Number Theory and Arithmetic Primitives

Layman approach to Number Theory and Discrete Mathematics

Avneet Singh
SysStruct
sshmatrix@pm.me

ABSTRACT

This paper is an attempt to introduce Number theory to amateur mathematicians and programmers without the use of formal jargon. We will introduce number systems in generic bases and formalise the fundamental operations of addition, subtraction, multiplication and division as self-(anti-)replication operations. We will then advance to the exponential operation and prove its non-commutativity, and attempt to prove a handful of famous conjectures in Number theory by Catalan and Fermat in a non-standard yet intuitive manner. We finally conclude this paper by introducing abstract Complex number systems and their interaction with the set of Natural numbers.

COUNTING STONES

In order to truly arrive at number theory in a natural sense, we'll start from the very basics of it all. Numbers form the building blocks of cryptography and most mathematics, physics and natural sciences. To naturally arrive at numbers and their geometry/topology, we will start from a simple yet abstract example of a collection of some stones circa 20,000 BC. Bob's tribe needs stones to make their flint tools and Bob is one of the stone gatherers; this is Bob's story. During this exercise, please refrain from using numbers as you know it in your subconscious. Try to think like Bob, who has no concept of 1, 2, 3 ⋯ etc.

Consider a collection of stones that are of approximately the same size, shape, weight and texture such that Bob is unable to objectively distinguish any one stone from the rest despite each stone being unique. To quantify this collection of stones into succinct information[1] leads Bob into questioning the nature of this collection. In order to differentiate or distinguish the stones among each other, Bob does the first natural thing – he names each stone. In other words, he assigns a unique label to each stone (see figure 1); such a system is a functioning naming system. Note that there is no condition on actual equivalence among any of the stones, and only an assertion is made that the observer is unable to tell them apart in a describable manner. Using this naming system (𓀀, 𓀁, 𓀂, 𓀃, 𓀄, 𓀅, 𓀆 as labels), Bob can tell someone else what he saw by showing them the labels, assuming that the labels are an agreed upon standard that everyone recognises. Note that Bob can choose any 'ordering' of the labels and the communication system works the same. This works well for everyone until one day Bob finds a massive pile of stones, all of different shapes and sizes in large quantities. The problem is simply that Bob's naming standard has only a finite number of labels and the stones are too many to each correspond to one label. In other words, Bob has run out of labels. In this moment of tryst, Bob realises that he is not limited by the number of labels at all; he can put two labels together and make a new label! Now he just needs to prescribe a method of deciding which two numbers to put together, how to order them etc.

[1] so that Bob can convey information succinctly to others without having to show them the stones

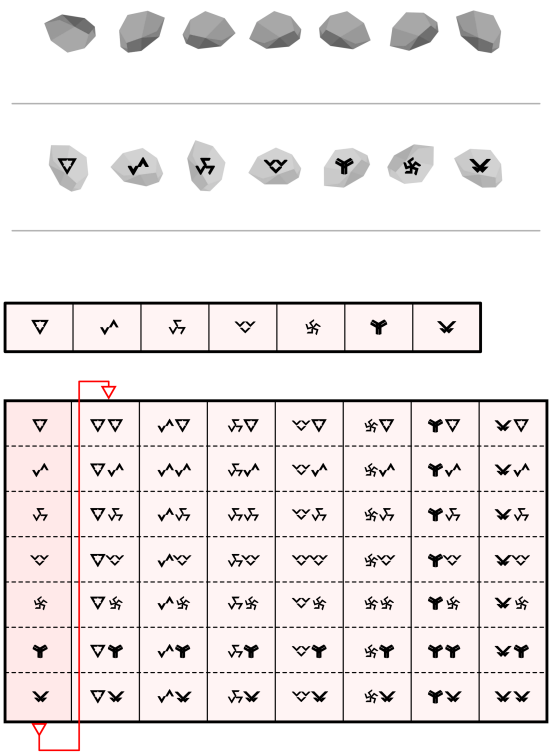

Figure 1: Bob's rudimentary number system

To follow Bob's footsteps, we start from 𓂝 until 𓅓, and then form the next label by joining: the first label with itself (𓂝 𓂝), then first label with second label (𓂝 𓃰), then first label with third label (𓂝 𓄿) and so on until Bob reaches (𓂝 𓅓). Bob proceeds to do this 'cycling' until he reaches (𓅓 𓅓),

