BOLYAI SOCIETY
MATHEMATICAL STUDIES, 11

Paul Erdős and his Mathematics. II,
Budapest, 2002, pp. 555–564.

You Can Enter Cantor's Paradise!

S. SHELAH*

The intention is to present naive cardinal arithmetic for wide audience: this is based on my lecture for the Bolyai prize. I will try to use a spiralic presentation returning to the same points on higher levels hence repeating ourselves, so that a reader lost somewhere, will not go away empty handed. Also I will assume essentially no particular knowledge and I will say little on the history to which many great mathematicians contributed.

This is dedicated to Paul Erdős, who, I would like to believe, would have been well pleased by the theorems.

1. Hilbert's First Problem

Recall (Cantor):

- We say that two sets A, B are *equinumerous* (or *equivalent*) if there is a one-to-one and onto mapping from A onto B;
- The **C**ontinuum **H**ypothesis, CH, is the following statement:
  every infinite set of reals is either equinumerous with the set $\mathbb{Q}$ of rational numbers, or is equinumerous with the set $\mathbb{R}$ of all reals;
- For a set X, let $\mathcal{P}(X)$ denote its power set, i.e., the set of all subsets of X.

  The **G**eneralized **C**ontinuum **H**ypothesis, GCH, is the statement asserting that for every infinite set X, every subset Y of the power set

* Partially supported by Israel Science Foundation, founded by the Israeli Academy of Sciences and Humanities, pub E25 in the author's list.

$\mathcal{P}(X)$ is either equinumerous with a subset of X, or is equinumerous with $\mathcal{P}(X)$ itself.

I think this problem is better understood in the context of:

1.1. Cardinal Arithmetic. Recall (Cantor), that we call two sets A, B equivalent (or equinumerous) if there is a one-to-one mapping from A onto B; the number of elements of A is the equivalence class of A denoted by $|A|$, we call it also *the power* or *the cardinality* of A. Having defined infinite numbers, we can naturally ask ourselves what is the natural meaning of the arithmetical operations and the order. There can be little doubt concerning the order:

- $|A| \leq |B|$ iff A is equivalent to some subset of B.

We know that

- any two infinite cardinals are comparable so it is really a linear order
- any cardinal λ has a successor λ^+, which means that
- $\lambda < \mu \Leftrightarrow \lambda^+ \leq \mu$.

Well, but what about the arithmetical operations? There are natural definitions for the basic operations:

- addition (such that $|A \cup B| = |A| + |B|$ when A, B are disjoint),
- multiplication (such that $|A \times B| = |A| \times |B|$),
- exponentiation (such that $|A|^{|B|} = |{}^B A|$, where ${}^B A = \{f : f$ a function from A to $B\}$).

A mathematician is allowed to choose his definitions and give them "nice" names, but do those operations have any laws? Are there interesting theorems about them? The answer is clear cut: all the usual *equalities* hold, that is, addition and multiplication satisfy the commutative, associative, and distributive laws and their infinite parallels. Also for exponentiation, e.g. $(\lambda^\mu)^\kappa = \lambda^{\mu \times \kappa}$, $\lambda^\mu \times \lambda^\kappa = \lambda^{\mu + \kappa}$. However this does not hold for the inequalities. For every infinite cardinal λ we have $\lambda = \lambda + 1$. This should not surprise us; it is to be expected that allowing infinite number will "cost" us some losses, (as extending $\mathbb{N}$, the integers, to rationals "costs" us the existence of successor and the proof by induction; this is very clear in a posteriory wisdom, of which we all have a lot). Cantor was going around asking: are there more points in the plane than on the line? People answered

him: don't you see that there are? But it is false, the line and the plane are equinumerous.

In fact we can totally understand addition and multiplication, as the following very nice rules holds for infinite numbers:

- $\mu + \lambda = \max(\mu, \lambda)$
- $\mu \times \lambda = \max(\mu, \lambda)$

School children would have loved such arithmetic!

You may wonder: is this not too good? Maybe all infinite numbers are equal so this arithmetic is not so interesting? But Cantor showed that $2^\lambda > \lambda$, meaning in particular that there are more reals than natural numbers; noting that he called the number of natural numbers $\aleph_0$, this is the first infinite cardinal and showed that the number of reals is $2^{\aleph_0}$.

Recall that every infinite number λ has a successor, one bigger than it but smaller or equal to any bigger number, and it is denoted by λ^+.

