Algorithms for testing prime factors against positive composite numbers (finding the unique factorization domain for said composite numbers) in base 10: a first course into formal mathematics

Labib Zakaria

April 26, 2019

Abstract

There exist many algorithms to test the primality of positive natural numbers both proved and unproved, as well as in base 10 and outside base 10. Once the primality of a number has been determined, natural questions are (1) what the unique prime factors of it are and (2) their degree, according to the fundamental theorem of arithmetic.

These questions can prove to be useful in beginning to analyze the properties of the number by allowing us to determine the number of (proper) divisors of a number as well as their sum and product. In regards to (1), there are many algorithms that could be applied to determine these prime factors through modular arithmetic algorithms. We will be tackling this question in base 10 specifically by constructing functions as curious mathematicians.

Contents

1 Motivation

At initial glance of the cases $(9^1)_{10} = (18)_{10}$, $(9^3)_{10} = (729)_{10}$, and $(9^5)_{10} = (59049)_{10}$ in our base 10 system), it may appear that the following conjecture is true:

Conjecture 1. *(Digit Sum & Opposite Parity in Bases & Powers) Let $b \in \mathbb{N}^+$ such that $b \neq 1, 2$. Now, define b as the base of a number system. Further, let $o \in \mathbb{N}^+$ (the set of positive counting numbers) such that $par(o) \neq par(b)$ (parity representing the oddness or evenness of a mathematical object). Then, $S([(b-1)^o]_b) = (b-1)\lceil \frac{o}{2} \rceil$, where S represents the digit sum function and the brackets represent an operation (the ceiling function) that takes a real number and outputs the lowest integer above it or equal to it.*

However, you should come to realize after interacting with different bases and different powers that this is not necessarily true. For example, calculating the digit sum of $(9^{30})_{10}$ on WolframAlpha yields 99, rather than 135. Further, we shall coin the powers that follow this conjecture as simple powers.

This is one of the aspects that makes number theory both such an interesting and frustrating field that reflects our human nature. Namely, numbers never seem to behave as nicely as we think they should, yet we still persist in our desire to find the patterns that hide behind them to find the truth that exists in this world. Sometimes, this casual play yields fruits for society, but either way it is fun in itself.

Particularly, in cryptography, prime numbers turn out to be useful because we have not found a function that maps the positive natural numbers to the corresponding primes by the order of the real numbers. Thus, modular arithmetic related to primes, like in this paper, is the framework for cryptography (like the RSA algorithm) and this framework can be exploited in the chase to catch criminals from digital evidence.

Even if those uses of number theory bore you, then you can always use it to surprise people with how "smart" you are or to complete computations in math class quickly. In these senses, number theory (and math in general) parallels investigation in the arts and sciences. It is like playing a challenging video game and strategizing to achieve various objectives in the game, while still maintaining the realism of tangible consequences to failures.

In a stronger effort to motivate, particularly the logic and interjections, note that simply knowing a ton of information gets you nowhere, unless you know how to use it. This is why I interject; I do not want to just throw information at people, but, rather, I want them to think about things philosophically and intuitively, without feeling overwhelmed in formalisms. In other words, I suppose that they are mind candy to keep people engaged through the whole paper and to help them understand it, despite the abstract math.

Let us consider the concept of infinity in such a framework. Many would agree that infinity is a very abstract concept, yet it is ubiquitous in life. Everyone is always trying to push ahead further and they can often do so "infinitely". We can keep measuring things to greater accuracy, we can improve in a domain infinitely, we can be held to some character trait until it becomes all that defines us and that even stops to matter, and so on, but we slow down the farther we go. Thus, we can sense the concept of infinity and it being associated with converging limits. (Try to model the ideas of divergence in a similar manner, considering both oscillatory divergence and infinite divergence.)

Thus, the idea of the convergence of infinite series and products begins to make sense and we can accept the ideas that 0.999...=1, that the probability of two positive natural numbers being coprime is $\frac{\pi^2}{6}$ from the Basel problem, and that objects can have fractional dimension.

Ultimately, knowledge exists to help us further our intuition, pushing ahead of what we thought we could achieve in a human spirit. For that, we should pay our respects by assimilating it into our lives. This quest for intuition is why I am often hesitant to work with examples when I can avoiding doing so; I fear that they may cloud my intuition by pulling me down a local, blind alley, rather than letting me see the whole world.