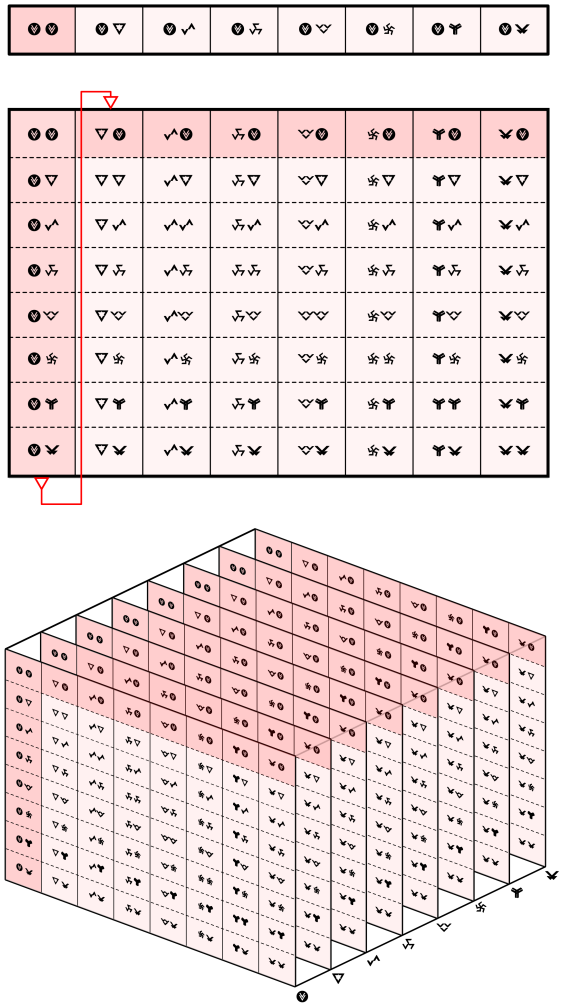

Figure 2: Symmetric number system after appending 𓅮 label

at which point he can describe a lot more stones to his tribe than before. In figure 2, we can visualise Bob's naturally constructed number system. Readers by now may have realised that this is exactly like our native Natural number system with (𓂝, 𓃰, 𓄿, 𓆑, 𓇋, 𓊪, 𓅓) → (1, 2, 3, 4, 5, 6, 7) with no presence of 8, 9 or 0, and it is nothing more. The terminology behind 'natural' is also a lot more intuitive to grasp. We can easily extend this system to count to 𓅓 𓅓 𓅓 or 𓅓 𓅓 𓅓 𓅓 or 𓅓 𓅓 𓅓 𓅓 𓅓, extending up to any number of digits.

In computer science terminology, we know this as base-𓅓 (or base-7) encoding; base-10 is equivalent to the Decimal number system that we commonly use. We can however see that using a very small base quickly leads to overcrowding of digits required to describe any number of stones. On the other hand, a very high base requires keeping a lengthy shared standard among different parties in Bob's ecosystem.

DISCOVERING (+, −, ×, ÷)

In no time, Bob realises that his number system has some very remarkable properties. For instance, one day his friend Alice found ▽√^ stones and Bob found ℨ⩔ stones. Typically he would start placing the combined set of stones on his lookup table (figure 1) and observing when he runs out of stones; then the label corresponding to the last stone is the total count of stones. This is an example of an addition operation that 'combines' or 'adds' or 'sums' the stones of Bob and Alice and counts them; let's represent this by +. Bob soon discovers though that he can be clever instead of following the rudimentary approach, i.e. he can describe the total quantity of stones by breaking the pairs ▽√^ and ℨ⩔ apart into single digits, adding the first and second digits individually across both pairs and then re-attaching (denoted by : operator) the individually summed digits in the same order. For example, ▽√^ + ℨ⩔ → ▽ + ℨ : √^ + ⩔ → ⩔ᛘ.

▽√^ + ℨ⩔ → ▽ : √^ + ℨ : ⩔ → ▽ + ℨ : √^ + ⩔ → ⩔ : ᛘ → ⩔ᛘ

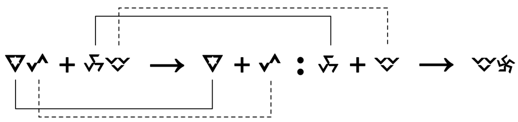

Figure 3: Bob's addition algorithm

In decimal representation, this is similar to 12 + 34 → 1 : 2 + 3 : 4 → 1 + 3 : 2 + 4 → 4 : 6 → 46. Bob is ecastatic! But he soon finds that in some cases, the sum of the individual digits is made up of two digits, whereas his primitive algorithm expects a single digit output. For example, consider the addition ▽卐 + √^ᛘ → ▽ + √^ : 卐 + ᛘ → ℨ : ▽⩔ → ?. It appears that Bob is stuck, or is he? Bob makes a quick observation that he just needs to split the pair ▽⩔ on the right again, keep the relevant second digit ⩔ and add the first digit ▽ to ℨ, such that

▽卐 + √^ᛘ → ▽ + √^ : 卐 + ᛘ → ℨ : ▽⩔ → ℨ + ▽ : ⩔ → ⩔⩔.