Now mathematicians tend to conjecture that things are nice and well understood. So, having only two natural operations to increase a cardinal, what is more natural than to conjecture that those two operations, λ^+ and 2^λ are equal. Also mathematicians tend to conjecture either that whatever they cannot prove may fail, or whatever they cannot build counterexample to is true; and being unable to construct an intermediate cardinal between λ and 2^λ (e.g. $\aleph_0$ and $2^{\aleph_0}$) it is natural to conjecture that there is nothing between them. This is

1.2. Hilbert's first problem, general version. The "generalized continuum hypothesis", or GCH, says: for every infinite number μ, its power 2^μ is its successor μ^+.

The interest is that if GCH holds, then not only addition and multiplication are easy, but also exponentiation is easy: for infinite cardinals λ, κ (on $\mathrm{cf}(\lambda)$ see below):

$$\lambda^\kappa = \begin{cases} \lambda & \text{if } \kappa < \mathrm{cf}(\lambda) \\ \max(\kappa^+, \lambda^+) & \text{if } \kappa \geq \mathrm{cf}(\lambda) \end{cases}$$

Dream: Find the laws of (infinite) cardinal exponentiation.

It has been assumed that if we understand cardinal arithmetic, that is (taking for granted the understanding of addition and multiplication) understand the behavior of exponentiation, we will generally understand

set theory much better, and so solve problems from many branches of mathematics in full generality.

2. Proven Ignorance: Showing that we Cannot Know!

The continuum problem: How many real numbers are there?

Cantor proved: There are *more* reals than rationals. ("There is no bijection from $\mathbb{R}$ onto the rationals $\mathbb{Q}$")

Recall that the continuum hypothesis (CH) says: yes, more, but barely. Every set $A \subseteq \mathbb{R}$ is either countable or equinumerous with $\mathbb{R}$.

Gödel proved: Perhaps CH holds.

Cohen proved: Perhaps CH does not hold.

Gödel: CH cannot be refuted. Moreover, the *generalized continuum hypothesis* may hold, in fact it holds if we restrict to the class L of constructible sets ([3]).

This universe L satisfies all the axioms of set theory, and in addition the generalized continuum hypothesis. The class L can be described as the minimal family of sets you absolutely must have as soon as you have all the ordinals = order types of linear orders which are well ordered, i.e., every non empty subset has a first element. We shall not deal with this here, and do not touch on metamathematical matters in general.

Cohen: You cannot prove that all sets are constructible, and you cannot even prove the weaker statement "CH" ([1]).

Cohen discovered the method of *forcing,* and used it to prove this "independence" result; he "fattened" the universe of set theory; not surprising in a posteriory wisdom. Again, this is not our topic.

Easton showed that there are no more rules than the classical ones if we restrict ourselves to the so called regular cardinals (they include $\aleph_0$ and all successor cardinals; the classical laws are: $2^\lambda > \lambda$ and $\mathrm{cf}(2^\lambda) > \lambda$; an infinite cardinal λ is regular if $\mathrm{cf}(\lambda) = \lambda$, on cf see later).

Concerning the remaining cardinals, the so called singulars, completing the theorem for them was thought of as a technical problem. The first such cardinal is $\aleph_\omega = \sum\limits_{n=0,1,2,\ldots} \aleph_n$, where $\aleph_0$ is the number of natural numbers and $\aleph_{n+1}$ is the successor of $\aleph_n$.

Very surprisingly, in the mid-seventies some rules were discovered by Silver ([6]), and by Galvin and Hajnal ([2]). Let $\aleph_{\omega_1}$ be the first cardinal below which there are uncountably (i.e. $> \aleph_0$) many cardinals. Call λ strong limit if $\mu < \lambda \to 2^\mu < \lambda$. If $\aleph_{\omega_1}$ is a strong limit cardinal then below $2^{\aleph_{\omega_1}}$ there are at most $2^{\aleph_1}$ cardinals.

There were more works, but the general opinion was that what is left is just showing fully we cannot prove anything more. E.g. in '86 Leo Harrington told me: *"Cardinal arithmetic? Yes, it had been a great problem, but now ..."* Not clear to me why, even if the only thing left is proving everything is independent, this is not a major problem, but this is irrelevant here. However, I would like to stress that the independence results help us to discover new good theorems by discarding many fruitless directions.