Back to the challenge of math, we would expect that mathematicians have discovered this prime-counting function.

Once again, however, our efforts are producing little fruit.

Recently, hopes have risen with regards to this problem. Last September, Michael Atiyah claimed to have a proof of the Riemann Hypothesis, which may provide an exact prime counting function if true. However, his presentation and paper certainly did not meet up to this claim.

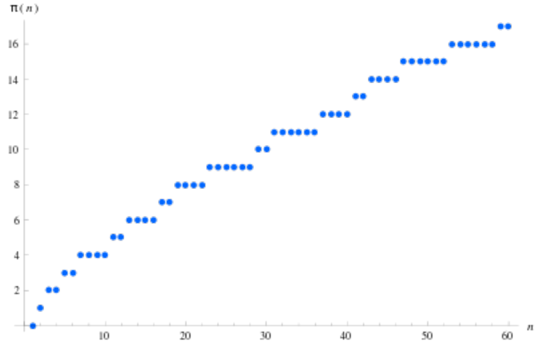

Figure 1: Prime Counting Function from 0 to 60, Image from Wikipedia

While I am sure that many are disappointed of this outcome, we must keep our heads high. We must gradually tackle approachable problems until we reach a point where insight can lead us to a conclusion on this matter.

I challenge you to consider the discussed similarities between these two problems of prime numbers and powers of the $(b-1)$th number in a base b system (that is, what is $[(b-1)^o]_b$ for different n and k as above [also try for o that have the same parity as b] or is it even possible to express this in an elegant, generalized manner), so that we can rise from the ashes to finally (in the likely distant future) solve the Riemann Hypothesis or other important or fun problems.

Suggestions: Analyze the function after reading this paper through analyses of graphs in Sage using analytically designed approximations and read through a variety of literature in mathematical analysis and number theory.

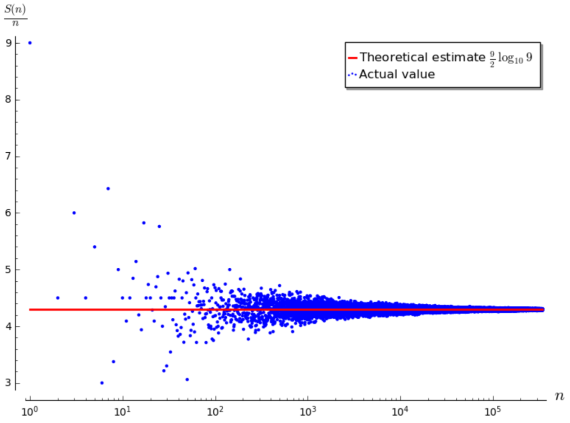

Figure 2: Here is a nice starter, Image from Sage.

2 Background

You might wonder why I am bringing up this convoluted and unrelated problem. I have a few points to support my decision. Since I am aiming this toward a general audience, I need to make sure that I establish some common ground between me and the audience, so that the audience is engaged toward what I am saying. In doing so, I am making a point of actively using personal pronouns (this is also an academic convention at the higher levels) and I am attempting to support my points through examples and pursuable logic (helping the audience to quickly grasp my points). Also, this specific problem will probably also be challenging, even for seasoned mathematicians, but is still accessible to the general intelligent person.

Now, I am aware that the uninitiated mathematician might feel intimidated by/unfamiliar with much of the content that I bring up and/or perhaps fascinated by the content. I feel many of the concepts are simple to briefly explain, so that is what I will do. I will not specifically discuss the concepts or approach to solve the problem that I brought up or simply provide a solution, but feel free to pursue the problem though many of the resources that I provide through this paper.

For those who do not have an understanding of how base number systems function, a base number system is a way of representing numbers. For our discussion, we only need to concern ourselves with positive integer bases and the positive integer numbers to be represented in those bases, however there are non-standard, general bases (complex, linear algebraic, etc.) and both positive and negative decimals/fractions for these bases. Feel free to expand on this discussion by considering these cases.