In decimal representation, this is similar to 15 + 26 → 1 + 2 : 5 + 6 → 3 : 11 → 3 + 1 : 1 → 4 : 1 → 41. What we have described here is the method of addition by 'carrying' which we have all been taught in primary schools when we were kids, and it can be extended to add numbers with arbitrarily large digits. For example,

⩗卐 + √^ᛘ → ⩗ + √^ : 卐 + ᛘ → ▽ℨ : ▽⩔ → ▽ℨ + ▽ : ⩔ → ▽⩔ : ⩔ → ▽⩔⩔, and

In decimal representation, this is similar to 67 + 56 → 6 + 5 : 7 + 6 → 11 : 13 → 11 + 1 : 3 → 12 : 3 → 123. The end of algorithm is determined by the : operator, i.e. when it has no pairs (or higher concatenations) to the right, at which point its function ends. In other words, the : operator always starts on the right side with a pair to its right and shifts leftwards with each iteration until it only has singles to its right. For example,

▽⩔卐 + √ㄱ√^♈ → ⩡ : ▽√ㄱ : ▽⩡ → ⩡ : ▽√ㄱ + ▽ : ⩡ → ⩡ + ▽ : ⩡ : ⩡ → 卐⩡⩡.

Once Bob discovers addition, it is only a matter of time before he realises that it is a commutative, symmteric and order-agnostic operation, i.e. ▽ + √ㄱ ≡ √ㄱ + ▽. The symmetric natures simply follows from the fact that the total count after adding Bob and Alice's stones is the same whether you start by putting Alice's stones first on the lookup table or Bob's. This realisation quickly extended to associativity of addition, i.e. ▽ + √ㄱ + ♈ ≡ (▽ + √ㄱ) + ♈ = ▽ + (√ㄱ + ♈). It is only natural from here on for Bob to discover subtraction (√ㄱ − ▽ ≡ 3 − 1 = 2), which is simply the inverse of addition in the sense that it undos the effects of addition. However, Bob notes that it is anti-commutative, non-associative, asymmetric, order-dependent and it is in fact undefined when the order is reversed, i.e. ▽ − √ㄱ. This is because Bob has no concept of negative integers (he is restricted to natural numbers) and it makes no intuitive sense for him to subtract or remove a larger count of stones from a smaller collection (e.g. ▽ − √ㄱ ≡ 1 − 3 = ?).

With his newly found obsession of counting, Bob soon starts to remember most of the basic additions without explicitly needing to perform the stone table lookup. However, adding countably many stone collections remained a challenge, e.g. (⩔卐 + 卐√^ + ⩔卐 + ⩔√ㄱ + √^⩡ + ⩔卐 + ⩔卐 + ⩔卐 + ⩔卐 + ⋯) = ?. While dealing with such lengthy evaluations, Bob notices that when there are several stone collections with the same count, his task is relatively quite easy e.g. ⩔卐 featuring ♈ (= 6) times in the above example. For instance, (⩔卐 + ⩔卐 + ⩔卐 + ⩔卐 + ⩔卐 + ⩔卐) is easier to evaluate since Bob remembers what he gets when he adds ⩔ (and 卐) repeatedly ♈ (= 6) times; he has performed this operation thousands of times in the past. In addition, he starts writing long evaluations like (⩔卐 + ⩔卐 + ⩔卐 + ⩔卐 + ⩔卐 + ⩔卐) as ⩔卐 × ♈, introducing the notation × for describing repetitions in order to shorten his notation. Using his memory of simpler multiplications, Bob is able to perform his 'carry over' addition faster and soon doesn't need to use the expanded notation for × at all! He can simply denote:

(⩔卐 + ⩔卐 + ⋯♈⋯ + ⩔卐) ≡ ⩔卐 × ♈ → ⩔ : 卐 × ♈ → ⩔ × ♈ : 卐 × ♈,

followed by,

⩔ × ♈ : 卐 × ♈ → ♈⩔ : √ㄱ⩡ → 卐⩔ + √ㄱ : ⩡ → ♈√ㄱ : ⩡ → ♈√ㄱ⩡.

In decimal notation, the above example is equivalent to:

$$(75 + 75 + \cdots 6 \cdots + 75) \equiv 75 \times 6 \rightarrow 7 : 5 \times 6 \rightarrow 7 \times 6 : 5 \times 6$$
$$\rightarrow 42 : 30 \rightarrow 42 + 3 : 0 \rightarrow 45 : 0 \rightarrow 450.$$

Curious bob immediately tests the multiplication operation for commutativity and associativity and finds that both properties hold; this doesn't come as a surprise to bob since he has constructed the × operation from series of + operations which are both atomically commutative as well as associative. With the ability to perform complex counting operations, Bob soon rises among the ranks of stone gatherers and starts his own business. Soon he employs hundreds of gatherers and becomes a wholesale stone supplier.

With rising business however, he finds himself spending a lot of time doing lengthy operations, even after using his 'carry over' algorithm and memorised tables. One day he gets an unprecedented total of 𒐗𒐜𒐐 (= 345 in decimal) stone gatherers, each collecting anywhere between 𒌋𒐐 (= 9) and 𒌋𒐜𒌋 (= 99) stones. This presented him with a huge number of table lookups and evaluations. For instance, he noted that there were 𒐗𒐜 (= 60) people who brought 𒌋𒁹𒐜 (= 93) stones each. Without his '×' notation, Bob would need to make a record of it in the form of (𒐗𒐜 + 𒐗𒐜 + ⋯ 𒌋𒁹𒐜 ⋯ + 𒐗𒐜). However, Bob uses his clever trick and quickly makes the abbreviation 𒐗𒐜 × 𒌋𒁹𒐜 (= 60 × 93).

