Number Bases and Modular Arithmetic

Andrew D Smith
University College Dublin

21 January 2023

1 Example Problems

(a) Write down your age and multiply it by 9. Take the digits of the product and add them together. If that number has more than one digit, then add the digits together and repeat until you have a single digit. Subtract that number from 11 and square the difference. Now pick a letter of the alphabet according to A = 1, B = 2, C=3 and so on, looping back to A = 27 etc if your number was more than 26. Think of a country beginning with that letter. Now look at the second letter of that country, and think of an animal beginning with that letter.

(b) For positive integers n, define the factorial, $n!$, by

$$n! = 1 \times 2 \times 3 \times \ldots \times n$$

What is the smallest n for which n! ends in ten zeroes?

(c) For a positive integer n, let $h(n)$ be the sum of the squares of the digits of n when written in decimal notation. We say n is *happy* if the sequence

$$n, h(n), h(h(n)), h(h(h(n))), \ldots$$

eventually gets stuck at 1. We say n is *sad* if the sequence contains infinitely many instances of the number 4. Show that every positive integer is either happy or sad.

(d) (EGMO Selection 2022, Q1) Let m and n be positive integers with

$$3^m = 7^n + 2.$$

Show that n must be an odd number.

2 Number Bases

2.1 Base 10

Our usual way of writing numbers is called *base ten*. For an integer up to 999, we can write it as a certain number of units, a certain number of tens and a certain number of hundreds.

Base ten is a convention linked to the number of digits on our hands. On the planet Neptune, intelligent creatures might have nine digits, and express numbers as units, nines and eighty-ones. How would arithmetic look there?

2.2 Base 9

Converting number bases uses the concept of division with remainder.

For example what we call 345_{10} would be written as 423_9 because (look at the last column)

$$\begin{array}{rcrlr} 345 \div 9 & = & 38 & \text{remainder} & 3 \\ 38 \div 9 & = & 4 & \text{remainder} & 2 \\ 4 \div 9 & = & 0 & \text{remainder} & 4 \end{array}$$

We can write

$$345_{10} = 4 \times 81 + 2 \times 9 + 3 = 423_9$$

2.3 Base 2

If you had only two fingers (or you are computer) you could count in base 2, also known as binary. We have $345_{10} = 101011001_2$ because

$$\begin{aligned} 345 = {} & 1 \times 2^8 + 0 \times 2^7 + 1 \times 2^6 + 0 \times 2^5 \\ & + 1 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 \end{aligned}$$

Operations in other number bases follow analogous rules to operations in base 10. Long division is much easier in base 2 (why?).

2.4 A Number Base Trick

Suppose you have a number written in base 10 and you want to figure out if it is divisible by 9. There is a trick, which is to add up all the digits, and if that sum is divisible by 9 then so was the original.

The same applies in base b. The sum of the digits of a number n in base b is a multiple of $b-1$ if and only if n is a multiple of $b-1$. This works because any power of b has a remainder of 1 on division by $b-1$.

3 Sets of Integers

We the set of (positive, negative and zero) integers is conventionally written $\mathbb{Z}$. Associated with this set are operations of addition, subtraction and multiplication.

3.1 Integer Division

Division in the set of integers sometimes works and sometimes does not. If we have to solve $3x = 18$ then the solution is $x = 18 \div 3 = 6$. But the equation $3x = 17$ has no integer solution in x. To find a solution we have to broaden our search to rational numbers, written $\mathbb{Q}$.

We can instead perform integer divisions with remainders:

$$17 \div 3 = 5 \text{ remainder } 2$$

The integer part of the quotient can be written:

$$5 = \left\lfloor \frac{17}{3} \right\rfloor$$

where $\lfloor x \rfloor$ means *round down to the nearest integer*, also the largest integer not exceeding x.

The remainder part is also called *modulo* and we write:

$$2 = 17 \mod 3$$

If the remainder on division of a by b is zero, we say b is a *factor* of a, or that b is a *divisor* of a, or that b *divides* a.

We write this in symbols with a vertical bar, so that:

$$a \mod b = 0 \iff b \mid a$$

If b does not divide a then we put a slash through the vertical line, so that, for example $3 \nmid 17$.

