. Ladder algebra and transcendence.

If we consider $\sqrt{2}$, then this is not a rational number, for if it were $\frac{m}{n}$, with m and n natural numbers divided out to be in lowest terms, then m and n cannot both be even. So assuming

$$\sqrt{2} = \frac{m}{n}, \tag{1}$$

if m and n were both odd, then on squaring both sides of (1), multiplying by n^2 gives an odd number, m^2, equal to an even number, $2n^2$. If m is in any situation even, say $2m'$, then n^2 is $2m'^2$, so n^2 is even and so is n, a contradiction. Finally, if m is odd and n is even, then m^2 is even, which contradicts its assumption.

Our point of view can be that $\sqrt{2}$ is irreducible to a rational number, in the same way $\sqrt{-1}$ is. For linear induction and its preferred evaluation, or the linear probability evaluation, I am unclear what values, if any, can be assigned.

However, if $\sqrt{2}$ was a rational number plus an infinitesimal, with m, n natural numbers, and k a Eudoxus number, then

$$\sqrt{2} = \frac{m}{n} + k\boldsymbol{\varepsilon},$$

and on squaring

$$2 - \left(\frac{m}{n}\right)^2 = 2k\frac{m}{n}\boldsymbol{\varepsilon} + k^2\boldsymbol{\varepsilon}^2,$$

where the left hand side is a rational number, which contains on the right infinitesimals multiplied by Eudoxus numbers, which is a contradiction.

We have seen that if we represent $\sqrt{2}$ by

$$\sqrt{2} = a + \frac{b}{2} + \frac{c}{2^2} + \cdots + \frac{d}{2^n} + \cdots, \tag{2}$$

then a, b, ... , d can be represented in a consistent allocation (mod 2), that is, a, b, ... , d are all either even (0) or odd (1), and by the previous discussion of the principle of induction, if there is no infinitesimal term to the right of (2) the property of their sum (mod 2) exists. For

ladder numbers, $\mathbf{\Omega} = 0 \pmod 2$ is a consistent type of preferred evaluation, and $\boldsymbol{\varepsilon} = \mathbf{\Omega}^{-1} = 0 \neq 1 \pmod 2$ is also.

Definition 1.4.1.The transfinite natural numbers $\mathbb{M}_t$, where t belongs to an index set which also satisfies the properties below, satisfy the following axioms

(1) $1 \in \mathbb{M}_t$
(2) for every $m \in \mathbb{M}_t$ there exists an S(m) interpreted as $(m + 1) \in \mathbb{M}_t$
(3) there is no number $0 \in \mathbb{M}_t$ with $S(0) = 1$
(4) for two numbers $m, n \in \mathbb{M}_t$, $S(m) = S(n)$ implies $m = n$
(5) $\mathbb{M}_t \subset \mathbb{M}_{S(t)}$
(6) $\mathbb{M}_t$ is not bijective to $\mathbb{M}_{S(t)}$
(7) there is no proper subset $\mathbb{M}'$ with the above properties satisfying $\mathbb{M}_t \subset \mathbb{M}' \subset \mathbb{M}_{S(t)}$
(8) (induction) a subset of $\mathbb{M}_t$ containing 1 and S(m) whenever $m \in \mathbb{M}_t$ is $\mathbb{M}_t$.

Notation 1.4.2. $\mathbb{M}_t$ with the number 0 appended to it is denoted by $\mathbb{M}_{tU0}$.

The preferred evaluation under linear induction defined in volume I, chapter I, section 8 of the sets $\mathbb{M}_t$ is even.

Definition 1.4.3. The *transrational numbers* $\mathbb{Q}_t$, $t \neq 1$, are the set of numbers $\pm m/n$ where $m \in \mathbb{M}_{tU0}$ and $n \in \mathbb{M}_t$.

Further, there exist numbers (1/m) which are smaller than any countable infinitesimal.

Definition 1.4.4. A *gaussian integer* (complex integer) is a number $x + iy \in \mathbb{Z}_G$ where i is the imaginary number $\sqrt{-1}$ and x and y are integers, that is, $\{x, y\} \in \mathbb{Z}$.

