A-Star 2016 Winter Math Camp

Justin Stevens

26th December, 2016

1 Introduction

Welcome to A-Star Winter Math Camp 2016! This is my fourth A-Star camp.

- I've attended once as a student before.
- I've taught the AMC class twice before in the summer of 2015 and 2016.
- Number Theory and Geometry are my favourite subjects to teach :).

1.1 Schedule

Time	Subject
9-10:30 AM	Number Theory
10:45AM-12:15PM	Algebra
1:45-3:15PM	Geometry
3:30-5:00PM	Counting

Table 1: A-Star Teaching Schedule

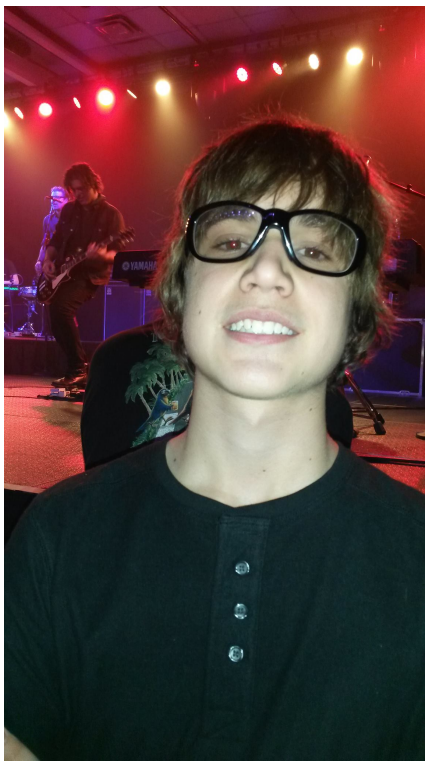
1.2 Icebreaker Activity

Three Truths and a Lie

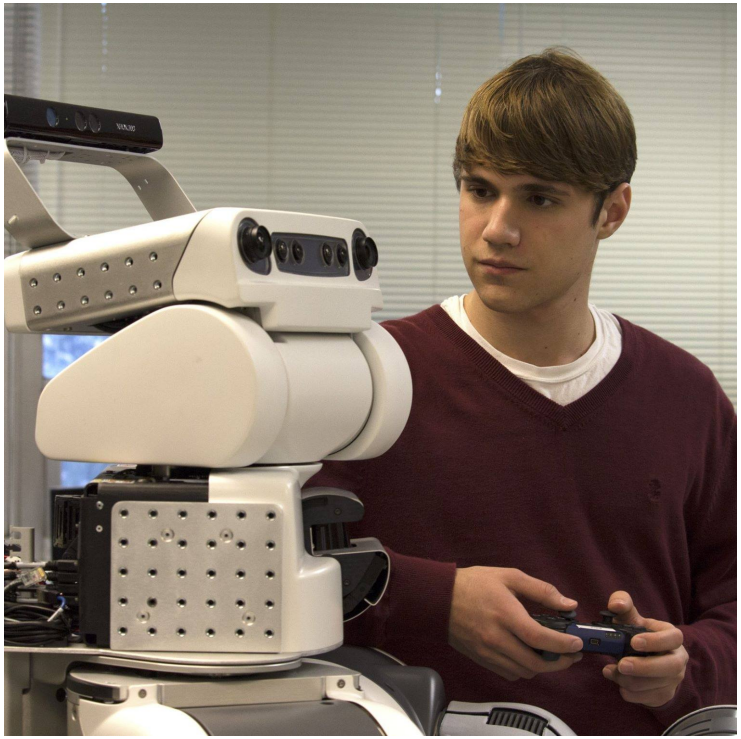
Write down three truths and one lie about yourself on your piece of paper. I'll guess which one is the lie! Good luck guessing which one is my lie.

- I've seen over 100 different bands live in concert.
- I've programmed a human sized robot.
- My family has 2 dogs.
- I've competed in and won a crib race.

Concerts: Truth



Robot: Truth



Dogs: Lie!

We have 5 cats though...

Crib Race??: Truth

Celebration!

Math Time

2 Divisibility Rules

- 2 - Last digit is even.
- 3 - Sum of the digits is divisible by 3.
- 4 - Number formed by last two digits is divisible by 4.
- 5 - Last digit is either 0 or 5.
- 6 - Divisibility rules for both 2 and 3 hold.
- 7 - Take the last digit of the number and double it. Subtract this from the rest of the number. Repeat the process if necessary. Check to see if the final number obtained is divisible by 7. [2]

Lucky Seven

Definition

When a divides b, we write $a \mid b$. Another way of saying this is that b is a multiple of a.

Choose **one** number below and determine if it is divisible by 7.

- 1729
- $2,718,281$
- $16,180,339$
- $31,415,926,535$

Taxicab Number

"It is a very interesting number; it is the smallest number expressible as the sum of two positive cubes in two different ways." - Srinivasa Ramanujan (1919)

$$\begin{aligned} 1729 &\rightarrow 172 - 2 \cdot 9 = 154 \\ 154 &\rightarrow 15 - 2 \cdot 4 = 7 \end{aligned}$$

Therefore, 1729 **is** divisible by 7.

Can you find the two ways Ramanujan referenced?

Euler's Number

$$\begin{aligned} 2718281 &\rightarrow 271828 - 2 \cdot 1 = 271826 \\ 271826 &\rightarrow 27182 - 2 \cdot 6 = 27170 \\ 27170 &\rightarrow 2717 - 2 \cdot 0 = 2717 \\ 2717 &\rightarrow 271 - 2 \cdot 7 = 257 \\ 257 &\rightarrow 25 - 2 \cdot 7 = 11 \end{aligned}$$

Therefore, 2718281 is **not** divisible by 7.

More on Euler's number (e) during Algebra lectures!