While the notation saves the day somewhat, it doesn't make Bob's job much easier. Unlike the previous (easier) example of 75 × 6 where Bob remembered the multiplication table of 6, in this case he doesn't know the multiplcative table of either 𒐗𒐜 (= 60) or 𒌋𒁹𒐜 (= 93). While worried at the start, Bob soon realises that in fact only needs the tables of smallest atomic labels since 𒐗𒐜 × 𒌋𒁹𒐜 → 𒐗 × 𒌋𒁹𒐜 : 𒐜 × 𒌋𒁹𒐜, where both the left and right side of : can be individually evaluated as 𒌋𒁹𒐜 × 𒐗 ≡ 𒌋 × 𒐗 : 𒁹 × 𒐗 : 𒐜 × 𒐗 and 𒌋𒁹𒐜 × 𒐜 ≡ 𒌋 × 𒐜 : 𒁹 × 𒐜 : 𒐜 × 𒐗 respectively, such that

$$\text{𒐗𒐜} \times \text{𒌋𒁹𒐜} \to \text{𒐗} \times \text{𒌋𒁹𒐜} : \text{𒐜} \times \text{𒌋𒁹𒐜} \to (\text{𒌋} \times \text{𒐗} : \text{𒁹} \times \text{𒐗} : \text{𒐜} \times \text{𒐗}) : (\text{𒌋} \times \text{𒐜} : \text{𒁹} \times \text{𒐜} : \text{𒐜} \times \text{𒐜}) \to (\text{𒐗} : \text{𒐐𒌋} : \text{𒐜}) : (\text{𒐗} : \text{𒐐𒐜} : \text{𒑱𒐜}) \to (\text{𒐜} : \text{𒐗} : \text{𒐜}) : (\text{𒌋𒁹} : \text{𒑱} : \text{𒐜}) \to \text{𒐜𒐗𒐜} : \text{𒌋𒁹𒑱𒐜} \to \text{𒐜𒐗𒐜} + \text{𒌋𒁹𒑱} : \text{𒐜} \to \text{𒌋𒐐𒐐𒑱} : \text{𒐜} \to \text{𒌋𒐐𒐐𒑱𒐜}$$

In decimal world, this is similar to

$$62 \times 99 \to 6 \times 99 : 2 \times 99 \to (6 \times 9 : 6 \times 9) : (2 \times 9 : 2 \times 9) \to (54 : 54) : (18 : 18) \to (54 + 4 : 4) : (18 + 1 : 8) \to (59 : 4) : (19 : 8) \to 594 : 198 \to 594 + 19 : 8 \to 6138.$$

Using shorthand notation '×' and lookup of simple multiplications in his memory, Bob is now able to calculate arbitrarily large multiplications with arbitrarily large 'arguments' α and γ ($\alpha \times \gamma$). What we have (re)constructed here is the well-known Vedic or Chinese or Japanese multiplication; one can imagine why there are so many names for it since it arises very naturally in any base system and was likely discovered independently by each intelligent civilisation.

Considering that Bob discovered the inverse of addition, it is natural for him to wonder if an inverse operation exists for multiplication; he denotes this operation with ÷. In a countable sense, Bob interprets that division is equivalent to distributing a collection of stones equally among some individuals, e.g. he denotes his intention of dividing 𒐜𒁹 stones among 𒑱 people with 𒐜𒁹 ÷ 𒑱. Bob initially deduces that division only makes sense if his collection of stones is sufficiently large to divide among any given group of people, i.e. for 𒑱 people, he needs at least 𒑱 stones to be able to give a single stone to everyone. This situation is similar to subtraction where Bob wasn't able to subtract a bigger count from a smaller count; now he is unable divide a smaller count by a bigger count. He finds that similar to subtraction, division is anti-commutative, non-associative, asymmetric and order-dependent. Bob lastly defines a corollary of division, the modulo operation %, which describes how many stones will remain after Bob has finished equally distributing as many as he possibly can among all group members, e.g. 𒐜𒁹 % 𒑱 = 𒌋.

PRIME COLLECTIONS

Bob's good days are yet again shortlived. One day, he is assigned the task of dividing the day's collection of ▽⩔√7 stones equally among Ұ people in a group. Bob quickly finds that he is unable to do so; in decimal terms he had been asked to divide 101 stones among 6 people equally. He further notices that for a given group of people, some collections cannot be equally distributed. He also notes that for any given collection of stones, he can distribute it equally to only certains groups. In other words, not all numbers are divisible by other smaller numbers! This property is somewhat more bizarre to interpret for Bob; subtraction never caused him trouble in the sense that he could always distribute any collection of stones among any group of people as long as he didn't need to be fair and equal. Division seems to create more constraints for Bob when the condition of equality is imposed among all members of the group. Some days later, Bob's friend Arya noted that he was unable to equally divide his collection of ▽⩔√7 among ▽✓^ (= 9) people. Bob finds it odd that neither he nor his friend could equally distribute their equivalent collections of ▽⩔√7 (= 101) stones to distinctly different groups of people (with 6 and 9 members). Bob investigates more and finds that the collection of ▽⩔√7 stones is in fact impossible to distribute equally among members of any countable group[2]; we know these numbers as prime numbers. Bob and Arya's investigations reveal that these numbers continue to exist no matter how far you extend the natural numbers, and their distribution is base-agnostic and aperiodic.