Definition 1.4.5. An *algebraic number* $x \in \mathbb{A}$ satisfies an additive polynomial equation in x

$$p_n x^n + p_{n-1} x^{n-1} + ... + p_0 = 0$$

of degree $n \in \mathbb{N}_{U0}$ with coefficients $p_n \in \mathbb{N}_{\neq 0}$, $p_k \in \mathbb{Z}$ for $k < n$.

Definition 1.4.6. A *gaussian algebraic number* $x \in \mathbb{A}_G$ satisfies an additive polynomial equation in x

$$q_n x^n + q_{n-1} x^{n-1} + ... + q_0 = 0$$

of degree $n \in \mathbb{N}_{U0}$ with gaussian integer coefficients $q_n \in \mathbb{N}_{\neq 0}$, $q_k \in \mathbb{Z}_G$ for $k < n$.

Real and complex transcendental numbers may be generated by series with a summation of terms over $\mathbb{N}$ or more generally over $\mathbb{M}_t$.

Definition 1.4.7. *Transgaussian, transalgebraic and transgaussian algebraic numbers* satisfy the same type of conditions for gaussian, algebraic or gaussian algebraic numbers, with $\mathbb{N}$ everywhere substituted by the set of transnatural numbers, $\mathbb{M}_t$.

Definition 1.4.8. A *transcomplex number* $\mathbb{C}_t$ is a number which is possibly not algebraic satisfying the axioms for a field.

Definition 1.4.9. A *transreal number* $\mathbb{R}_t$ is a number which is possibly not algebraic, which has no components containing $i = \sqrt{-1}$ irreducibly, and satisfies the axioms for a field.

Thus when t = 1, the transrational numbers are called *rational numbers*, the transreal numbers are called *real numbers* and the transcomplex numbers are called *complex numbers*.

Proposition 1.4.7. *If* x *is transalgebraic and* w *is transcomplex, then* xw *is transcomplex.*

Definition 1.4.8. If v and w are transcomplex then v and w are *additively independent* if there exists no transalgebraic number x such that

$v + xw = 0$.

Definition 1.4.9. If v and w are transcomplex then v and w are *multiplicatively independent* if there exists no transalgebraic number x such that

$xvw = 1$.

Definition 1.4.10. If u, v and w are transcomplex then they are *ring independent* if there exist no transalgebraic numbers x and y such that

$(u + xv)w = y$.

Theorem 1.4.11. u, v *and* w *are mutually ring independent if and only if they are additively and multiplicatively independent*. □

We may extend these considerations to superexponential operations, in particular to the superrings of volume I, chapter IV.

Definition 1.4.12. A summation S of terms over $\mathbb{M}_t$ is *convergent over* $\mathbb{M}_t$ *with respect to the partially ordered function* f if there exists a bounded term b so that the function f(b) of b is greater than S.

Possible transcendental numbers may satisfy polynomial equations of degree $n \notin \mathbb{Z}$, for example of non-finite degree.

With no ladder numbers, the definition of the empty set in mZFC and its properties under induction previously discussed show it is possible for finite rational numbers to have empty infinitesimal sets whilst at the same time infinite sequences of rationals can contain sets of infinitesimals in the complement of ∅, satisfying the same predicate. We refer to *Innovation in mathematics* [Ad14] for other work showing that representable infinitesimals exist. □

The transcendental number π may be represented by

$$\pi = q + \frac{r}{p} + \frac{s}{p^2} + \cdots + \frac{t}{p^n} + \cdots \tag{3}$$

Since practical evaluations of π are generated by countable algorithms and in no other way, we are justified in representing π by a collection of numbers differing by a Eudoxus number times an infinitesimal

$$\pi^* = q + \frac{r}{p} + \frac{s}{p^2} + \cdots + \frac{t}{p^n} + \cdots + m\boldsymbol{\varepsilon}. \tag{4}$$

In the same way as it is possible to change the base point of a vector in a vector space, it is possible to change the value of m in (4). For instance, we could have $m = 0$. For this value of π at $m = 0$, its evaluation (mod p^n) is possible if and only if we ignore subsequent terms in the series which relative to p^n contain terms $\frac{u}{p^v}$, where the denominator is equivalent to dividing by zero (mod p^n). However, it is possible to evaluate an approximation to π (mod p), and this holds for fractions in p for all primes. The limit of this fraction differs from the selected value of π by at most an infinitesimal. □

We can extend this discussion and introduce the hypothesis that $\sqrt{2}$ and π are *real numbers* defined by at most transfinite polynomials.