The book ([4]) for which I am honoured by the Bolyai Prize is based on:

Thesis 1 ("Treasures are waiting for you"). *There are many laws of (infinite) cardinal arithmetic concerning exponentiation; they look meager as we have concentrated on 2^λ, but if we deal with relatively small exponent and large base, then there is much to be said.*

I think that though GCH has not been seriously considered as a true axiom, it has influenced the way we thought about the problem, so traditionally set theorists concentrate on 2^λ; but actually it seem reasonable that on the case λ^κ with $\kappa \ll \lambda$ which is closer to finite products (about which we know everything) we will be able to say more.

We wonder: What is the simplest open case of cardinal arithmetic?

Clearly we have to consider countable products i.e with the index set being the set of natural numbers (as finite products are easy), or if you prefer, consider exponentiation of the form $\lambda^{\aleph_0}$,

Now, $\aleph_0$ is the first infinite cardinal (the cardinality of the set $\mathbb{Q}$ of rationals and the cardinality of the set $\mathbb{N}$ of natural numbers), $2^{\aleph_0} = \aleph_0^{\aleph_0}$ is called the continuum, on which we know everything (i.e., we know that we may not know more). Moreover, let $\aleph_1$ be the successor of $\aleph_0$, $\aleph_2$ be the successor of $\aleph_1$ and generally $\aleph_n$ be the n-th uncountable cardinal (i.e $> \aleph_0$). Now it is not hard to prove that $\aleph_n^{\aleph_0} = \max(\aleph_n, 2^{\aleph_0})$.

So the first non trivial case is the (infinite) product of those numbers: $\prod\limits_n \aleph_n$, or equivalently,

(1) what is $\aleph_\omega^{\aleph_0}$?

where $\aleph_\omega$ is the sum of the $\aleph_n$'s.

If the continuum (i.e. $2^{\aleph_0}$) is above all the $\aleph_n$, then this product is equal to the continuum; so assume that the continuum is one of them.

Let $\aleph_{\omega_n}$ be the first cardinal below which there are $\aleph_n$ infinite cardinals.

Theorem 2. $\prod_n \aleph_n < \aleph_{\omega_4}$ *when the product is not* $2^{\aleph_0}$.

You may think this is a typographical error (in fact almost all who saw it for the first time were convinced this is a typographical error) and we still do not know;

Dream/Question: Why the hell is it four? Can we replace it by one? Is 4 an artifact of the proof or the best possible bound?

I think the four looks strange because we are looking at the problems from a not so good perspective.

3. pcf THEORY

Close to my heart is

Thesis 3. *Cardinal arithmetic is loaded with independence results because we ask the "wrong" questions. The "treasures" thesis above is not enough; we should replace cardinality by cofinality, a notion explained below (pcf theory). More fully, the unclarity comes from the interaction of two phenomena: the values of* 2^λ *for* λ *regular on which we know all the rules (see above) and the "cofinality arithmetic" where there is much to be said.*

As an illustration, let us look again at $\aleph_\omega^{\aleph_0}$.

Look at the family $[\aleph_\omega]^{\aleph_0}$ of countable subsets of any set of cardinality $\aleph_\omega$, e.g. $\aleph_\omega$ by the usual convention that $\aleph_\omega$ itself is such a set. It is partially ordered by inclusion. Now, instead of asking about its cardinality as above (we know that the number of countable subsets of $\aleph_\omega$ is $\aleph_\omega^{\aleph_0}$), we **ask** what is the minimal number of members so that any other is included in at least one of them, and we call this number its cofinality, denoted by $\mathrm{cf}\left([\aleph_\omega]^{\aleph_0}\right)$? The theorem quoted above really says

Theorem 4. $\mathrm{cf}\left([\aleph_\omega]^{\aleph_0}, \subseteq\right) < \aleph_{\omega_4}$.

This is meaningful even if the continuum, $2^{\aleph_0}$ is large. This exemplifies that even if one restricts oneself to sets of reals only, set theory is not

changed much and in particular, cardinal arithmetic reinterprets as above (even if we restrict ourselves to simply defined sets of reals (with arbitrary maps)).

We now pay some debts, defining $\mathrm{cf}(\lambda)$ and regular cardinals.

Definition 5.