The Golden Ratio - $\phi = \frac{1+\sqrt{5}}{2} = 1.6180339\cdots$

$$\begin{aligned}
16180339 &\to 1618033 - 2 \cdot 9 = 1618015 \\
1618015 &\to 161801 - 2 \cdot 5 = 161791 \\
161791 &\to 16179 - 2 \cdot 1 = 16177 \\
16177 &\to 1617 - 2 \cdot 7 = 1603 \\
1603 &\to 160 - 2 \cdot 3 = 154 \\
154 &\to 15 - 2 \cdot 4 = 7
\end{aligned}$$

Hence, 16180339 **is** divisible by 7.

2.1 Pi-ython Program

$31,415,926,535$ is too big of a number. Therefore, I wrote a computer program!

Seven.ipynb

It **is** divisible by 7.

AMC Number Theory

In [8]:
```
#Author:  Justin Stevens
#A-Star Winter Math Camp, 2016
#Determines if a number is divisible by 7

def divis_sev(x):
    """Inputs an integer x and prints out a list of numbers generated by following the -2 last digit rule
        Returns True or False based on whether the integer is divisible by 7."""
    cur_num=x
    while cur_num>7:
        print(cur_num)
        trunc_num=cur_num//10  #Removes last digit from the number
        last_dig=cur_num%10   #Stores the last digit in last_dig
        cur_num=trunc_num-2*last_dig  #Applies the divisibility rule for 7
    if cur_num>0:
        print(cur_num)
    if cur_num%7==0:
        return True
    else:
        return False
```

In [13]:
```
divis_sev(31415926535)
```

```
31415926535
3141592643
314159258
31415909
3141572
314153
31409
3122
308
14
```

Out[13]: True

2.2 Explanation of the Magic

Let the number that we want to determine its divisibility by 7 be N. Let the last digit of N be x. Then, we can represent N as

$$N = 10a + x.$$

Note that we want to prove that 7 divides N implies that 7 also divides $a - 2x$.

To do so, we will multiply N by some integer.

Magic Continued

The magic integer is 5. The reason is because 5 and -2 leave the same remainder when dividing by 7.

If 7 divides N, then 7 should also divide $5N$. From the expression above for N, we have

$$5N = 50a + 5x.$$

Now, the question is, how do we get $a - 2x$ out of this?

Moving Around

We think to take the difference between $5N$ and $a - 2x$. Since we know that $5N$ is divisible by 7 if the difference is divisible by 7, then $a - 2x$ must also be divisible by 7.

Using the expression for $5N$ we found on the previous slide,

$$\begin{aligned} 5N - (a - 2x) &= 50a + 5x - (a - 2x) \\ &= 49a + 7x. \end{aligned}$$

This is clearly a multiple of 7, therefore, our proof is complete!

2.3 More Divisibility Rules

- 8 - The numbers formed by the last three digits are divisible by 8.
- 9 - The sum of the digits is divisible by 9.
- 10 - The number ends in 0.
- 11 - Let E be the sum of the digits in an even place. Let O be the sum of the digits in an odd place. 11 must divide the difference $E - O$ for the number to be divisible by 11.
- 12 - Combination of divisibility rules for 3 and 4.
- 13 - Same as the divisibility rule for 7, except replace $-2x$ with $+4x$.

2.4 Eleven

Let $N = 1734579$. We check to see if N is divisible by 11. We begin labeling the digits beginning by labeling 9 as 0. Why 0? Think of how lists are stored in Python! Then, 7 is labeled as 1, 5 is labeled as 2, and so forth. We make all of the even digits red and all of the odd digits blue.

$$N = 1734579.$$

Then, we calculate the sum of the even digits and odd digits:

$$E = 1 + 3 + 5 + 9 = 18\,, O = 7 + 4 + 7 = 18.$$

Note that $E - O = 18 - 18 = 0$, which is divisible by 11, therefore, 11 divides N.

3 Factorials

One of my favourite problems in number theory has to do with factorials. The factorial of a positive integer n is defined as the product of all the natural numbers less than or equal to n. In other words,

$$n! = n \times (n-1) \times (n-2) \times \cdots 1.$$

For instance, $6! = 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 720$.

3.1 Zeros at the end of a Factorial

Note that $6! = 720$ ends in one zero. The number

$$25! = 15511210043330985984000000$$

ends in 6 zeros.

Problem

How many zeros does $100!$ end in?

How Does Zero Work?

Zeros at the end of a number come from powers of 10. For instance, we can rewrite

$$25! = 15511210043330985984 \times 10^6.$$

Therefore, the problem is equivalent to finding the largest power of 10 that divides $100!$.

Definition

Define $v_p(n)$ to be the integer e such that $p^e \mid n$, but $p^{e+1} \nmid n$. Another way to write this is $p^e \parallel n$.

3.2 V for Vendetta

We desire to find $v_{10}(100!)$. Since $10 = 2 \cdot 5$, the largest power of 10 that divides $100!$ is the **minimum** of $v_2(100!)$ and $v_5(100!)$.

We begin by calculating $v_2(100!)$. We write out

$$100! = 100 \cdot 99 \cdot 98 \cdot 97 \cdots 3 \cdot 2 \cdot 1.$$

Consider all the numbers in the product above.

How many of them are multiples of 2? Multiples of 4? Multiples of 8? Multiples of 16? Multiples of 32? Multiples of 64?

Floor Function

The number of multiples of 2 in $100!$ is simply the number of even numbers in the product. Half of the numbers are even, therefore, there are $\frac{100}{2} = 50$ multiples of 2.

For other powers of 2 that do not evenly divide into 100, we must introduce the floor function.