FINDING ZERO THROUGH EXPONENTS

Let's fast-forward a little bit and re-discover zero, i.e. 0. In figure 1, Arya notices that the horizontal and vertical axis are not the same 'stone units' in length, i.e. horizontal axis is one (→ ▽ → 1) stone unit longer than vertical axis. Arya also notices that there is no formal label for describing complete absence of stones. He thereby suggests Bob that he should:

a) add one more cell representing 🅥 (≡ 🅥🅥 ≡ 🅥🅥🅥 ⋯) at the top of the first column, and,

b) introduce labels of the form ▽🅥, ✓^🅥, √7🅥, ⋯ ⩔🅥 such that the table's axis are equal in length.

Bob however is not convinced since,

i) he probably doesn't think that the 'absence of stones' needs a label, and secondly,

ii) his intuitive interpretation of ▽▽ following ⩔ (i.e. first stone in the first column of paired labels) doesn't work if ▽🅥 happens to follow ⩔.

Bob resists the idea of 🅥 for the longest time; infact, the concept of zero originated much later than the basic airthmetic operations of addition (+), subtraction (−), multiplication (×) and division (÷). This is not surprising since these operations do not need zero in their primal definitions. The presence of zero however makes complex combinations (aka 'functions') of (+, −, ×, ÷) much easier to describe or evaluate despite being unintuitive. This eventually led to the acceptance of zero (≡ 🅥 ≡ 0) at par with natural numbers about 18,000 years later. In essence, zero makes natural numbers complete or 'whole', thus leading to the term whole numbers. In our fictional present however, Bob finds zero too abstract and unintuitive, and doesn't include it in his number system. With time, Bob's number system finds utility

[2]with the exception of distributing a single stone per person

in all aspects of life, and being able to count and do basic arithmetic using the 'stone table' lookup in figure 1 (which later became abacus) becomes equivalent to a Doctorate in Advanced Mathematics. Bob soon realises that he can not only count and describe objects using his system but he can quantify the 'size' of an object (once he assigns one stone unit to a specific size for setting a formal standard). By interpreting the table in 1 such that each cell now represents the 'size' of an object, Bob discovers the concept of length (units along a string or line), area (units on flat surfaces) and volume (units inside bulk volume). In his native number system, the definition of length is the same as counting stone units along a path, say for example 𒐗 units. The definition of area (with side length 𒐗) in his system yields 𒐗 + (𒐗 × 𒐗) units and the volume can be counted in 𒐗 + (𒐗 × 𒐗) + (𒐗 × 𒐗 × 𒐗) units.

There is no reason for Bob to stop at multiplication and he can go on to formulate even more complex operations. For instance, recall that Bob derived multiplication from the idea of repetitive 'self-additions'; in the same spirit, Bob can now perform 'self-multiplications' to derive the exponent(ial) operation, e.g. $𒁹^{𒐗} = 𒁹 \times 𒁹 \times \cdots 𒐗 \cdots \times 𒁹$. Bob is further surprised to note that exponential operation is almost non-commutative, non-associative, asymmetric and order-dependent; this isn't the case for either addition or multiplication – both of which are commutative, associative, symmetric and order-agnostic. It appears as if higher-order operations[3] generated from self-operating on lower-order operations leads to unusual behaviour after the second order (= 2-order).

The culmination of exponent leads Bob to note that in order to count to increasingly higher values (≡ increasingly more 'digits'), he needs to keep extending the 'dimensions' of his 'counting box'. The 'counting volume' required to count up to α digits in natural number system is written as a series sum $(𒐗 + 𒐗^{𒐗} + 𒐗^{𒐗^{𒐗}} + \cdots + 𒐗^{\alpha})$. This is somewhat inconvenient. Due to the asymmetric-by-1 nature of Bob's natural number system, many identities tend to have unnecessarily complicated and serial forms. In the whole number system however, the counting volume for α digits is simply $𒐗^{\alpha}$; this is equivalent to 10^{α} digits in the decimal system. This finally convinces Bob to accept 𒐕 in his counting system, thereby formalising whole numbers as the default counting framework.