1. A cardinal number κ is *regular*, if: whenever A is of size κ, $A = \bigcup_{i \in I} A_i$, and all A_i are of smaller cardinality than A, then I must be at least of size κ. *(A set of size κ cannot be written as a union of "few" "small" sets.)*
2. Otherwise κ is called singular; $\mathrm{cf}(\kappa)$ is the size of the smallest set I that can appear in $(*)$ above.
3. For a partial order P let $\mathrm{cf}(P)$, its cofinality, be the minimal cardinal κ such that some subset Q of P of cardinality λ, Q is cofinal in P, i.e. $(\forall x \in P)\ (\exists y \in Q)\ [x \leq_P y]$.

Note that successor cardinals, λ^+, are regular, and the first singular cardinal is $\aleph_\omega$; regular limit cardinals are "large", and the cofinality of any linear order with no last elements is a regular cardinal.

So replacing λ^κ by $\mathrm{cf}\left([\lambda]^\kappa, \subseteq\right)$, where $[\lambda]^\kappa$ is the family of subsets of (a set of cardinality) λ of cardinality $\leq \kappa$, ordered by inclusion, we get a much more "robust" theory, where there are more answers and less "we cannot answer".

In fact, we are driven further. Suppose we consider linear orders L_t for $t \in T$ and assume that $\mathrm{cf}(L_t)$ is bigger than the cardinality of T. We can look at the product, $\prod_{t \in T} L_t$ ordered by: $f \leq g$ iff $(\forall t \in T)(f(t) <_{L_t} g(t))$. This is not a linear order though it is not grossly not so, because the number of factors is small compared to the cofinality of the factors, as assumed. We can try to "localize" as done in other cases in mathematics; e.g. for analysing $\mathbb{Z}$, we may like to analyse what occurs when we have just one prime, so we consider the p–adics; sometime we may deduce information on $\mathbb{Z}$ by looking at all those completions (and the reals). Here we like to make the order linear; so let I be a maximal ideal of the Boolean algebra of subsets of T, then define **linear** order $<_I$ on $\prod_{t \in T} L_t$ by

$$f <_I g \quad \text{iff} \quad \left\{t \in T : \neg\left[f(t) < g(t)\right]\right\} \in I.$$

So $\mathrm{cf}\left(\prod_{t \in T} L_t, <_I\right)$ is a regular cardinal.

Now the product stops giving us a specific result and instead gives us a spectrum:

Definition 6. For a set $\mathfrak{a} = \{\lambda_t : t \in T\}$ of regular cardinals each bigger than the cardinality of T, let $\mathrm{pcf}(\mathfrak{a})$ be the set of cardinals of the form $\mathrm{cf}\left(\prod\limits_{t\in T} L_t, <_I\right)$, where each L_t is a linear order of cofinality λ_t and I is a maximal ideal on the Boolean algebra of subsets of T.

This may remind you of what we do for rings for which decomposition to primes does not behave as in the integers.

Theorem 7. *For $\mathfrak{a} = \{\lambda_t : t \in T\}$ as above:*

(1) $\mathrm{pcf}(\mathfrak{a})$ *is a set of regular cardinals, with at most* $2^{|T|}$ *elements,*

(2) $\mathrm{pcf}(\mathfrak{a})$ *has a largest element denoted by* $\max \mathrm{pcf}(\mathfrak{a})$.

(3) *The cofinality of the partial order* $\prod\limits_{t\in T} \lambda_t$ *is* $\max \mathrm{pcf}(\mathfrak{a})$.

(4) *For every* $\theta \in \mathrm{pcf}(\mathfrak{a})$ *there is a set* $\mathfrak{b}_\theta \subseteq \mathfrak{a}$ *such that: for any maximal ideal I on T the cofinality of* $\left(\prod\limits_{t\in T} \lambda_t, <_I\right)$ *is* $\min\{\theta \in \mathrm{pcf}(\mathfrak{a}) : \mathfrak{b}_\theta \notin I\}$.

Note that in part (1), the number of maximal ideals on T is $2^{2^{|T|}}$, so it gives some information (though not clear if the best possible one). Now this operation, pcf has various rules, from them we can derive the bound $\aleph_{\omega_4}$ for $\mathrm{cf}\left([\aleph_\omega]^{\aleph_0}, \subseteq\right)$.

Such rules are

Rule (local behavior): If $\mathfrak{b}$ is a subset of $\mathrm{pcf}(\mathfrak{a})$ (with both $\mathfrak{a}, \mathfrak{b}$ sets of regular cardinals bigger than the number of members) **then** any member λ of $\mathrm{pcf}(\mathfrak{b})$ belongs to $\mathrm{pcf}(\mathfrak{c})$ for some subset $\mathfrak{c}$ of $\mathfrak{b}$ of cardinality smaller or equal to the cardinality of $\mathfrak{a}$.