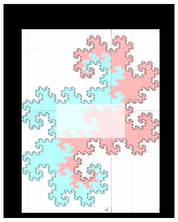

Figure 3: Complex numbers with integer part all zeros under the base i-1 form the fractal Twindragon in the complex plane, Image from Wikipedia.

Definition 1. *(Base/Radix of a Number System & Number Represented by a Base/Radix) Let $b \in \mathbb{N}^+$ such that $b \neq 1$. Now, define b as the base/radix of a number system. For a number $n \in \mathbb{N}$, (base form) $(n_1n_2n_3...n_{d-1}n_d)_b$=$\sum_{i=1}^{d} n_ib^{d-i}$ (polynomial form) where $\exists$ (there exist) $n_i < b$ $\forall$ (for all) b, n_i.*

About these prime-factorization-based functions I have brought up, notice how numbers are defined relatively from their bases. This insight seems to have some vague connection to these functions. We start with a seed, from which grows a tree. How might this tree be growing?

Again, to extend extraneously, you might be familiar with the set of complex numbers (which is a canonical embedding of the real numbers) $\{a + bi \in \mathbb{C} | a, b \in \mathbb{R}, i^2 = -1\}$. These can be used within different bases and different number systems as well.

In fact, algebra is much broader than many of us are aware, encompassing many generalizations to describe different structures that commonly occur in math. This part of algebra is called abstract/modern algebra and some of the structures that it examines are sets denoted as groups, fields, rings, and magmas, which are represented as various categories that feature functors as maps and find use in functional programming.

These structures follow some of the basic axioms that one might learn in a middle or high school Algebra 1 class and various concepts are applied to them such as equivalence relations, mapping, ordering, and set constructions [4]. You can also extend the complex number system into the quaternions, octonions, sedenions, and infinitely other number systems based on similar 2^n dimensional constructions of different imaginary variables (called Cayley-Dickson constructions). However, as you generalize the number system, you lose properties between the numbers. When you interact with mathematical objects, you also want to be careful to ensure that you are applying definitions, theorems, lemmas, and proofs to maximally general objects.

Interestingly, you can apply the theory of groups to solve Rubik's cubes (composition of moves, quotient groups, automorphism groups, cardinality, order, etc.) and quaternions (the 2^2 dimensional number system with imaginary units i,j, and k where $ijk = i^2 = j^2 = k^2 = -1$) are useful in depicting 3D rotations as well as matrices.

The same sorts of abstractions sprang from calculus and geometry to yield the mathematical fields of analysis and topology respectively, which have proven immensely useful to the sciences in the development of mathematical models (knot theory helps to describe enzymes and topological properties help to describe phases of matter both from topology and differential/integral equations can be used to model scientific situations as well as complex analysis in describing various physical situations). Similarly, from abstract algebra, we now consider the logical, proof-related, and set-theoretic implications of the current construction of math. In fact, we have realized that there are certain statements which are unprovable depending upon the specific axiom system.

In exchange for not having to design complex experiments and run them multiple times, mathematicians must rigorously prove their results under these frameworks of logic, proof, and set theory, as well as the knowledge contained in the various mathematical fields. That is soon what we shall do after we discuss some of the basic results of number theory and review the terminology.

The fundamental theorem of arithmetic states that every positive natural number > 1 can be expressed as the product of unique positive prime factors (inclusively) up to each of their degrees, ignoring arrangement (i.e., $\forall n > 1, \exists p_1, p_2, p_3..., p_{a-1}, p_a$ and $d_1, d_2, d_3..., d_{a-1}, d_a$ such that $\prod_{i=1}^{a} p_i^{d_i} = n$ where $\prod$ represents a continued product, each p_i represents a unique positive prime factor, and each d_i represents the respective prime's degree). The generalization of this notion is known as the unique factorization domain (UFD) in abstract algebra.

Note that 1 is considered to be an empty product and is not considered prime. Also, a product of one number is still a product. This theorem provides a basis for many procedures to determine interesting properties of numbers, such as their numbers of divisors and the sum and product of these divisors.