Definition

The floor function of a real number x is defined as the largest integer less than or equal to x. In other words, it is the result of truncating x. For instance, $\lfloor 3.14159 \rfloor = 3$ and $\lfloor -16.3 \rfloor = -17$.

Using our new friend, the floor function, we answer the question about multiples.

- There are $\lfloor \frac{100}{2} \rfloor = 50$ multiples of 2.
- There are $\lfloor \frac{100}{4} \rfloor = 25$ multiples of 4.
- There are $\lfloor \frac{100}{8} \rfloor = 12$ multiples of 8.
- There are $\lfloor \frac{100}{16} \rfloor = 6$ multiples of 16.
- There are $\lfloor \frac{100}{32} \rfloor = 3$ multiples of 32.
- There are $\lfloor \frac{100}{64} \rfloor = 1$ multiple of 64.

How Much Power Does 2 Have?

I claim that the number of powers of 2 in $100!$ is the sum of all the numbers above:

$$50 + 25 + 12 + 6 + 3 + 1 = 97.$$

For the numbers in the product $100!$ that have a highest power of 2^1, we have counted them once in the number 50.

For those that have a highest power of 2^2, they contribute a total of 2 to the product $100!$. We have counted them *once already* in the number 50 since they are also multiples of 2. Since they should contribute a total of 2 to the product, we add them one time more in the number 25.

Similarly, for the numbers that have a highest power of 2^3, they should contribute a total of 3 to the product $100!$. They have been counted once in the number 50 and once in the number 25, therefore, we should add them one time more in the number 12.

This logic extends to the powers $2^4, 2^5$, and 2^6.

Hence, $v_2(100!) = 97$. Are we done now?

Forgot About Magic 5

Nope! We also must compute $v_5(100!)$. We use the same method as above to determine that:

- There are $\lfloor \frac{100}{5} \rfloor = 20$ multiples of 5^1.
- There are $\lfloor \frac{100}{25} \rfloor = 4$ multiples of 5^2.

Therefore, $v_5(100!) = 20 + 4 = 24$.

Finishing the Problem

Therefore, $5^{24} \parallel 100!$ and $2^{97} \parallel 100!$. Hence, the largest power of 10 that divides $100!$ is 24 and the number of zeros at the end of $100!$ is $\boxed{24}$.

We indeed verify through the use of Mathematica that

$$100! = 106992388562667004907159682643816214685929638952175999932299156089414639761565182862536979208272237582511852109168640000000000000000000000.$$

3.3 Legendre's Formula

Adrien-Marie Legendre (1752-1833) generalized this problem.

Theorem

The number of powers of a prime p that divide into $n!$ is

$$v_p(n!) = \sum_{k=1}^{\infty} \left(\left\lfloor \frac{n}{p^k} \right\rfloor \right).$$

Summation Symbol

The $\sum$ symbol represents a summation. The k at the bottom is the variable that is being summed over. The 1 and ∞ are the ranges for the sum. For instance,

$$\sum_{k=1}^{4}(k^2) = 1^2 + 2^2 + 3^2 + 4^2.$$

In the case of the sum above,

$$\sum_{k=1}^{\infty}\left(\left\lfloor\frac{n}{p^k}\right\rfloor\right) = \lfloor\frac{n}{p^1}\rfloor + \lfloor\frac{n}{p^2}\rfloor + \lfloor\frac{n}{p^3}\rfloor + \lfloor\frac{n}{p^4}\rfloor + \cdots.$$

Define $s_p(n)$ to be the sum of the digits when the number n is expressed in base p. Then, an alternative way of writing Legendre's Formula is

$$v_p(n!) = \frac{n - s_p(n)}{p-1}.$$

For instance, 100 in base 2 is $100 = 1100100_2$. The sum of the digits is $s_2(100) = 3$. Therefore,

$$v_2(100!) = \frac{100-3}{1} = 97.$$

Furthermore, $100 = 400_5$. The sum of the digits is $s_5(100) = 4$. Therefore,

$$v_5(100!) = \frac{100-4}{4} = 24.$$

4 Euclid's Elements

Around the time of 300 BC, a great Greek mathematician rose from Alexandria by the name of Euclid. He wrote a series of 13 books known as *Elements*. Elements is thought by many to be the most successful and influential textbook ever written. It has been published the second most of any book, next to the Bible. [3]

The book covers both Euclidean geometry and elementary number theory. This chapter will focus solely on **Book VII, Proposition 1.**

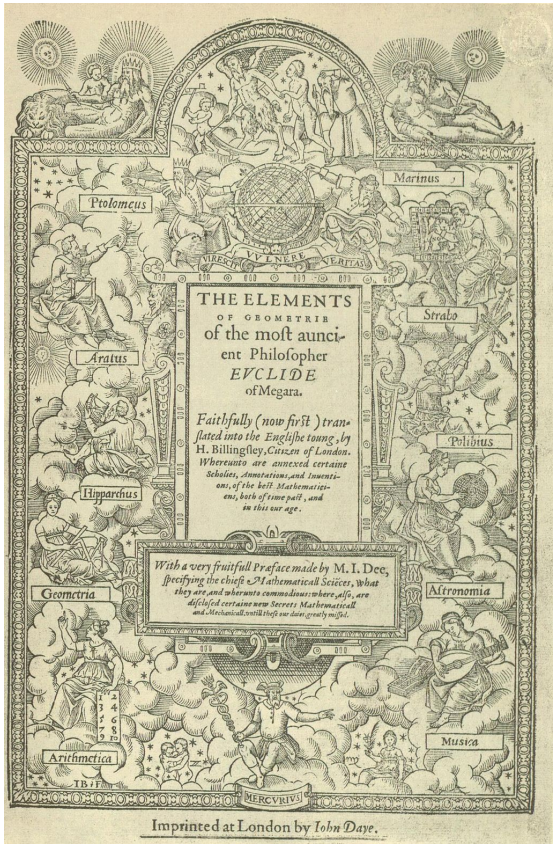


Figure 1: "Frontispiece of Sir Henry Billingsley's first English version of Elements in 1570" - Source: Wikipedia [3]