Remark 1.4.13. In this text we will deal with possibly nonconvergent series invariant under linear induction defined in volume I, chapter I, section 8. This linear induction may be

defined for a transfinite number of elements, but each evaluation block must be proved invariant by an induction procedure on blocks which terminates finitely. □

We mention an application. The proof of the general Riemann hypothesis then proceeds as an extension of the case for 'local function fields'. □

1.4. The Goodwin bijection.

As mentioned by Roger Goodwin in a conversation about a mathematical problem not otherwise mentioned in this work, we can consider maps from circles to parabolas. In a more general context we can put this proposition in the following way.

We may wish to consider the congruence, or clock, arithmetic generated by

$$e^{2\pi i/m}$$

with $m \in \mathbb{M}_t$, or otherwise we may wish to consider a real number m. This has a mapping to a circle in complex coordinates x and y given either by the compact representation

$$xx^* + yy^* = rr^* \qquad (1)$$

with x*, y* and r* the complex conjugates of x, y and r respectively, or as containing

$$x^2 + y^2 = r^2. \qquad (2)$$

There is a sense in which we will use it that the representations of the varieties (1) and (2) are algebraic. Indeed we met in [Ad15], chapter XI, substitutions of type

$$x = z + p,$$
$$y = z + q. \qquad (3)$$

For example equation (2) now becomes

$$2z^2 + 2(p + q)z + p^2 + q^2 – r^2 = 0,$$

which we might represent as the quadratic equation in additive format

$$z^2 + az + b = 0, \qquad (4)$$

with $a = (p + q)$ and $b = [p^2 + (a – p)^2 – r^2]/2 = p^2 – ap + (a^2 – r^2)/2$, so that (4) has the standard solution as a quadratic equation. From this point of view, a circle is transalgebraic.

We now have the situation where we may posit that transcomplex numbers exist, but from the models given no standard examples of the above type to generate them. □

1.5. l-adic numbers.

1.6. l-adic Fourier series.

1.7. Gauss, Ramanujan and Kloosterman sums. [HW79]

A function g(n) is *multiplicative* when the g.c.d. of n and n′ is 1 implies

$$g(nn') = g(n)g(n'). \qquad (1)$$

We will write e[t] for $e^{2\pi it}$. Then

$$e[m/n] = e[m'/n]$$

if and only if $m = m' \pmod n$.

Gauss's sum is defined as

$$S(m, n) = \sum_{k=0}^{n-1} e^{2\pi i k^2 m/n} = \sum_{k=0}^{n-1} e\left[\frac{k^2 m}{n}\right], \qquad (2)$$

and because for any u

$$e\left[\frac{(k+un)^2 m}{n}\right] = e\left[\frac{k^2 m}{n}\right],$$

we obtain whenever $k = k' \pmod n$

$$e\left[\frac{k^2 m}{n}\right] = e\left[\frac{k'^2 m}{n}\right],$$

so that we are able to put

$$S(m, n) = \sum_{k(n)} e\left[\frac{k^2 m}{n}\right],$$

where by k(n) we mean that k runs through all residues (mod n). If the meaning is clear we will usually shorten k(n) in this sum to k.

Lemma 1.7.1. *If the g.c.d. of* n *and* n′ *is* 1, *and* a *runs through all residues* (mod n), *whereas* a′ *runs through all residues* (mod n′), *then* a′n + an′ *runs through all residues* (mod nn′).

Proof. The number of (a′n + an′) is nn′, and if

$$a_1'n + a_1n' = a_2'n + a_2n'$$

this implies

$$a_1n' = a_2n' \pmod n,$$

giving

$$a_1 = a_2 \pmod n.$$

Likewise

$$a'_1 = a'_2 \pmod{n'},$$

so that all these nn′ numbers differ (mod nn′). □

Corollary 1.7.2. *If the g.c.d. of* n *and* n′ *is* 1, *then* a *runs through all residues coprime to* n *and* a′ *runs through all residues coprime to* n′ *if and only if* a′n + an′ *runs through all residues coprime to* nn′.