Regarding the divisor counting, sum, and product functions, I will not specifically discuss these, however they do exist and are dependent upon these unique prime factors and their orders. Further, many people enjoy finding numbers that are related by outputs of the divisor counting, sum, and product functions, such as amicable numbers (the set of all combined pairs of numbers such that the sum of the proper divisors of each are equal to the other number)

Now, we move into modular arithmetic. The concept behind modular arithmetic is to model (abstract algebraic) division as repetitions of subtraction and multiplication as repetitions of subtraction and to use the results of subtracting by the modular base [1]. We say that $a \equiv b \mod c \iff$ (if and only if) a and b yield the same remainder when divided by c (or $a - b = cd$ where $d \in \mathbb{Z}$). Addition, subtraction, multiplication and exponentiation behave in a familiar manner in modular arithmetic (division does not always hold).

Figure 4: Modular arithmetic is useful in solving various real-world problems such as converting between am-pm and military time, finding out what day it will be in some number of days given the current day, and finding out when two events overlap (look into the Chinese remainder theorem). For instance, this clock says that it is $12:40 \equiv 12:40 \mod 12$ and if it is am (in military time) then this would convert to $0:40 \equiv 12:40 \mod 12$, otherwise it remains the same. Image from Wikipedia.

3 Non-Trivial Prime Factors (NTPFs)

Firstly, when I reference NTPFs, note that I am referring to prime factors other than 2 or 5 because the respective algorithms for divisibility are obviously that the last digit is 0, 2, 4, 6, or 8 and that the last digit is 0 or 5. This convention (that is, not discussing the cases of divisibility by 2 or 5) is also widely adopted in the literature of this area. Additionally, these two algorithms are quite easy to prove.

Rather, the nature of the algorithms that I present regarding NTPFs will be much more similar to that of the divisibility algorithm for 7 (where one takes the last digit and doubles it, then subtracting the result from the truncated number and checking congruence to $0 \mod 7$).

Further, I will not present the general divisibility algorithm that one might commonly find on Wikipedia and (perhaps) in introductory number theory courses. While I admit that this algorithm is clean and elegant, mathematicians become adaptable to solving problems by viewing these problems under different perspectives.

4 Trivial Prime Factors (TPFs)

You might wonder why I am categorizing primes into two distinct classifications. It is simply an organizational choice that I feel makes the paper more approachable and also allows me to provide a taste of the style of proof that I will use to prove the results of this paper.

Now, recall that 2 and 5 are the TPFs of the base 10 number system.

We will provide a definition of TPFs and prove that 2 and 5 are TPFs in the base 10 number system

Definition 2. *(TPFs) We will define TPFs to be prime numbers in a base system that evenly divide the base and thus result in a simple algorithm for detection from composite numbers.*

Proof. (2 and 5 are the TPFs of the base 10 number system)

By the fundamental theorem of arithmetic, 10=(2)(5)

Any positive integer power of 10 is divisible by 2 and 5 because $(ad)^c = a^c d^c$ over the set of integers

Therefore, all digits of a base 10 number other than the last must be evenly divisible by 2 because they all represent the coefficients that couple with each power of 10 in polynomial form.

Thus, any algorithm that checks a number's divisibility by 2 or 5 (or any trivial prime factors in a base) needs and should only check the congruence of the last digit to 2 or 5 (the respective trivial prime factor) depending on which factor is being tested. A corollary is that there are no prime numbers in base 10 (or b) other than 2 or 5 (the unique prime factors of b to degree 1) that have last digits that are divisible by 2 or 5 ("). □

5 Variables

Now, we will approach the problem of crafting and proving algorithms for non-trivial prime numbers. I will simply list the variables which we will use:

n :=prime factor being tested

z :=truncated n (n w/o last digit)= $\frac{n-l}{10}$

l :=last digit of n= $n - 10z$

u :=composite number being tested

v :=truncated u= $\frac{u-w}{10}$

w :=last digit of u= $u - 10v$

You should be able to see that we have cases where $l = 1, 3, 7, 9$. The idea for creating these functions came from the basic idea in number theory that the last digit of the result of the power of a number is periodic. For example, $2^1 = 2$, $2^2 = 4$,$2^3 = 8$, $2^4 = 16$, $2^5 = 32$ and then we should be able to see that the last digit of 2^6 must be 4 and that the last digit of 2^7 must be 8 because of how we leave behind the last digit in the multiplication process.