We say two integers m and n are *congruent* modulo b, denoted by a triple equals $\equiv$, if their difference is $n - m$ is a multiple of b, so that the following are equivalent:

$$m \equiv n \mod b \iff m \mod b = n \mod b \iff b \mid n - m$$

We can also apply division to negative numerators, where we have, for example:

$$-17 \equiv 1 \mod 3$$

3.2 The Set $\mathbb{Z}_b$

There are two ways to think of the set $\mathbb{Z}_b$. It could be

(a) The set of possible remainders on division by b, that is $\{0, 1, 2, \ldots b - 1\}$, or;

(b) The set of congruence classes in $\mathbb{Z}$, when we say two integers are in the same *congruence class* if their difference is a multiple of b

According to the first definition, the elements of $\mathbb{Z}_b$ are the integers $0, 1, 2, \ldots b - 1$. Under the second definition, the elements of $\mathbb{Z}$ are themselves sets of integers. We sometimes write $[b]$ for the congruence class containing b.

The concept of congruence classes is important in higher mathematical algebra, underpinning the concept of a *quotient group* in group theory.

We can define addition in $\mathbb{Z}_b$ as addition modulo b. If $b = 3$ then, for example, we have

$$2 + 2 = 1 \mod 3$$

3.3 Multiplication Mod b

What does it mean to add or multiply two congruence classes $[x]$ and $[y]$ modulo a base b? Remember, each congruence class is a set of integers. Their sums and products are also sets of integers.

We can define sums of congruence classes by adding representatives of each class. But for this to make sense, we have to be sure that the sum ends up in the same congruence class regardless of which representatives we chose.

For example, to add the congruence classes $[1]+[2]$ modulo 3, we might guess the answer is $[0]$, but for this to work we have to know that if we take any two numbers $x \equiv 1 \mod 3$ and $y \equiv 2$ mod 3 then the sum $x+y$ is divisible by 3.

We can prove this by writing $x = 3u+1$ and $y = 3v+2$ for integers u and v, in which case

$$x + y = 3(u + v + 1)$$

A product of congruence classes is defined the same way, by multiplying representatives of each class. As before, we have to check that the way we pick the representatives does not change the equivalence class of the product. For example, module 3 we have $[1] \times [2] = [2]$ because the product:

$$(3u+1)(3v+2) = 9u^2 + 6u + 3v + 2 = 3(3uv + 2u + v) + 2$$

is always congruent to 2 mod 3.

3.4 Sums of Digits in Base b

Suppose n has a representation with $k+1$ digits in base b, so that:

$$n = d_k b^k + d_{k-1} b^{k-1} + \ldots + d_2 b^2 + d_1 b + d_0$$

We can prove by induction on j that for $j = 0, 1, 2 \ldots$:

$$b^j \equiv 1 \mod b - 1$$

That is why adding the digits in base b gives a test of divisibility by $b - 1$.

3.5 Division Mod b

Can we define division modulo b?

It seems to work modulo 3. Of course, we cannot divide by zero. But otherwise, we have the division table:

Numerator	$\div$[1]	$\div$[2]
[0]	[0]	[0]
[1]	[1]	[2]
[2]	[2]	[1]

For example, the equation $[2] \div [2] = [1]$ arises because $[1] \times [2] = [2]$. Algebraists say that $\mathbb{Z}_3$ is a *field*.

This does not work for all modular bases. For example with $b = 12$ we have:

$$[2] \times [3] = [6]$$
$$[2] \times [9] = [6]$$

Therefore, we cannot assign a unique meaning to $[6] \div [2]$.

4 Primes and Relative Primality

4.1 Primes

A positive integer p is *prime* if it has exactly two positive factors, namely 1 and p.

All positive integers are either 1 (which does not count as a prime), prime, or *composite*, that is a product of two or more primes, not necessarily distinct.

In an integer n is composite, then it must have at least one prime factor between 2 and $\sqrt{n}$ inclusive. To so why, suppose there is a factor $b > \sqrt{n}$; then n/b is also a factor and is less than $\sqrt{n}$.

4.2 Relative Primality

We say two positive integers a and b are *relatively prime* if they have no common prime factor.

Bézout's Lemma states that if a and b are relatively prime integers, then there are integers x and y so that:

$$ax + by = 1$$

The converse is also true. If we have integers a, b, x, y with $ax + by = 1$, then a and b must be relatively prime (as any prime factor should also divide 1, a contradiction).