Proof. (a′n + an′) is coprime to nn′ and therefore to n and n′ separately, so an′ is coprime to n and a′n coprime to n′, so a is coprime to n and a′ is coprime to n′, and conversely. □

Theorem 1.7.3. *If the g.c.d. of* n *and* n′ *is* 1, *then*

$$S(m, nn') = S(mn', n)S(mn, n').$$

Proof. Let k, k′ run through all the residues for (mod n) and (mod n′) respectively, so by the previous lemma

$$K = kn' + k'n$$

runs through all residues (mod nn′). Further,

$$mK^2 = m(kn' + k'n)^2 = mk^2n'^2 + mk'^2n \pmod{nn'},$$

so that

$$\begin{aligned} S(mn', n)S(mn, n') &= \sum_k e\left[\frac{k^2 mn'}{n}\right] \sum_{k'} e\left[\frac{k'^2 mn}{n'}\right] \\ &= \sum_{k,k'} e\left[\frac{k^2 mn'}{n} + \frac{k'^2 mn}{n'}\right] = \sum_{k,k'} e\left[\frac{m(k^2 n'^2 + k'^2 n^2)}{nn'}\right] \\ &= \sum_K e\left[\frac{mK^2}{nn'}\right] = S(m, nn'). \square \end{aligned}$$

Ramanujan's sum is

$$c_q(m) = \sum_{k^*(q)} e\left[\frac{km}{q}\right], \tag{3}$$

where k*(q) indicates that k runs through residues coprime to q. On occasion we will replace k*(q) by k.

Using the primitive complex qth root of unity $\omega_q = e^{2\pi iq}$, so that ${\omega_q}^q = 1$, we can rewrite Ramanujan's sum as

$$c_q(m) = \sum_k \omega^m.$$

Theorem 1.7.4. *If the g.c.d. of* q *and* q′ *is* 1, *then*

$$c_{qq'}(m) = c_q(m)c_{q'}(m).$$

Proof. By corollary 1.4.2

$$c_q(m)c_{q'}(m) = \sum_{k,k'} e\left[m\left(\frac{k}{q} + \frac{k'}{q'}\right)\right] = \sum_{kk'} e\left[\frac{m(kq'+k'q)}{qq'}\right] = c_{qq'}(m). \square$$

Lemma 1.7.5. *If the g.c.d. of* k *and* n *is* 1, *the congruence*

$$ky = ky' \pmod n$$

holds if and only if

$$y = y' \pmod n.$$

Note that we cannot infer in general that $ky = ky' \pmod n$ implies $y = y' \pmod n$, since

$$2 \times 3 = 2 \times 6 \pmod 6,$$

but

$$3 \neq 6 \pmod 6.$$

Proof. $k(y - y') = 0 \pmod n$. Since $k \neq 0 \pmod n$, $y - y' \neq 0 \pmod n$ is a contradiction. $\square$

Corollary 1.7.6. *If* y, y′, ... are all incongruent residues (mod n) and the g.c.d. of k and n is 1, then ky, ky′, ... are also all incongruent residues.

Proof. By induction on lemma 1.4.5. $\square$

Lemma 1.7.7. *If the g.c.d. of* k *and* n *is* 1, *the congruence*

$$ky = c \pmod n$$

has exactly 1 *solution.*

Proof. This is a corollary of 1.4.6, since if there were more solutions than one, for two distinct values of y there would be a congruence relation. But there is at least one solution, since there exists a c with ky = c, and the ky are a complete set of incongruent residues. $\square$

Kloosterman's sum is

$$S(u, v, n) = \sum_j e\left[\frac{uj+vk}{n}\right], \tag{4}$$

in which j runs through all residues coprime to n, and we define k by

$$jk = 1 \pmod n. \tag{5}$$

Lemma 17.2.7 shows equation (5) can be satisfied.