So, I figured that I could exploit this local periodicity in multiplication with some form of a number, alongside modular arithmetic to reveal if a number is divisible by another number in a different way than the division algorithm (and the general divisibility algorithm on Wikipedia).

Note that I will only cover cases 3 and 7 because case 3 covers the process for developing algorithms for 1 and 9. As for 7, it proves to be more problematic (fractions...). Might this be related to the fact that $7 = 5 + 2$ and $5(2) = 10$, the second of which is the base of our number system?

What is also interesting is that we are dealing with multivariate functions that take u and n as inputs and output single numbers from them. It would be very interesting to see visualizations of these functions with their domain restrictions somehow, perhaps through plots of points and curve fitting or intersection geometry.

Feel free to try to predict what algorithms I will design from these variables.

6 L=3

Lemma 1. *If $l = 3$, then $z + l(1 + 3z) \equiv 0 \mod n$*

Proof. When you plug in 3 for l in the modular expression, you get that $10z + 3 \equiv 0 \mod n$.

Now, it is quite elementary to see that we are inverting the truncation of the number. However, note that this intuition is not enough to validate the acceptance of this lemma.

We begin by defining these transformations in the framework of our base 10 system.

When we truncate the number n to yield z, what we are really doing is subtracting 3 from it and dividing by 10. In other words, $z = \frac{n-3}{10}$. (Now, we can see that this same construction with $l = 7$, yields $z + l(1 + \frac{9z}{7}) = 10z + 7$, which would force problematic divisions in the form of fractions in the modularity statement and bring up complications.)

Thus, 10z+3=n, and we can now substitute this in the modular expression.

Obviously, $n \equiv 0 \mod n$ because n must evenly divide itself (note that $\mod 0$ is not viable or is trivial because division by zero is not well-defined and all it means is that both numbers are equal and also that n must have a last digit of 3, which it cannot have if it is 0). □

Theorem 1. *(Divisibility by Base 10 Factors That End with 3) If and only if $u \equiv 0 \mod n$, then $v + w(1 + 3z) \equiv 0 \mod n$*

Proof. Applying the substitutions $z = \frac{n-3}{10}$ from the last lemma and $v = \frac{u-w}{10}$ and multiplying by 10 and simplifying, we obtain $u + 3wn \equiv 0 \mod n$.

Note that $3wn \equiv 0 \mod n$ and thus only u can provide any possible congruence different from 0 (or a multiple of n), so the theorem is necessarily true and we have established a logical dependence (equivalence) of these two modular statements by contraposition and inversion (and/or negation, conversion and inversion). □

As to why you might want to apply this algorithm, you should notice that we eliminated a factor of 10 from u and merely had to add back a term based on a truncation of n, significantly reducing computational load compared to only subtracting the left side by the modular base if u is very large relative to n.

Also, you might want to set the algorithm up for multiple iterations before subtracting by the modular base depending on the modular base and the value of the left side.

When applying the algorithm, testing the prime factor against itself yields the prime factor on the left side because z=v and w=l thus we get the result of the last lemma.

Thus, you should subtract by the modular base when u decreases less than subtracting by the modular base.

I am aware that this algorithm technically also holds for negative and 0 u (respectively the left side simply becomes the negative counterpart of the positive result or 0) and you can also apply positives in those cases.

However, this restriction ensures that we follow the fundamental theorem of arithmetic because we must assume that the primes and composites are both positive, otherwise we void uniqueness of factorization.

Also, this highlights an extremely important and well-known inequality in math in the form that is most familiar for most.

With our restrictions, notice that the left side cannot be 0 or a negative number, even after applying the algorithm any number of times. This is because u must be positive and because the minimum that 3wn can be is 0, where the lowest possible factor in this term is w=0.

Thus, this is the case of the (restricted) triangle inequality $x + y > z$ where $z = 0$ from $0 \mod n$ and $x + y$ is from $u + 3wn$. If we were to extend the domain to include 0, then we would get the (extended) triangle inequality $x + y \geq z$.

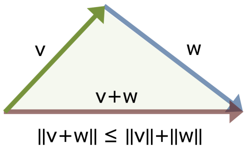

Figure 5: The general triangle equality for vectors, Image from Wikipedia.

This inequality is important in many areas of math (and also in many applications of math) because it intuitively relates to the concept of distance (being greater than zero for objects that do not coincide in a mathematical space).