THE CURIOUS CASE OF COMMUTING EXPONENTS

Let's now give Bob a break and fast-forward to the 1600s onward. Recall from the previous paragraph that we had termed the exponent operator 'almost' non-commutative; the reason for this is that exponents of the form α^{γ} are non-commuatitive for all natural values of α and γ except 𒐗𒐗 (= 2) and 𒐖 (= 4). Nearly absolute non-commutativity of exponents is the subject of perhaps the largest collection of famous proven and unproven conjectures in Mathematics; Catalan's conjecture, Fermat-Catalan conjecture, Fermat's Last Theorem or Fermat's conjecture, Beal's conjecture, Modularity theorem etc. In this section, we will attempt to prove the non-commutativity of exponents, in particular the Catalan's conjecture, in the most generic way possible. Catalan' conjecture formally states that 8 and 9 are the only two consecutive powers, i.e. $x^a - y^b = 1$ has only one solution (x, y, a, b) = (2, 3, 3, 2). We will try to prove a slightly different version of it for natural numbers which states that $a^b - b^a > 0$ for all a > b except (a, b) = (4, 2); this is not much

[3] addition = 1-order; multiplication = 2-order; exponential = 3-order

different than proving that $x^a - y^b = 1$ has only one solution for $a > b$. Let's call this the commutative Catalan's conjecture, which is simply that exponents do not commute except for $4^2 = 2^4$.

Let's begin by considering a general enough example in order to maintain an intuitive perspective and we will then build a formal treatment based on it. Let's try to prove that $9^{14} > 14^9$. Our method relies on breaking our conditional expression into atomic evaluations. For instance consider the following list which we have derived from 9^{14} by incrementing the base and decrementing the exponent recursively by 1.

$$9^{14} \ ? \ 10^{13} \ ? \ 11^{12} \ ? \ 12^{11} \ ? \ 13^{10} \ ? \ 14^9, \tag{1}$$

where ? denotes the unknown conditional relation between two terms. Our goal is to eventually evaluate some or all of these ? conditions. In formal terms, to prove $a^b > b^a$ given $a > b$, derive a list from a^b by incrementing the base and decrementing the exponent recursively by 1,

$$a^b \ ? \ (a+1)^{b-1} \ ? \ (a+2)^{b-2} \ ? \ \cdots \ ? \ (b+2)^{a-2} \ ? \ (b+1)^{a-1} \ ? \ b^a. \tag{2}$$

Let's make a note of some generalities that we have lost when we chose the specific example of 9^{14}; this will help us correct for these loses when formalising our proof for general a and b. We note that $a - b = 14 - 9 = 5$ which is an odd number and thus our list has even number of elements amounting to $a - b + 1 = 6$. The result of this is the appearance of term $\cdots \ 11^{12} \ ? \ 12^{11} \ \cdots$ $(\cdots \ k^{k+1} \ ? \ (k+1)^k \ \cdots)$ right in the middle of our list. If $a - b$ was to be an even number, then our list would contain odd number of elements and the term in the middle would read $\cdots \ (k-1)^{k+1} \ ? \ k^k \ ? \ (k+1)^{k-1} \ \cdots$. Our proof relies on the fact that it is easier to prove relations between consecutive terms in (1)–(2) than between the end terms directly! In an ideal world, if we could prove that all ? = > in (1)–(2), then it naturally follows that $9^{14} > 14^9$ in (1) and $a^b > b^a$ in (2). Life is however unfair and we will see next that this is not the case.

To see this, let's investigate the central atomic relation $k^{k+1} \ ? \ (k+1)^k$ when $a - b$ is odd and expand the right side into its polynomial form,

$$k^k \cdot \ k \ ? \ k^k + \alpha_{k-1} k^{k-1} + \alpha_{k-2} k^{k-2} + \cdots \ {}_{k+1 \text{ terms}} \ \cdots + \alpha_2 k^2 + \alpha_1 k + 1,$$

$$k \ ? \ 1 + \alpha_{k-1} k^{-1} + \alpha_{k-2} k^{-2} + \cdots \ {}_{k+1 \text{ terms}} \ \cdots + \alpha_2 k^{-(k-2)} + \alpha_1 k^{-(k-1)} + k^{-k},$$

$$k \ ? \ \sum_{i=0}^{k} \alpha_{k-i} k^{-i}. \tag{3}$$

The coefficients for this polynomial are well-known and given by

$$\alpha_{k-i} = {}^kC_i = \frac{k!}{i! \ k-i!} < k^i. \tag{4}$$

The inequality above gets stricter with increasing k such that $\alpha_{k-i} << k^i$ for $k >> 1$. Note that ${}^kC_i$ peaks when $i = k/2$ for even k and $i = (k-1)/2$ and $(k+1)/2$ for odd k. Using the 'weak' inequality in (4), we can already conclude by counting the summation terms (= k + 1) that

$$k \ ? \ \sum_{i=0}^{k} \alpha_{k-i} k^{-i} < k + 1,$$

which is trivial and not helpful whatsoever. However, it turns out that upon considering the 'stricter' inequality in (4) and after a bit of clever algebraic manipulation, (4) results in a much stricter and useful condition,

$$\sum_{i=0}^{k} \alpha_{k-i} k^{-i} < 3, \tag{5}$$

for all values of $k > 1$! This is much more helpful and finally leads to

$$k^{k+1} - (k+1)^k \geq k - 3. \tag{6}$$

where the equality holds for $k = 2$ only! We have proven what we set out to prove about the condition $k^{k+1} \; ? \; (k+1)^k$. We found that $? = >$ for all $k > 1$. Moreover, for $k = 2$ specifically, we find that $2^3 - 3^2 = -1$, which is exactly the statement of traditional Catalan's conjecture. Note that we have proven the classical Catalan's conjecture for consecutive powers of a specific form[4] and not for general exponents of general bases.