4.1 Division Algorithm

The way division is commonly introduced in primary school is seen in the picture below:

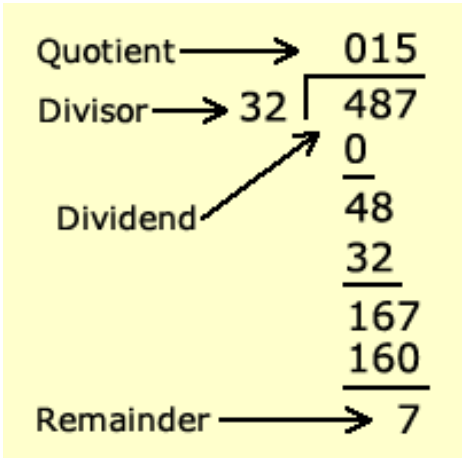


Figure 2: Source: CalculatorSoup

The division algorithm rigorizes this process. In the integers, $\mathbb{Z}$, the statement of the division algorithm is below:

Theorem

For every integer pair a, b, there exists distinct integer quotients and remainders, q and r, that satisfy

$$a = bq + r \quad | \quad 0 \leq r < |b|.$$

The proof of this comes from either the well-ordering principle or induction. We show the proof involving the well-ordering principle.

Proof. We consider the case when b is positive for simplicity. Consider the set

$$S = \{a - bq \quad | \quad q \in \mathbb{Z}^+, \, a - bq > 0\}.$$

In other words, this set consists of the positive integer values of $a - bq$ for q also being a positive integer. In order to continue with the proof, we must cite a famous Lemma from set theory. [4]

Lemma (Well-ordering principle)
Every non-empty subset of positive integers has a least element.

Therefore, the set S has a *minimum element*, say when $q = q_1$ and $r = r_1$. I will prove that $0 \leq r_1 < b$.

Assume for the sake of contradiction otherwise and that

$$a - bq_1 = r_1 \geq b. \tag{1}$$

However, then I claim that $a - b(q_1 + 1)$ is a smaller member of set S.

Indeed, since $q_1 + 1 \in \mathbb{Z}^+$, the first condition is satisfied.

Furthermore, using 1, $a - b(q_1 + 1) = a - bq_1 - b \geq 0$. Therefore, both conditions are satisfied, and we have found a smaller member of set S. This contradicts the minimality of q_1 and r_1. Hence, $0 \leq r_1 < b$. $\square$

Examples of Division Algorithm

When $a = 102$ and $b = 18$, applying the division algorithm gives

$$102 = 18 \times 5 + 12,$$

therefore $q = 5$ and $r = 12$.

Exercise

Find q and r when $a = 2016$ and $b = 37$.

Definition

We define the **greatest common divisor** of two integers to be the largest positive integer that divides both of the numbers.

Note that in the previous example, $\gcd(a, b) = \gcd(102, 18) = 6$. Similarly, $\gcd(b, r) = \gcd(18, 12) = 6$.

In the other example, we have $2016 = 37 \cdot 54 + 18$. Hence, $q = 54$ and $r = 18$. Furthermore, $\gcd(a, b) = \gcd(2016, 37) = 1$ and $\gcd(b, r) = \gcd(37, 18) = 1$.

Therefore, we conjecture that in general, $\gcd(a, b) = \gcd(b, r)$.

4.2 Book VII, Proposition 1

"When two unequal numbers are set out, and the less is continually subtracted in turn from the greater, if the number which is left never measures the one before it until a unit is left, then the original numbers are relatively prime." - Euclid

Theorem

Given naturals a, b, upon using the division algorithm to obtain a quotient and remainder, q, r, one has that $\gcd(a, b) = \gcd(b, r)$.

Proof. I claim that the set of common divisors between a and b is the same as the set of common divisors between b and r.

If d is a common divisor of a and b, then since d divides both a and b, d divides all linear combinatinations of a and b. Therefore, $d \mid a - bq = r$, meaning that d is also a common divisor of b and r.

Conversely, if d is a common divisor of b and r, then d is a common divisor of all linear combinations of b and r, therefore, $d \mid bq + r = a$. Hence, d is also a common divisor of a and b.

We have established that the two sets of common divisors are equivalent, therefore, the greatest common divisor must be equivalent. $\square$

Theorem (Euclidean Algorithm)

For two natural a, b, $a > b$, to find $\gcd(a, b)$ we use the division algorithm repeatedly

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\cdots \\ r_{n-2} &= r_{n-1}q_n + r_n \\ r_{n-1} &= r_nq_{n+1}. \end{aligned}$$

Then we have $\gcd(a, b) = \gcd(b, r_1) = \cdots = \gcd(r_{n-1}, r_n) = r_n$.

Examples of Euclidean Algorithm

Note that the greatest common divisor is the *last non-zero remainder*.

- Find $\gcd(301, 603)$.
- Find $\gcd(110, 490)$.
- Find $\gcd(153, 289)$.
- Find $\gcd(481, 2627)$.
- $\star$ Find $\gcd(1558, 8774)$.

We'll discuss our findings in a few minutes!

Problem

Find $\gcd(301, 603)$.

Solution. Note that

$$603 = 301 \times 2 + 1.$$

Therefore, by the Euclidean Algorithm, we have

$$\gcd(603, 301) = \gcd(1, 301) = \boxed{1}.$$

□

Problem

Find $\gcd(110, 490)$.