With this discussion, I extend to analysis and topology again in reference to fractals (said to have non-integer Hausdorff dimension, search inductive dimension and measure theory). With this, I also reference p-adic numbers, which follow a different notion of distance than we intuitively follow.

Theorem 2. *(Nondivisibility for Base 10 Factors that end with 3) If the left side is ever between 0 and n (exclusive), then it is not in the congruence class (the countably infinite set of integers that is divisible by n, which some may recognize in the contexts of an abstract algebraic equivalence relation and Cantor set theory) because these are two consecutive multiples of n.*

Proof. We begin with the assumption that $u \equiv 0 \mod n$

In a similar fashion to irrationality arguments of numbers, there cannot be a multiple of n between two consecutive multiples of n.

Thus, by contradiction (the law of the excluded middle), u is not a multiple of n. □

Finally, we set a negative.

I know I slammed a lot at you, though I did provide a brief interlude and am also doing so now. I will review many of these concepts at §8 for those of you who do not remember your logic from middle/high school geometry/logic, but I want to provide you the opportunity to work these ideas out yourself. On that note, though, I would like to note how I hope that you see that logic is a central and intuitive part of how we think from this genuine mathematical work, rather than random and (perhaps) ridiculously connected statements you might have previously seen.

Extending this note on genuine mathematical work, notice that I have no "proof table/chart". Math is not just about robotically stringing together statements or completing rote exercises in a "correct" way. It is also about the struggle to coherently frame and attack a problem based on truth and falsity, as I alluded to earlier.

This is how actual mathematicians work and communicate.

Now, we will move onto the tough case, conclude, reflect, and move forward.

7 L=7

Lemma 2. *If $l = 7$, then $z - l(2 + 3z) \equiv 0 \mod n$*

Proof. We will need to cut many corners and take a new approach to develop an algorithm for 7 because my process results in a fractional coefficient before one of the variables which complicates the situation.

By observation, this works (it is a generalization of the division by 7 algorithm I mentioned earlier).

Plugging in 7 for l and $\frac{n-7}{10}$ for z and simplifying, we obtain $-2n \equiv 0 \mod n$, which is true as always because the left side is an integer multiple of n, though I know it is disappointing that we settle for a negative on the left side. □

Theorem 3. *(Divisibility by Base 10 Factors That End with 7) If and only if $u \equiv 0 \mod n$, then $v - w(2 + 3z) \equiv 0 \mod n$*

Proof. Applying the substitutions $z = \frac{n-7}{10}$ from the last lemma and $v = \frac{u-w}{10}$ and multiplying by 10 and simplifying, we obtain $u \equiv 0 \mod n$.

Once again, the problem reduces to a logical dependency on u. Thus, we apply the same logical manipulations to prove the statement. □

One observation about this algorithm is that it appears to have greater potential to reduce u, judging from how it subtracts rather than adds.

However, this is problematic because we can now face negative u of high magnitude after repetitions, as we have seen from the last lemma. Thus, we may need to use additions of the modular base (and more of them) if the algorithm relies on reaching the modular base.

8 Trial Runs

I was personally hoping to leave countless frontiers to be explored for the reader, but let us now examine 2 cases so that I can satisfy those who want to see my results in action. Hopefully, you have constructed the algorithms for the cases where $l = 9$ and $l = 1$, based on my $l = 3$ proofs, which use $v + w(1 + z)$ and $v + w(1 + 9z)$ respectively.

Proof. 12409 is not divisible by 3, 11, 17, and/or 19

The first number we will test is 12409, which is a prime number and thus should fail all the algorithms. Knowing this, let us still assume that this number is still divisible by 3, 11, 17, and 19. Then, $v + w(1 + z)$, $v + w(1 + 3z)$, $v + w(1 + 9z)$, and $v - w(2 + 3z)$ are all congruent to $0 \mod$ bases 19, 3, 11, and 17 respectively.

19: $12409 \mapsto 1249 \mapsto 141 \mapsto 16$. Contradiction!

3: $12409 \mapsto 1249 \mapsto 133 \mapsto 16$. Contradiction!

11: $12409 \mapsto 1258 \mapsto 141 \mapsto 16$. Contradiction!