In our grand scheme or list of conditionals in (2), we have solved for at least one of the conditions such that

$$a^b \; ? \; (a+1)^{b-1} \; ? \; \cdots \; ? \; k^{k+1} > (k+1)^k \; ? \; \cdots \; ? \; (b+1)^{a-1} \; ? \; b^a, \tag{7}$$

for odd values of $a - b$. The central atomic relation(s) $(k-1)^{k+1} \; ? \; k^k \; ? \; (k+1)^{k-1}$ for even values of $a - b$ can be evaluated in the exact same manner such that

$$a^b \; ? \; (a+1)^{b-1} \; ? \; \cdots \; ? \; (k-1)^{k+1} > k^k > (k+1)^{k-1} \; ? \; \cdots \; ? \; (b+1)^{a-1} \; ? \; b^a, \tag{8}$$

for even values of $a - b$. To continue proving the rest of the conditionals, we first consider all terms to the right of $>$ since they are easier to prove. In order to prove these en masse, consider a sightly modified version of (6) where the base and the exponent are independent of each other,

$$k^{p+1} - (k+1)^p \; ? \; 0. \tag{9}$$

What can we infer about this conditional? We can see that it tries to make some statement about powers formed from consecutive bases with decrementing exponents but the base and the exponent are not related; this is similar to but not the precise statement of classical Catalan's conjecture which we now must endure to prove the modified Catalan's conjecture. We can start exploring the nature of our statement by choosing a value of $k = 2$ and $p = 1$, and begin incrementing p by 1. We quickly find that $2^{p+1} - 3^p > 0$ for $p = 1$ only.

Next consider $k = 3$; we find that $3^{p+1} - 4^p > 0$ for $p < 5$, and $3^{p+1} - 4^p < 0$ for $p > 4$.

Then consider $k = 4$; we find that $4^{p+1} - 5^p > 0$ for $p < 8$, and $4^{p+1} - 5^p < 0$ for $p > 7$.

Then consider $k = 5$; we find that $5^{p+1} - 6^p > 0$ for $p < 10$, and $5^{p+1} - 6^p < 0$ for $p > 9$.

Then consider $k = 6$; we find that $5^{p+1} - 7^p > 0$ for $p < 13$, and $5^{p+1} - 6^p < 0$ for $p > 12$.

[4] where the base and the (decrementing) exponent are bound by a difference of 1; general form doesn't insist on either a fixed difference or decrementing exponents although the case of incrementing exponents is trivial to disprove

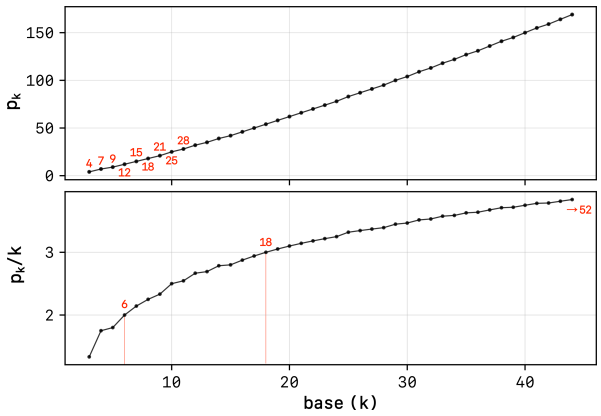

Figure 4: Zero cross-overs p_k and p_k/k for k up to 44. Note: $p_k/k = 4$ at $k = 52$. The bottom plot shows what looks like an asymptotic curve but this is not the case; p_k/k extends to ∞ and it is not asymptotic to any straight line of any slope.

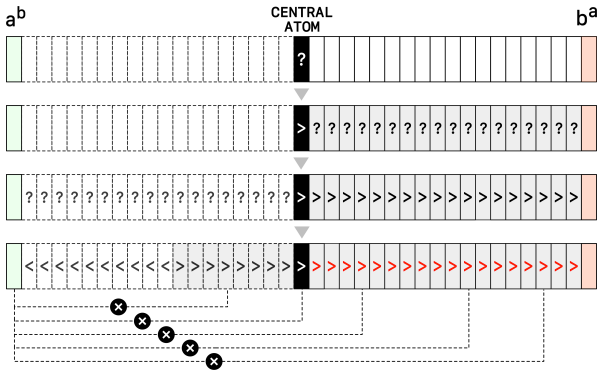

Figure 5: Proof consists of recognising the central atom and proving its conditional ? = >. We then prove that the conditionals to the right of the central atom are also ? = >, followed by proving that some of the conditionals on the left extend the trend from righthand side, such that ? = > for p_k < k and ? = < otherwise.