Solution. We repeatedly use the division algorithm as follows:

$$\begin{aligned} 490 &= 110 \times 4 + 50 \\ 110 &= 50 \times 2 + \boxed{10} \\ 50 &= 10 \times 5. \end{aligned}$$

Therefore $\gcd(110, 490) = \boxed{10}$. □

Problem

Find $\gcd(153, 289)$.

Solution. We repeatedly use the division algorithm as follows:

$$\begin{aligned} 289 &= 153 \times 1 + 136 \\ 153 &= 136 \times 1 + \boxed{17} \\ 136 &= 17 \times 8 + 0. \end{aligned}$$

Therefore $\gcd(153, 289) = \boxed{17}$. □

Problem

Find $\gcd(481, 2627)$.

Solution. We repeatedly use the division algorithm as follows:

$$\begin{aligned} 2627 &= 481 \times 5 + 222 \\ 481 &= 222 \times 2 + \boxed{37} \\ 222 &= 37 \times 6 + 0 \end{aligned}$$

Therefore $\gcd(481, 2627) = \boxed{37}$. □

4.3 Mathematica Function: QuotientRemainder

Problem

Find $\gcd(1558, 8774)$.

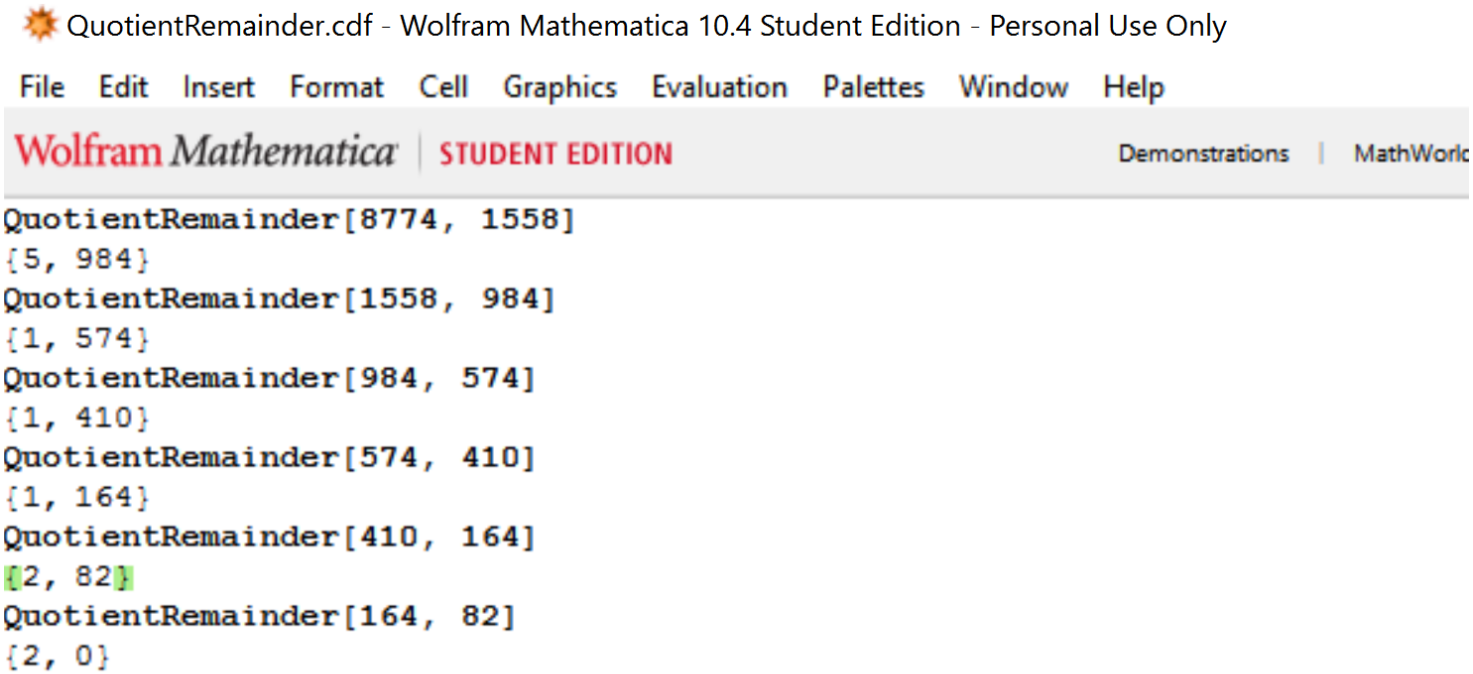
Solution. I'm going to use Mathematica to assist me. On Mathematica, I can compute the quotient and remainder with the command

QuotientRemainder(8774, 1558).

The output of this command is $\{5, 984\}$. Here, $q = 5$ and $r = 984$.

Therefore, $8774 = 1558 \times 5 + 984$.

From this image, can you determine what $\gcd(1558, 8774)$ is? □



5 Contest Style Euclidean Algorithm Problems

Problem (AIME 1986)

What is the largest positive integer n such that $n^3 + 100$ is divisible by $n + 10$?

Problem (AIME 1985)

The numbers in the sequence $101, 104, 109, 116, \ldots$ are of the form $a_n = 100 + n^2$, where $n = 1, 2, 3, \ldots$. For each n, let d_n be the greatest common divisor of a_n and a_{n+1}. Find the maximum value of d_n as n ranges through the positive integers.

5.1 AIME 1986 #5

Solution. We desire to find out when $n+10$ divides n^3+100. To get a good sense for the problem, we attempt to divide n^3+100 by $n+10$ using unknown coefficients:

$$\begin{aligned} n^3+100 &= (n+10)\left(n^2+an+b\right)+c \\ &= n^3+n^2(10+a)+n(b+10a)+10b+c. \end{aligned}$$

Next, we must equate coefficients on the two sides in order to find the quotient and remainder.