17: $12409 \mapsto 1195 \mapsto 94 \mapsto -11$. Contradiction! □

If 12409 is not the product of these four numbers, then what is? Typing into a calculator, we get 10659. Let us use this for a final number.

Proof. 10659 is divisible by 3, 11, 17, and 19

19: $10659 \mapsto 1083 \mapsto 114 \mapsto 19$. Proved!

3: $10659 \mapsto 1074 \mapsto 111 \mapsto 12$. Proved!

11: $10659 \mapsto 1155 \mapsto 165 \mapsto 66$. Proved!

17: $10659 \mapsto 1020 \mapsto 102 \mapsto 0$. Proved! □

You can check that all the numbers being tested in the last proof were divisible by the modular base and/or that all the numbers being tested in the first proof were not divisible by the modular base, if you are skeptical. You can even try to investigate this material further, perhaps starting with the question of why all the algorithms based on the l=3 case converged to 16 in the first proof. Then, you might ask how they would behave against other primes.

9 Avenues for Further Exploration

Two other interesting, related questions would be how to find the degree that the modular base divides some number being tested and how to reduce the number of necessary computations to answer the divisibility question (based on the number being tested and considering when the equality portion of the extended triangle inequality will kick in). What parallels might our results have with other problems, so that we might be able to apply them to these problems whether merely in other base number systems or mathematical fields or even other disciplines?

I would love to be able to actually construct this algorithm, but I am not very familiar with programming. Programming is certainly useful, however, to accumulate data that could be applied to solve various mathematical problems, as well as problems in other disciplines. I hope that we can all come to appreciate the great degree of certainty that we have crafted from millenia of invention of math. It is both a powerful and difficult discipline.

On the note of systems of modular congruences, I, again, advertise investigating the Chinese Remainder Theorem to understand their workings.

Back to the conjecture I brought up in the motivation section, part of the conflict might arise from the fact that odd and even bases operate in similar fashions to integration and differentiation respectively, in terms of symbolic complexity.

This is in the sense that parity is a complex, global property in odd bases (dependent on the parity of all the digits because not every non-zero digit other than the last guarantees a factor of two), while parity is merely a local, simple property dependent on the last digit in even bases (every non-zero digit other than the last guarantees a factor of 2). In base 3, for instance, 113 is 15 in base 10, while 123 is 18 in base 10.

Further, this suggests strong, fundamental, and insightful connections between analysis and number theory. Considering that it is possible to have complex bases, you might then wonder if you can extend the ideas of derivatives and integrals to non-integer degrees and you might be delighted to learn that there is such a thing as fractional calculus.

Time to go out and play with some more mathematical ideas!

10 Conclusion

Congratulations, we just got through a formal math paper, learning tons and constructing functions that map from numbers divisible by some prime factor to the same number or to a lower number that maintains the divisibility by the prime factor! We composed each of these functions with themselves in trial runs and quickly reduced them to manageable numbers. Now, are these functions invertible and can you satisfyingly prove your answer?

That is a great accomplishment in itself.

I hope that everyone reading this feels like they got something out of it. For the seasoned mathematician, I hope that they were able to review some concepts, appreciate the constructive perspective on math, and find inspiration for future work. For the uninitiated mathematician, I hope that they learned some things and that I piqued their curiosity in math. Either way, we can benefit from consuming more mathematical content from the next section.

As for those promised explanations, I have covered a nice bit of logic and proof without thorough explanations, also building in a high level of mathematical rigor for the mathematically inexperienced. I have used a variety of proof techniques (direct, contradiction, contrapositive) and logical manipulations (inversion, negation, contraposition, conversion, law of the excluded middle).

We start with negation, so first I ask a question. (In the real numbers,) what is not positive (or zero)? This is the set of all negative numbers. In the same sense, negation is just taking what is not in the bounds of the statement. In other words, it is similar to our common usage of the word.

When we invert a statement $p \implies q$, we get $\neg$ (not) p $\implies$ (not) q. When we take the contraposition of the original statement, we now take the converse (switch) of the second version of the statement ($\neg$ (not) q $\implies$ (not) p).