The representation in Bézout's lemma is not unique. For example, we could replace a by $a + y$ and replace b by $b - x$ and the result still holds.

We will not prove Bézout's lemma here. The proof, which uses Euclid's greatest common divisor algorithm, is not difficult. It is also constructive, in other words, method of the proof not only sohws that x and y exist, but gives an algorithm for finding them.

Bézout's lemma implies Euclid's lemma, that if a, b are integers and $p \mid ab$ then either $p \mid a$ or $p \mid b$ (or both). To see why, let us suppose that $p \mid ab$ but $p \nmid a$. Then p and a are relatively prime and Bézout's lemma implies there are x and y such that:

$$ax + py = 1$$

Now multiply each side by b which gives:

$$abx + pby = b$$

Now p is a factor of both terms on the left hand side, and so is a factor of their sum on the right hand side, which completes the proof.

This was not Euclid's original proof, partly because Euclid lived around 300BC, while Bézout lived in the 18th century.

Some students think Euclid's lemma is obvious from writing down the prime factorisations of a and b, noting that if a prime p fails to appear in either factorisation then it also absent from the product. However, this apparent proof requires the unique factorisation of integers into primes, which is true but the proof requires Euclid's lemma. So this student proof is not a proof at all; it is a circular argument.

4.3 The Set $\mathbb{Z}_b^\times$

We define the set $\mathbb{Z}_b^\times$, sometimes called the *multiplicative group* modulo b, to be the subset of $\{1, 2, 3, \ldots b-1\}$ which are relatively prime to b.

The number of such elements of $\mathbb{Z}_b^\times$ is written $\phi(b)$, and called Euler's *totient* function. If b is prime then $\phi(b) = b - 1$. If b is composite then $\phi(b) < b - 1$.

The set $\mathbb{Z}_b^\times$ is *not* closed under addition. A counterexample is that $1, 2 \in \mathbb{Z}_3^\times$ but $1 + 2 \equiv 0 \notin \mathbb{Z}_3^\times$.

The set $\mathbb{Z}_b^\times$ is, however, closed under multiplication. The proof involves a slight generalisation of Euclid's lemma (also derivable from Bézout's lemma) that if a and c are relatively prime to b, then so is the product ac.

More importantly, each element a of $\mathbb{Z}_b^\times$ has a unique multiplicative inverse which we can write a^{-1}. To see why this works, let us use Bézout's lemma to write:

$$ax + by = 1$$

Then $ax \equiv 1 \mod b$ so x is the multiplicative inverse a^{-1}. We can then use the inverse to define division within $\mathbb{Z}_b^\times$ by $c \div a = a^{-1}c$.

4.4 Cyclic Groups

A group is said to be *cyclic* if there is an element to which we can repeatedly apply the group operation and generate the whole group.

The additive group $\mathbb{Z}_b$ is always cyclic, because we can consider the elements 1, $1+1$, $1+1+1$ and so on, which passes through all congruence classes before returning to zero after b steps.

What about the multiplicative group $\mathbb{Z}_b^\times$? Take the example of $b = 9$ and start with the element 2. Repeated multiplications give:

Exponent	Power	Mod 9
0	1	1
1	2	2
2	4	4
3	8	8
4	16	7
5	32	5
6	64	1

This covers all $\phi(9) = 6$ elements of $\mathbb{Z}_9$. In that case, we say that 2 is a *primitive root* of 9.

Not all elements of $\mathbb{Z}_9$ are primitive roots. For example, 4 is not a primitive root.

4.5 Classification of $\mathbb{Z}_b^\times$

With a lot more effort (not involving new concepts) it can be proved that:

- If b is prime, then $Z_b^\times = Z_b \backslash \{0\}$, $\mathbb{Z}_b$ is a field and its multiplicative group is cyclic.

- If b is 4, a power p^k of an odd prime or twice a power $2p^k$ of an odd prime, $\mathbb{Z}_b$ is not a field (some non-zero elements have no inverse) but $\mathbb{Z}_b^\times$ is cyclic under multiplication.

- There is no other b for which $\mathbb{Z}_b^\times$ is cyclic under multiplication.

Artin's conjecture is that any integer a which is neither -1 nor a square is a primitive root of $\mathbb{Z}_p^\times$ for infinitely many primes p. It is widely believed to be true but at the time of writing (2023) has not been proved.