We can continue to do this and evaluate the 'cross over' point p_k for each k such that $p_k = (1, 4, 7, 9, 12, 15, 18\cdots)$ for $k = (2, 3, 4, 5, 6, 7, 8\cdots)$. Without getting caught in empirical details (see figure 4), we can conclude that $k^{p+1} - (k+1)^p > 0$ for all $p < k$ for all $k > 2$. The case of $k = 2$ is again an exception similar to the previous analysis; for $k = 2$, $p = 1 < k = 2$. With this assertion, we have proved that ? = > for all terms to the right of > in equations (7) and (8)! In fact, our previous proof of the central atom in (7) is a special cases of $p = k - 1 < k$. Now (7), (8) can be updated as follows:

$$a^b \;?\; (a+1)^{b-1} \;?\; \cdots \;?\; k^{k+1} > (k+1)^k > \cdots > (b+1)^{a-1} > b^a, \tag{10}$$

for odd values of a − b, and

$$a^b \;?\; (a+1)^{b-1} \;?\; \cdots \;?\; (k-1)^{k+1} > k^k > (k+1)^{k-1} > \cdots > (b+1)^{a-1} > b^a \tag{11}$$

for even values of a − b. Now we are only left with the conditionals to the left of the central atomic relations in (10)–(11). Unlike the previous conditionals to the right of the central atom(s) where ? was >, this is in fact not true for the terms to the left. This follows straight from our analysis that led to assertion about (9), i.e. for p sufficiently larger than k ($p > p_k$), $k^{p+1} - (k+1)^p < 0$. Since exponents increase leftward in our list, we find that it is entirely possible for the terms to become monotonically decreasing instead of increasing (moving leftward) somewhere between the start and the middle of the list! In figure 5, we can see this effect visualised graphically. If we were to accept empirical evidence from figure 4, we can determine precisely where the possible shift from monotonic descension to ascension occurs (aka at $p = p_k + 1$) for any given k. Without empirical evidence however, we are a bit stuck so to speak. For instance, our initial example in (1) is now simplified to

$$9^{14} \;?\; 10^{13} \;?\; 11^{12} > 12^{11} > 13^{10} > 14^9,$$

which is easily reducible to

$$9^{14} > 10^{13} > 11^{12} > 12^{11} > 13^{10} > 14^9,$$

$$9^{14} > 14^{9},$$

since we know empirically from figure 4 that remaining ? = > for p < 26 for k = 10 and p < 22 for k = 9. This is cheating though and we couldn't make a similar statement if k was arbitrarily large.

–

NUMBER THEORETIC PROOFS & CONJECTURES

Readers may be interested in knowing that while exponents are responsible for the larger set of number theoretic conjectures (which can be interpreted as a measure of 'symmetries' in the counting system), more elementary operations of addition and multiplication also possess their smaller but fair share of similar conjectures (and associated symmetries). For addition operation, Goldbach's conjecture is one of the oldest conjecture in mathematics and still unproven to this day! It astonishingly makes the simple statement that all even natural numbers greater than 2 can be represented as sum of two prime numbers, i.e. $2{\cdot}c = a_p + b_p$ for all $c > 1$. The equivalent of this symmetry for multiplication operation is the Prime Factorisation theorem, or more formally known as the Fundamental Theorem of Arithmetic. This is however easier to prove from first principles than the equivalent symmetry for addition.

Readers should find it odd that a clearly more complex prime factorisation symmetry is astonishingly easier to prove than the seemingly innocent statement by Goldbach. Perhaps yes, but could one can justify this by saying that the origin of primality of numbers lies in the product operation itself and therefore the prime factorisation theorem is in fact a corollary to the definition of prime numbers? In other words, the prime factorisation theorem relates the prime numbers (aka the prime subgroup) to the operation of $\times$ which is the group operation responsible for their very definition. The addition operation however is an operation from a different (additive) group and has nothing to do with prime numbers 'directly'. Goldbach's conjecture is thus akin to proving a symmetry between the + operation from additive group and the prime elements (or subgroup) from the multiplicative group; this should be more difficult to prove as a result of the cross-group operation-element interaction(s).

In fact, a similar difficult-to-prove conjecture exists for the exponent operation in the category of cross-group 'interacting' conjectures: Fermat's Last theorem, i.e. no natural number solutions (except 1) exist for $a^n + b^n = c^n$ for $n > 2$. This is an example of a cross-group conjecture trying to prove a symmetry between the 'power' operation from the exponent group (and its elements) to the + operation from the additive group, and it had been excrutiatingly difficult for number theorists to prove until 1995. It is meaningful to note a trend here among these conjectures and the difficulty associated with their proofs: cross-group conjectures among groups that are directionally far-related in the sense of group heirarchy appear to be more difficult to prove formally than the cross-group conjectures among nearby heirarchical groups. This statement will make more sense with an immediate corollary: recall that the prime factorisation theorem not only states that all natural numbers (except 1) has prime factors but also tells us about the the exponents of those prime factors required to arrive at the original number through multiplication. This is an example of cross-group operation between the exponent group and the prime subgroup in the multiplicative group!

REFERENCES

_

METADATA

Github:
Contracts:
Source:
SHA-1 Checksum:
Date: April 22, 2024