Equating coefficients yields

$$\begin{aligned} 10 + a &= 0 \\ b + 10a &= 0 \\ 10b + c &= 100. \end{aligned}$$

Solving this system of equations gives $a = -10, b = 100, c = -900$. Therefore,

$$n^3 + 100 = (n + 10)(n^2 - 10n + 100) - 900.$$

If $n+10$ divides n^3+100, then we must have $\gcd(n^3+100, n+10) = n+10$.
By the Euclidean Algorithm, $\gcd(n^3+100, n+10) = \gcd(900, n+10)$.
Therefore, equating the two, we must have

$$\gcd(900, n+10) = n+10.$$

Hence, the largest possible value of n is when $n = \boxed{890}$. □

5.2 AIME 1985 #13

Problem

The numbers in the sequence $101, 104, 109, 116, \ldots$ are of the form $a_n = 100 + n^2$, where $n = 1, 2, 3, \ldots$. For each n, let d_n be the greatest common divisor of a_n and a_{n+1}. Find the maximum value of d_n as n ranges through the positive integers.

Solution. We begin by writing d_n as the greatest common divisor of a_n and a_{n+1}:

$$d_n = \gcd(a_n, a_{n+1}) = \gcd(n^2 + 100, (n+1)^2 + 100).$$

If d_n divides both a_n and a_{n+1}, then it must divide their difference:

$$\begin{aligned} d_n &\mid \Big((n+1)^2 + 100\Big) - \Big(n^2 + 100\Big) \\ d_n &\mid 2n + 1. \end{aligned}$$

Hence, $d_n = \gcd(n^2 + 100, 2n + 1)$.

Since $2n + 1$ is odd, d_n must also be odd. Therefore, we can multiply $n^2 + 100$ by 4 without affecting the greatest common divisor:

$$d_n = \gcd(4n^2 + 400, 2n + 1).$$

Can you think of how to simplify the expression from here?

We use difference of squares to observe $4n^2 - 1 = (2n+1)(2n-1)$.

We add 401 to both sides of the equation to get $4n^2 + 400$:

$$4n^2 + 400 = (2n+1)(2n-1) + 401.$$

Therefore, by the Euclidean algorithm, $d_n = \gcd(2n+1, 401)$.

This is maximized when $n = 200$ and $d_n = \boxed{401}$. $\square$

6 $\star$ Division in Other Domains

While the statement of the division algorithm may now seem like a mere formality, it is actually very vital to our number system. Without the division algorithm, we would not have unique prime factorization amongst the integers.

Furthermore, it is applicable when considering domains other than the integers, such as $\mathbb{Z}[i]$ (Gaussian integers) and $\mathbb{Z}[\omega]$ (Eisenstein integers).

With Respect to Gauss

The Gaussian integers are lattice points in the complex plane. [5]

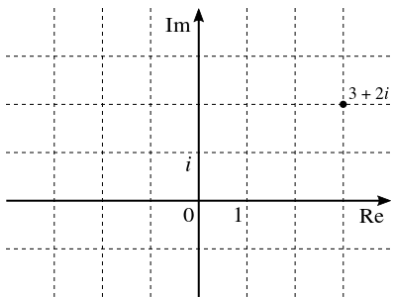


Figure 3: Source: Wikipedia

Rigorously, they are defined as the set

$$S = \{a + bi \quad | \quad a, b \in \mathbb{Z}\}.$$

6.1 Gaussian Division Problem [1]

Problem

Find the quotient and remainder when we divide $z = -1 + 4i$ by $w = 1 + 2i$ in $\mathbb{Z}[i]$.

To begin with, before I give a rigorous definition of division in $\mathbb{Z}[i]$, I want you to explore possible quotients and remainders. That is, with no restrictions other than sticking to the Gaussian integers, find a pair q, r such that

$$z = -1 + 4i = (1 + 2i)q + r = wq + r.$$

We'll discuss our findings in a few minutes!

Here are some examples of possible pairs (q, r):

- $-1+4i = (1+2i)(1) + (-2+2i)$, therefore, $(q, r) = (1, -2+2i)$.
- $-1+4i = (1+2i)(2) + (-3)$, therefore, $(q, r) = (2, -3)$.
- $-1+4i = (1+2i)(i) + (1+3i)$, therefore, $(q, r) = (i, 1+3i)$.
- $-1+4i = (1+2i)(-i) + (-3+5i)$, therefore, $(q, r) = (-i, -3+5i)$.
- $-1+4i = (1+2i)(1+i) + i$, therefore, $(q, r) = (1+i, i)$.

Summarizing in a Table

Quotient	Remainder
1	$-2+2i$
2	-3
i	$1+3i$
$-i$	$-3+5i$
$1+i$	i

Table 2: Division Algorithm applied to $z=-1+4i$ divided by $w=1+2i$.

Magnitude

Now the question lies on which remainder is best. When we worked with integers, we simply had the condition $0 \leq r < |b|$. However, how do we compare the values of two imaginary numbers such as $-2+2i$ and -3?

In order to do this, we recall the magnitude of a complex number $z = a+bi$. By definition,

$$|z| = \sqrt{z\bar{z}} = \sqrt{a^2+b^2},$$

where $\bar{z}$ is the complex conjugate.

The magnitude was also equivalent to the Euclidean distance between a point in the complex plane and the origin.

6.2 Norms

Since with Euclidean Domains, we want to work with integers, we define the **norm** of a complex number $z = a + bi$ to be

$$N(a + bi) = z\bar{z} = a^2 + b^2.$$

The norm function is used in comparing lengths of Gaussian Integers when using the division algorithm.

Note that the norm function over $\mathbb{Z}$ was $N(b) = |b|$.