5 Primes Among Large Integers

In this advanced section, we explore some facts about primes, particularly large primes. Euclid proved there are infinitely many primes by supposing (for a contradiction) there are finitely many. If there are finitely many primes, multiply them together and add one, calling that number x. Now x cannot be prime as it exceeds all the primes in the product. However, it is not composite either, because none of the primes in the list divides x. This is the contradiction.

Primes appear to become sparser for larger numbers, but never die out completely. The *twin prime* conjecture asserts that there are infinitely many pairs $(p, p+2)$ of primes that differ by 2. This is widely believed to be true but, at the time of writing (2023) has not been proved. Bertrand's postulate states that for each integer

$n \geq 2$ there is always a prime p with $n < p < 2n$. This is proven to be true (the proof is fiddly but not intrinsically hard).

5.1 Importance of Heuristics

A heuristic argument is a sequence of plausible guesses or conjectures that fall short of a rigorous proofs. They indicate why a statement might be true. Sometimes numerical analysis gives further weight to heuristic arguments. When a heuristic argument is well-supported numerically, mathematicians conclude it is probably true, and invest more effort in trying to prove it. This can avoid wasted effort trying to prove conjectures that are false. A good heuristic argument can sometimes be turned into a proof by filling the gaps.

There are many heuristic arguments in the theory of prime numbers. There is a heuristic argument about twin primes, estimating how many there should be, which accords closely to the number of twin primes we see from calculations.

We have seen Artin's conjecture about primitive roots. This is also backed up by heuristic arguments and also by numerical evidence. We will now look at some simpler heuristic arguments about the distribution of primes.

5.2 Some Interesting Questions

Let N be a very large integer. Let X be a random draw from the set 1 to N, with all choices equally likely.

(a) What is the probability that X is prime?

(b) Let Y be an independent draw from the same distribution as X. What is the probability that x and y are relatively prime?

5.3 The Average Gap Function

Let $k \geq 1$ be an integer. We define $g(k)$ to be the number of integers p in the range $2^k < p \leq 2^{k+1}$, divided by the number of prime integers in the same range. We call this the *average gap* between primes in that range. The number of primes in that range is then $2^k/g(k)$.

5.4 Estimating Proportions of Primes

Some values are tabulated below

k	Gap $g(k)$	List of primes
1	2	3
2	2	5, 7
3	4	11, 13
4	3.2	17, 19, 23, 29, 31
5	4.57...	37, 41, 43, 47, 53, 59, 61

We look at two ways of estimating the proportion of primes between 2^{2k} and 2^{2k+2}. The direct method is the number of primes divided by the length of the interval, which is a weighted average:

$$\frac{\frac{2^{2k}}{g(2k)}+\frac{2^{2k+1}}{g(2k+1)}}{3\times 2^{2k}}=\frac{1}{3}\times\frac{1}{g(2k)}+\frac{2}{3}\times\frac{1}{g(2k+1)}$$

The second way is to count all the numbers from $2^{2k}+1$ to 2^{2k+2}, knocking out first those divisible by 2 (half of them), then those divisible by 3 (a third of those remaining) and so on, for all relevant primes. The relevant primes are those up to 2^{k+1} since every composite number up to 2^{2k+2} has a prime factor at most 2^{k+1}. Heuristically, we might guess that:

$$\frac{1}{3}\left(\frac{1}{g(2k)}+\frac{2}{g(2k+1)}\right)\approx\prod_{p\leq 2^{k+1}}\left(1-\frac{1}{p}\right)$$

Replacing k by $k-1$ also gives:

$$\frac{1}{3}\left(\frac{1}{g(2k-2)}+\frac{2}{g(2k-1)}\right)\approx\prod_{p\leq 2^{k}}\left(1-\frac{1}{p}\right)$$

Dividing these equations gives:

$$\frac{\frac{1}{g(2k)}+\frac{2}{g(2k+1)}}{\frac{1}{g(2k-2)}+\frac{2}{g(2k-1)}}\approx\prod_{2^k<p\leq 2^{k+1}}\left(1-\frac{1}{p}\right)$$

Now we can estimate the right hand side, knowing that a proportion $1/g(k)$ of numbers in that range are prime, so assuming primes are evenly distributed over that interval, we have:

$$\prod_{2^k<p\leq 2^{k+1}}\left(1-\frac{1}{p}\right)\approx\prod_{j=2^k+1}^{2^{k+1}}\left(\frac{j-1}{j}\right)^{1/g(k)}=\left(\frac{2^k}{2^{k+1}}\right)^{1/g(k)}$$