I think that the law of the excluded middle is something people understand (we do not accept statements that are both true and false, thus these cases are considered false). In other words, for something to be considered true, it must be true in its entirety, anything less and it is false.

With logic, I also recommend reading about the difference between $\wedge$ (and) and $\vee$ (or). Essentially, $\wedge$ means that both conditions must intercept, while $\vee$ means that it only needs to be in at least one set. I also recommend reading about tautologies (necessary truths) and axioms. Also, when I refer to something being well-defined, I am referring to there being a logical contradiction between rules or a possibly infinite set of interpretations for the described thing.

I will, of course, recommend reading about set theory because it is the foundation of modern math and the axioms and sets that you interact with will have a great impact on how broadly you can prove results.

Then, we come to proofs. The one big thing that it is annoying about how people interpret proof problems is specifically about the word ”any”. In logic, any means all and does not mean at least one item in the described set. Thus, you cannot simply provide an example that works, but prove that the relationship is true through necessary truths (definitions, lemmas, theorems, etc.).

Also, as I mentioned earlier, proof is about explaining the process to get to the result as much as it is about getting to the result, as well as its significance. Thus, proofs should contain more words than anything else.

Make sure that your proofs starts with words to build initial momentum.

I feel like direct proof is straightforward to understand (prove that the assumption leads to the conclusion).

Some people are confused by the difference between proofs by contradiction and contrapositive. The difference is that in contradiction, we assume that the opposite of the assumption of the statement we are trying to prove, and then that we prove that this does not logically lead to the opposite conclusion of what we are trying to prove. Thus, we negate the opposite conclusion to lead to the conclusion that we were actually trying to prove. While with contrapositive, we start by negating the conclusion and logically prove that this leads to a negation of the assumption.

As for commentary on if vs if and only if (iff), just getting to the same result does not necessarily mean that the journey was the same for everyone. For instance, if someone lives somewhere, it does not necessarily mean that they were born there. They could have traveled there or been taken there.

I did not talk about induction and exhaustion. These have a bad reputation and I also think that they are often not as meaningful or elegant as the other proof techniques. With exhaustion, there must be a finite number of cases, so that you can prove each case individually. Then, you have induction, which applies to the (positive) natural numbers, where you prove the first case, assume the kth case is true, and prove the k+1th case on this foundation.

You should also check out the pigeonhole principle.

Finally, just explore tons of different technical fields of math and find what you harmonize with.

List of Figures

References

[1] Ben Lynn: Number Theory Notes (Modular Arithmetic), `https://crypto.stanford.edu/pbc/notes/numbertheory/arith.html`

[2] Terence C. Tao: What is good mathematics? `https://arxiv.org/abs/math/0702396` [math.HO]

[3] William Thurston: On proof and progress in mathematics, `https://arxiv.org/abs/math/9404236v1` [math.HO]

[4] Alexander Paulin: Introduction to Abstract Algebra Notes, `https://math.berkeley.edu/~apaulin/AbstractAlgebra.pdf`

[5] Harold Simmons: An introduction to category theory, `http://www.cs.man.ac.uk/~hsimmons/zCATS.pdf`

[6] B.V. Shabat: Introduction to Complex Analysis - excerpts, `http://math.stanford.edu/~ryzhik/shabat-all.pdf`

[7] William F. Trench: Introduction to Real Analysis, `https://math.berkeley.edu/~apaulin/AbstractAlgebra.pdf`

[8] Terence C. Tao: An introduction to measure theory, `https://terrytao.files.wordpress.com/2012/12/gsm-126-tao5-measure-book.pdf`

[9] Tomoo Matsumura: Introduction to Topology, `https://pi.math.cornell.edu/~matsumura/math4530/IntroToTopology.pdf`

[10] Elliot Mendelson: Introduction to Mathematical Logic, `https://www.karlin.mff.cuni.cz/~krajicek/mendelson.pdf`

[11] W.W. Tait: Lectures on proof theory, `http://home.uchicago.edu/~wwtx/Proof.pdf`

[12] Samuel R. Buss: An introduction to proof theory, `https://math.ucsd.edu/~sbuss/ResearchWeb/handbookI/ChapterI.pdf`

[13] William A.R. Weiss: An introduction to set theory, `http://www.math.toronto.edu/weiss/set_theory.pdf`