Making the Table Normal

Quotient	Remainder	Norm
1	$-2+2i$	8
2	-3	9
i	$1+3i$	10
$-i$	$-3+5i$	34
$1+i$	i	$\boxed{1}$

Table 3: Extension of Table 2 with Norms

We therefore see that the best way to divide $z = -1 + 4i$ by $w = 1 + 2i$ of the quotients attempted is

$$z = -1 + 4i = (1 + 2i)(1 + i) + i = wq + r.$$

Note that

$$N(r) = 1 < N(w) = 5.$$

This property is unique to the quotient and remainder pair we've found.

In general, the statement of the division algorithm over $\mathbb{Z}[i]$ ensures the existance and uniqueness of a pair (q, r) for which

$$z = wq + r \quad | \quad N(r) < N(w).$$

6.3 Visualizing Division in Gaussian Integers

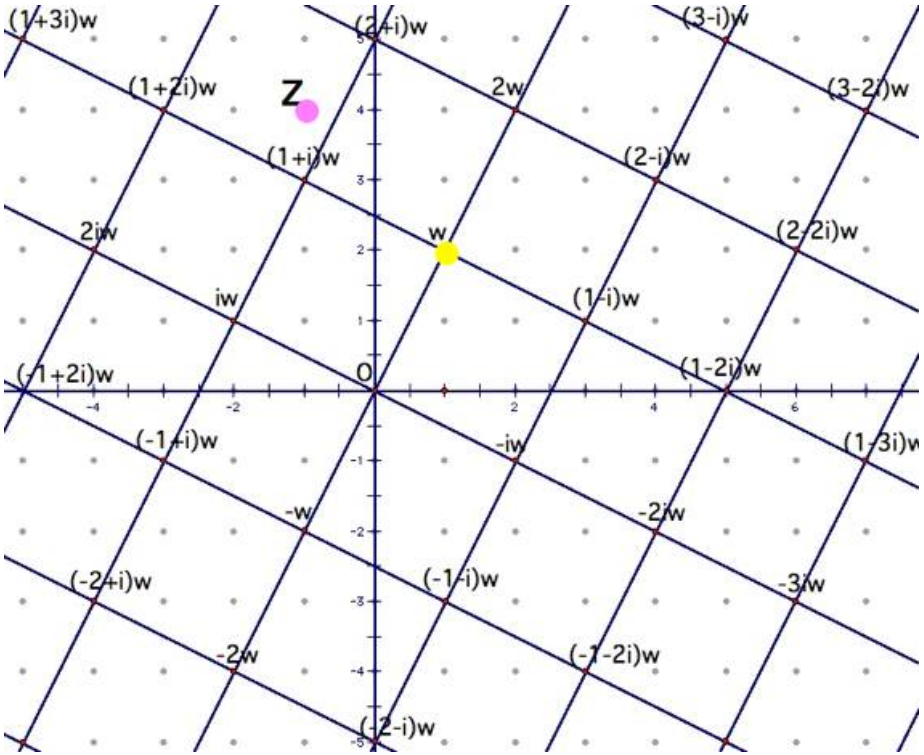


Figure 4: Source: Clay Kitchings [1]

7 Base Numbers

Base numbers are the heart of computers with both binary and hexadecimal. Binary can refer to the 2 states of a switch - on or off. Hexadecimal can be used to describe locations in computer memory or colours with HTML.

Definition

When we write numbers using the first b whole numbers (i.e. $0, 1, 2, \cdots, b-1$), this is a base b system. [6]

We can think of base conversions as different ways of *grouping numbers*.

7.1 Binary

The most common and applicable base is binary. In binary, the only two usable digits are 0 and 1. Therefore, we have to write every number as a sum of powers of 2.

For instance, to write 19 in binary, we would write

$$19 = 16 + 2 + 1 = 2^4 + 2^1 + 2^0 = 10011_2.$$

Similarly, to convert from binary to decimal, we find the power of 2 that each 1 corresponds with:

$$101010_2 = 2^5 + 2^3 + 2^1 = 32 + 8 + 2 = 42.$$

7.2 Base Conversion Problem

When working with bases that are not binary, things get slightly more complicated. If we want to convert the positive number n into base b, we use a similar algorithm to binary.

We attempt to find the highest power of the base b that goes into the number n. We then subtract this from the number n and repeat until we get to the units digit.

Problem

Convert 2016 into base 8.

7.3 Subtracting Powers of 8

We begin by listing powers of 8:

$$8, 64, 512, 4096, \cdots .$$

The largest power of 8 that is less than 2016 is 512. We divide 2016 by 512 using the division algorithm:

$$2016 = 512 \times 3 + 480.$$

We then repeat the process by finding the largest power of 8 less than 480, 64. We divide 480 by 64 using the division algorithm:

$$480 = 64 \times 7 + 32.$$

Finally, we write $32 = 8 \times 4$. Therefore,

$$2016 = 3 \times 512 + 7 \times 64 + 4 \times 8 = 3740_8.$$

To verify using Mathematica, we use the command BaseForm[2016,8].

7.4 Magic 8 Ball

Instead of subtracting off powers of 8, another method exists to convert 2016 to base 8. We can repeatedly divide by 8 until the quotient is 0 and look at the remainders:

$$\begin{aligned} 2016 &= 8 \cdot 252 + \mathbf{0} \\ 252 &= 31 \cdot 8 + \mathbf{4} \\ 31 &= 8 \cdot 3 + \mathbf{7} \\ 3 &= 8 \cdot 0 + \mathbf{3} \end{aligned}$$

We append each of the remainders in *backwards order* to determine $2016 = 3740_8$.

8 Contest Style Base Number Problems

Problem

Funky base conversions.