Putting this together, and introducing a temporary function $u(2k)$, we have:

$$\begin{aligned}\frac{3}{u(2k)} &= \frac{1}{g(2k)} + \frac{2}{g(2k+1)} \\ &\approx \left(\frac{1}{g(2k-2)} + \frac{2}{g(2k-1)}\right) \times 2^{-1/g(k)} \\ &= \frac{3}{u(2k-2)} \times 2^{-1/g(k)}\end{aligned}$$

so:

$$u(2k) \approx 2^{1/g(k)} u(k-2)$$

We propose the formulas:

$$\begin{aligned}g(2k) &= \frac{g(2k-1)}{4} + \frac{u(2k)}{3} \\ &\quad + \frac{1}{12}\sqrt{9g(2k-1)^2 + 16u(2k)^2} \\ g(2k+1) &= -\frac{g(2k-1)}{2} + 2\frac{u(2k)}{3} \\ &\quad + \frac{1}{6}\sqrt{9g(2k-1)^2 + 16u(2k)^2}\end{aligned}$$

This (with some algebra) satisfies the definition of $u(2k)$. It also produces a smooth sequence of values as $g(2k-1)$, $g(2k)$ and $g(2k+1)$ are in arithmetic progression.

This gives us two ways of guessing $g(k)$ for large k:

- Calculating directly by enumerating the primes (very hard work)

- Applying the heuristic argument, which is much easier but is at best approximately true.

It is *much* easier to prove results from the heuristic argument. For example, the heuristic approximation implies (with some work, involving logarithms) that, for large k, the average gap $g(k)$ between prime numbers from $2^k + 1$ to 2^{k+1} is proportional to k. This *prime number theorem* can also be proved for rigorously for actual primes rather than some heuristic approximation, but that proof is very much more difficult.

5.5 Probability of Relative Primality

Let us take a single prime p_1. What is the probability that a random positive integer is divisible by p_1? The answer must be $\frac{1}{p_1}$.

The probability that two independent integers X and Y are both divisible by p_1 is $\frac{1}{p_1^2}$, for similar reasons.

So the probability that at most one of X and Y is divisible by p_1 is $1 - \frac{1}{p_1^2}$.

Now suppose we have a finite sequence $p_1, p_2, \ldots p_k$ of primes. The probability that for all of these primes at most one of X and Y is a multiple of p is the product:

$$\prod_{j=1}^{k} \left(1 - \frac{1}{p_j^2}\right)$$

Now if we consider a large enough set of primes, this is the probability that X and Y are relatively prime. The probability of relative primality is then the infinite product over all primes:

$$\prod_p \left(1 - \frac{1}{p^2}\right) = \frac{6}{\pi^2}$$

You are not expected to prove the right hand side of this equation.

6 Problem Solutions

6.1 Elephant Problem

Is your animal grey, with big ears and a trunk?

How does it work?

Multiplying your age by 9 gives a multiple of 9. So the process of adding digits ends up with 9 whatever your age.

Then the trick relies on there not being many countries beginning with D (Dominican Republic, Djibouti?) and few animals beginning with E.

6.2 Factorial Problem

We seek the smallest n such that $n!$ ends in ten zeroes. We could do this by brute force, but there are easier ways.

To end in 10 zeroes, $n!$ must be divisible by 10^{10}, which means it must be divisible both by 5^{10} and by 2^{10}.

The highest power of 5 that divides $n!$ is (close to) the number of multiples of 5 in the set $\{1, 2, 3, \ldots n\}$, which is $\lfloor \frac{n}{5} \rfloor$. That suggests we need $n = 50$ to have 5^{10} dividing $n!$. But this argument is not quite right, because one of those factors is 25, which is divisible by 5^2. So 5^{10} is a factor of 45!, but not of any smaller factorial. By the same logic, 2^{10} certainly divides 45!.

More generally, the highest power of a prime p dividing $n!$ is:

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \left\lfloor \frac{n}{p^4} \right\rfloor + \ldots = \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor$$

Remark: One proof of Bertrand's postulate uses this expression and considers the highest power of p that divides the integer

$$\frac{(2n)!}{(n!)^2}$$

After many lines of work, the assumption of no primes between n and $2n$ leads to a contradiction.