Theorem 1.7.8. *If the g.c.d. of* n *and* n′ *is* 1, *then*

$$S(u, V, n) = S(u, v, n)S(u, v', n'),$$

where

$$V = vn'^2 + v'n^2.$$

Proof. On putting

$$jk = 1 \pmod n,\ j'k' = 1 \pmod{n'},$$

we obtain

$$S(u, v, n)S(u, v', n') = \sum_{j,j'} e\left[\frac{uj+vk}{n} + \frac{uj'+vk'}{n'}\right]$$

$$= \sum_{j,j'} e\left[u\left(\frac{jn'+j'n}{nn'}\right) + \frac{vkn'+v'k'n}{nn'}\right]$$
$$= \sum_{j,j'} e\left[\frac{uJ+K}{nn'}\right], \qquad (6)$$

in which

$J = jn' + j'n$, $K = vkn' + v'k'n$.

We wish to show that

$K = VJ' \pmod{nn'}$, (7)

where J' satisfies

$JJ' = 1 \pmod{nn'}$,

so that equation (6) becomes

$$S(u, v, n)S(u, v', n') = \sum_J e\left[\frac{uJ+K}{nn'}\right] = S(u, V, nn').$$

But

$(j'n + jn')J' = JJ' = 1 \pmod{nn'}$,

giving

$jn'J' = 1 \pmod{n}$, $n'J' = jkn'J' = k \pmod{n}$,

and therefore

$n'^2J' = n'k \pmod{nn'}$.

Correspondingly

$n^2J' = nk \pmod{nn'}$,

so that we find

$VJ' = (vn'^2 + v'n^2)J' = vn'k + v'nk = K \pmod{nn'}$

and this is just equation (7), which we wished to prove. □

1.8. The Rogers-Ramanujan identities.

We can exhibit any square m^2 as

$m^2 = 1 + 3 + 5 + ... + (2m - 1)$.

If we now take a partition of $n - m^2$ into m parts at most, with the parts in descending order, we obtain a partition of n into parts without repetitions or sequences, or parts whose minimal difference is 2.

On the other hand, the right hand side enumerates partitions into numbers of the form $5m + 1$ and $5m + 4$. Hence we obtain the purely combinatorial theorem

Theorem 1.8.1. *The number of partitions of* n *with minimal difference* 2 *is equal to the number of partitions into parts of the form* $5m + 1$ *and* $5m + 4$.

From this we will be able to prove

Theorem 1.8.2.

$$1 + \frac{x}{1-x} + \frac{x^4}{(1-x)(1-x^2)} + \frac{x^9}{(1-x)(1-x^2)(1-x^3)} + \cdots$$
$$= \frac{1}{(1-x)(1-x^6)\cdots(1-x^4)(1-x^9)},$$

which can be expressed as

$$1 + \sum_1^\infty \frac{x^{m^2}}{(1-x)(1-x^2)\cdots(1-x^m)} = \prod_0^\infty \frac{1}{(1-x^{5m+1})\cdots(1-x^{5m+4})}.$$

There is a similar theorem to 1.7.1.

Theorem 1.8.3. *The number of partitions of* n *into parts not less than* 2, *and with minimal difference* 2 *is equal to the number of partitions into parts of the form* $5m + 2$ *and* $5m + 3$.

We can prove this equivalence in the same way, starting from the identity

$m(m + 1) = 2 + 4 + 6 \ldots + 2m.$

This leads to the analogue of theorem 1.7.2.

Theorem 1.8.4.

$$1 + \frac{x^2}{1-x} + \frac{x^4}{(1-x)(1-x^2)} + \frac{x^{12}}{(1-x)(1-x^2)(1-x^3)} + \cdots = \frac{1}{(1-x^2)(1-x^7)\cdots(1-x^3)(1-x^8)},$$

which can be put in the form

$$1 + \sum_1^\infty \frac{x^{m(m+1)}}{(1-x)(1-x^2)\cdots(1-x^m)} = \prod_0^\infty \frac{1}{(1-x^{5m+2})\cdots(1-x^{5m+3})}.$$

The interest of the formulas arises from the unexpected part played by the number 5.

It is natural to ask if there is any proof by elementary methods, and an elaborate proof was found this way by Schur. The theorems were first discovered independently by Rogers and Ramanujan, and we will provide here the proof by Rogers.

1.9. Theta functions.