Rule (convexity): $\mathrm{pcf}\{\aleph_n : n \geq 1\}$ is an initial segment of the set of successor cardinals.

Rule (continuity): if L is a linear order, $\langle \lambda_i : i \in L\rangle$ is an increasing continuous sequence of cardinals bigger than the cardinality of L and $\lambda = \Sigma_{i\in L}\lambda_i$ and $\mathrm{cf}(\lambda) > \aleph_0$ then for some closed unbounded subset C of L we have $\max \mathrm{pcf}\left(\{\lambda_i^+ : i \in C\}\right) = \lambda^+$.

Now we can explain better the inequality $\mathrm{cf}\left([\aleph_\omega]^{\aleph_0}, \subseteq\right) < \aleph_{\omega_4}$: we look at the set $\mathrm{pcf}\left(\{\aleph_n : n = 1, 2, 3, \ldots\}\right)$, on it we have a linear order (the order on the cardinals) and a closure operation (which is pcf itself),

this is topology of a special kind; we have enough rules such that if the size of the set is too large then we get a contradiction.

4. GCH Revisited

We can interpret pcf theory as a positive solution of Hilbert's first problem, after considering the inherent limitations. We may interpret the problem more strictly "cardinal arithmetic is easy", and we present now a positive solution from [5], discussed in details in its introduction, explaining why reinterpreting GCH under the known restrictions, we can prove that it holds almost always. We define a variant of exponentiation, which gives a different "slicing" of the GCH, specifically represent it as an equality on two cardinals ($\lambda^{\langle\kappa\rangle} = \lambda$), and present a theorem saying that the equality holds "almost always".

Definition 8. (1) For $\kappa < \lambda$ regular let $\lambda^{\langle\kappa\rangle}$, the revised power of λ by κ, be the minimal cardinality of a family $\mathcal{P}$ of subsets of λ of cardinality κ such that any other such set is the union of $< \kappa$ sets from $\mathcal{P}$.

(2) For $\kappa < \lambda$ regular let $\lambda^{[\kappa]}$, the revised power of λ by κ, is the minimal cardinality of a family $\mathcal{P}$ of subsets of λ of cardinality κ such that any other such set is a subset of the union of $< \kappa$ sets from $\mathcal{P}$.

Remark. (1) GCH is equivalent to: for every regular $\lambda > \kappa$ we have $\lambda^{\langle\kappa\rangle} = \lambda$;

(2) Note that $\lambda^{[\kappa]} \leq \lambda^{\langle\kappa\rangle} \leq \lambda^{[\kappa]} + 2^{\kappa}$ hence for $\lambda \geq 2^{\kappa}$ the two revised powers are equal, so below it does not matter which version we use.

(3) So a weak version of GCH is: for "most" pairs (λ, κ) of regular cardinals we have $\lambda^{[\kappa]} = \lambda$.

Notation. *Let* $\beth_0 = \aleph_0$, $\beth_{n+1} = 2^{\beth_n}$, $\beth_\omega = \sum_{n<\omega} \beth_n$.

The Revised GCH Theorem 9. *For any* $\lambda > \beth_\omega$, *for any* $\kappa < \beth_\omega$ *large enough, we have* $\lambda^{[\kappa]} = \lambda$.

REFERENCES

[1] P. J. Cohen, *Set Theory and the Continuum Hypothesis,* Benjamin (1966).

[2] F. Galvin and A. Hajnal, Inequalities for cardinal powers, *Annals of Mathematics,* **101** (1975), 491–498.

[3] K. Gödel, *The consistency of the axiom of choice and the generalized continuum-hypothesis with the axioms of set theory,* Princeton University Press (1940).

[4] S. Shelah, *Cardinal Arithmetic,* Oxford University Press (1994).

[5] S. Shelah, The Generalized Continuum Hypothesis revisited, *Israel Journal of Mathematics,* **116** (2000), 285–321.

[6] J. Silver, On the singular cardinals problem, in: *Proceedings of the International Congress of Mathematics,* Vancouver (1974), volume I, 265–268.

Saharon Shelah

Institute of Mathematics
Hebrew University
Givat Ram
Jerusalem 91904
ISRAEL

e-mail: shelah@math.huji.ac.il