6.3 Happy Numbers Problem

We need to search all positive integers n to see what happens to the sequence n, $h(n)$, $h(h(n))$ etc. The challenge is to reduce this to a finite problem we can search by hand.

Start with some test calculations on numbers up to 100.

The happy numbers up to 100 are 1, 7, 10, 13, 19, 23, 28, 31, 32, 44, 49, 68, 70, 79, 82, 86, 91, 94, 97, 100.

All others are unhappy and eventually lead to the cycle 4, 16, 37, 58, 89, 145, 42, 20, 4 ....

What about numbers bigger than 100? It turns out then that $h(n) < n$ for $n \geq 100$ so all of these reduce to below 100 which we have checked manually.

We will show that $h(n) < n$ for all $n \geq 100$ in several steps, starting with $n \geq 1000$.

Suppose a number n has d digits. Then

$$10^{d-1} \leq n < 10^d$$

In that case, as all digits are at most 9, we have:

$$h(n) \leq 81 \times d$$

Now I claim the following lemma. Let $d \geq 4$. Then $81d < 10^{d-1}$. To prove this, the result clearly holds for $d = 4$ as $324 < 1000$. But then if the result holds for some d, it holds for $d+1$ as:

$$81(d+1) \leq 81(d+1) + 81(9d-1) = 10 \times 81d < 10^d$$

The last equation holds on multiplying the relation $81d < 10^{d-1}$ by 10.

From this lemma, then for $n \geq 1000$ we have $h(n) \leq 81d < 10^{d-1} \leq n$, so $h(n) < n$.

Now consider three-digit numbers

$$n = 100a + 10b + c$$
$$h(n) = a^2 + b^2 + c^2 \leq 9a + 9b + 9c$$

As $a \geq 1$, we have $8c \leq 72 \leq 72a$ and so

$$9a + 9b + 9c \leq 9a + 9b + c + 72a < 100a + 10b + c$$

So $h(n) < n$ which completes the proof. The only cases we have to check manually are starting with $n \leq 99$, which we have already done.

Question: Can you generalise the result to arbitrary base b?

6.4 EGMO Selection 2022 Q1

The question concerns solutions to:

$$3^m = 7^n + 2$$

in positive integers n. We have to show that n is odd.

Most students spotted the solution $3^2 = 7 + 2$ where $n = 1$, which is of course odd. As powers of 3 are few and far between, while powers of 7 spread out rapidly, it seems very unlikely that $7^n + 2$ would again be a power of 3. So, most likely, the only solution is $m = 2$, $n = 1$ in which case of course it follows that n is odd. Sadly, it is very hard to prove that is the only solution.

Some students considered the last digit, or the last two digits of 3^m and 7^n. We have the following tables, which imply either $m \equiv 2 \mod 20$ and $n \equiv 1 \mod 4$, or $m \equiv 1 \mod 20$ and $n \equiv 0$ mod 4. We cannot from this conclude n is odd.

m	3^m	n	7^n	$7^n + 2$
mod 20	mod 100	mod 4	mod 100	mod 100
0	1	0	1	3
1	3	1	7	9
2	9	2	49	51
3	27	3	43	45
4	81			
5	43			
6	29			
7	87			
8	61			
9	83			
10	49			
11	47			
12	41			
13	23			
14	69			
15	7			
16	21			
17	63			
18	89			
19	67			

Solution: Look at other number bases, specifically base 4 and base 7.

Suppose for a contradiction that n is even. Then $7^n \equiv 1 \mod 4$, which implies $3^m \equiv 3 \mod 4$ and m is odd.

Calculating modulo 7, odd powers $3^m \mod 7$ are $3, 6, 5, 3, \ldots$ contradicting the implication of the given equation that $3^m \equiv 2 \mod 7$.

Variant on Proof: We prove the result by looking at congruences, first modulo 7 and then modulo 4.

Working modulo 7, we have $3^m \equiv 2 \mod 7$. Working through powers of 3 modulo 7, this is equivalent to $m \equiv 2 \mod 6$, so we can write $m = 6a + 2$.

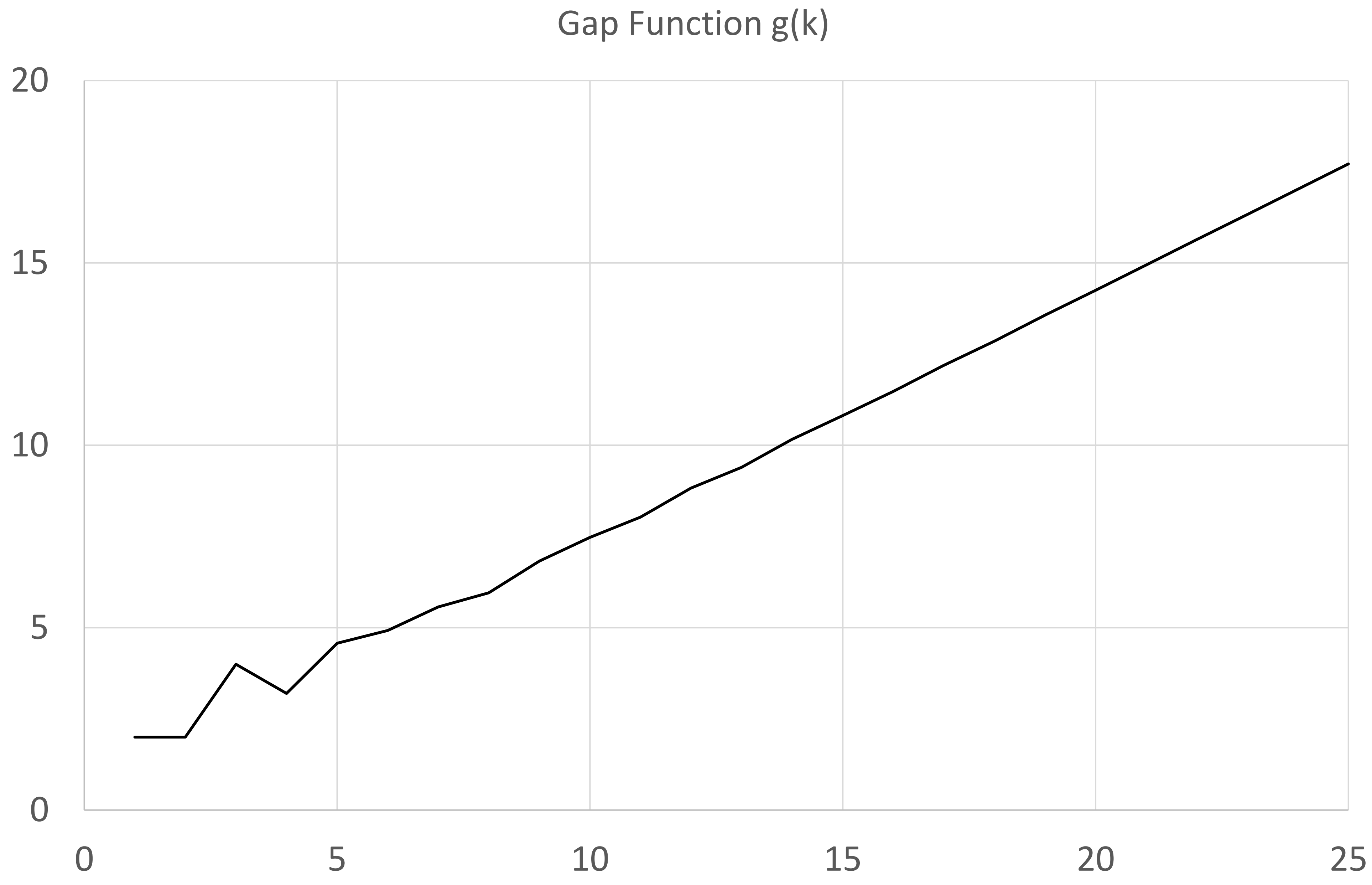
Now suppose for a contradiction that $n = 2b$ is even. In that case we must have:

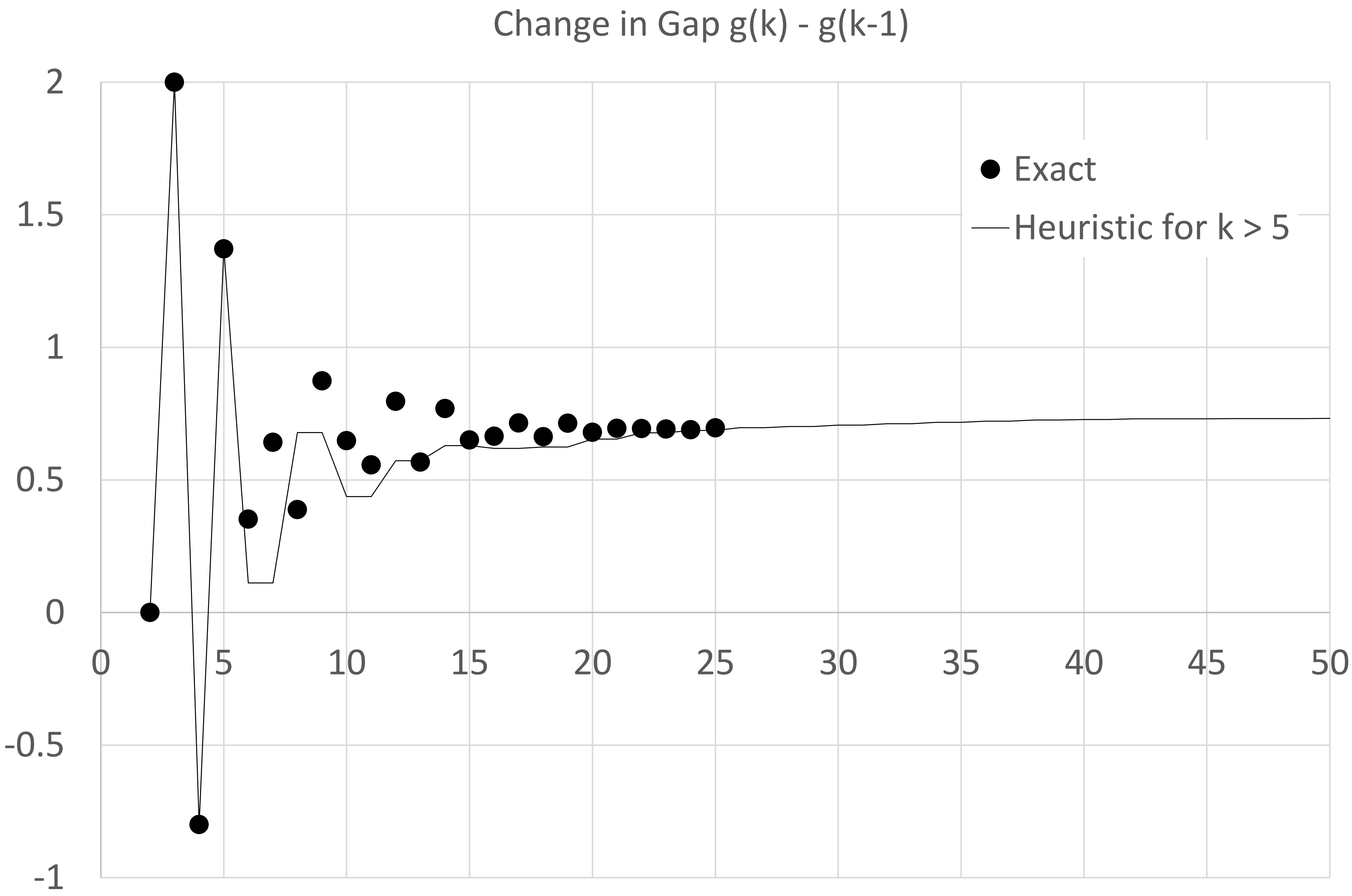
$$2 = 3^m - 7^n = 3^{6a+2} - 7^{2b} = (3^{3a+1} - 7^b)(3^{3a+1} + 7^b)$$

The right hand side is the product of two even numbers so must be a multiple of 4, which is a contradiction.

The final contradiction can be phrased on other ways. Viewing the original equation modulo 4, given that m is even, we have $1 \equiv (-1)^n + 2 \mod 4$ which implies n is odd.

Equivalently, we can interpret the whole equation modulo 28 from the beginning, to find the same result.


Gap Function g(k)
20
15
10
5
0
0
5
10
15
20
25


Change in Gap g(k) - g(k-1)
2
1.5
1
0.5
0
-0.5
-1
0
5
10
15
20
25
30
35
40
45
50
● Exact
Heuristic for k > 5