1. Convert 25681_9 to base 3.
2. Convert $11,101,001,111_2$ to base 8.

Problem (AIME 1986)

The increasing sequence $1, 3, 4, 9, 10, 12, 13 \cdots$ consists of all those positive integers which are exponent powers of 3 or sums of distinct powers of 3. Find the 100^{th} term of this sequence.

8.1 Funky Base Conversions

Solution. We begin by writing out

$$\begin{aligned} 25681_9 &= 2 \cdot 9^4 + 5 \cdot 9^3 + 6 \cdot 9^2 + 8 \cdot 9^1 + 1 \cdot 9^0 \\ &= 2 \cdot \left(3^2\right)^4 + 5 \cdot \left(3^2\right)^3 + 6 \cdot \left(3^2\right)^2 + 8 \cdot \left(3^2\right)^1 + 1 \cdot \left(3^2\right)^0 \\ &= \mathbf{2} \cdot 3^8 + \mathbf{5} \cdot 3^6 + \mathbf{6} \cdot 3^4 + \mathbf{8} \cdot 3^2 + \mathbf{1} \cdot 3^0. \end{aligned}$$

The problem we have is that in base 3, the only digits we are allowed to use are $0, 1, 2$. Therefore, what do we do about the $5, 6, 8$?

We conver them all to base 3! $5 = 3 \cdot 1 + 2, 6 = 3 \cdot 2 + 0, 8 = 3 \cdot 2 + 2$. We plug these in to the above equation:

$$\begin{aligned} 25681_9 &= \mathbf{2} \cdot 3^8 + \mathbf{5} \cdot 3^6 + \mathbf{6} \cdot 3^4 + \mathbf{8} \cdot 3^2 + \mathbf{1} \cdot 3^0 \\ &= \mathbf{2} \cdot 3^8 + (3+2) \cdot 3^6 + (3 \cdot 2) \cdot 3^4 + (3 \cdot 2 + 2) \cdot 3^2 + \mathbf{1} \cdot 3^0 \\ &= \mathbf{2} \cdot 3^8 + \mathbf{1} \cdot 3^7 + \mathbf{2} \cdot 3^6 + \mathbf{2} \cdot 3^5 + \mathbf{2} \cdot 3^3 + \mathbf{2} \cdot 3^2 + \mathbf{1} \cdot 3^0 \\ &= \boxed{212202201_3}. \end{aligned}$$

A shortcut to doing this would be converting each digit directly to base 3 and appending the digits:

$$2 = 2_3,\ 5 = 12_3,\ 6 = 20_3,\ 8 = 22_3,\ 1 = 01_3.$$

For problem 2, inspired by our success in the previous problem, we manipulate the sum of powers of 2. Since $8 = 2^3$, we have to group the numbers in groups of 3:

$$\begin{aligned} 11,101,001,111_2 &= 2^{10} + 2^9 + 2^8 + 2^6 + 2^3 + 2^2 + 2^1 + 2^0 \\ &= (2+1)\,2^9 + \left(2^2+1\right)2^6 + \mathbf{1}\cdot 2^3 + \left(2^2+2^1+2^0\right) \\ &= \mathbf{3}\cdot 8^3 + \mathbf{5}\cdot 8^2 + \mathbf{1}\cdot 8^1 + \mathbf{7}\cdot 8^0 \\ &= \boxed{3517_8}. \end{aligned}$$

Note that as before, a shortcut exists! The commas are extra helpful here.

$$11_2 = 3,\ 101_2 = 5,\ 001_2 = 1,\ 111_2 = 7.$$

□

8.2 AIME 1986

Solution. We begin by writing out the first few terms of the sequence as sums of distinct powers of 3.

$$\mathbf{1} = 3^0,\ \mathbf{3} = 3^1,\ \mathbf{4} = 3^1 + 3^0,\ \mathbf{9} = 3^2,$$
$$\mathbf{10} = 3^2 + 3^0,\ \mathbf{12} = 3^2 + 3^1,\ \mathbf{13} = 3^2 + 3^1 + 3^0,\ \cdots.$$

Does anyone notice anything interesting about the powers of 3 used?

Number in Sequence	3^2	3^1	3^0
1	0	0	1
3	0	1	0
4	0	1	1
9	1	0	0
10	1	0	1
12	1	1	0
13	1	1	1

Table 4: Coefficients of Powers of 3

The numbers on the right hand of the table should look familiar!

Definition

A **bijection** is a function between two sets X and Y such that every element in X is mapped to Y and every element in Y is mapped to X. Mathematically, we write this as $f : X \to Y$.

Where is there a bijection in this problem?

Term #	Number in Sequence	3^2	3^1	3^0
1	**1**	0	0	1
2	**3**	0	1	0
3	**4**	0	1	1
4	**9**	1	0	0
5	**10**	1	0	1
6	**12**	1	1	0
7	**13**	1	1	1

Table 5: Extension of Table 4 Adding the Term Number

There appears to be a bijection between the term number in the sequence on the left hand side and the decimal form of the binary numbers formed on the right hand side of the table! Note that $7 = 111_2$ for instance.

Now, how do we find the 100th term in the sequence? In order to do this, we first have to convert 100 to binary:

$$100 = 64 + 32 + 4 = 2^6 + 2^5 + 2^2 = 1100100_2.$$

Then, by the bijection established above, each of the 1's and 0's actually correspond to powers of 3. Therefore, the 100th term in the sequence is

$$3^6 + 3^5 + 3^2 = \boxed{981}.$$

□

9 Fundamental Theorem of Arithmetic

In 1801, Gauss proved the Fundamental Theorem of Arithmetic in his book "Disquisitiones Arithmeticae".

Theorem

Every integer at least 2 is either prime itself or is the unique product of primes.

This theorem is the reason 1 is not a prime number; otherwise, the product would not be unique! Before proving the Fundamental Theorem of Arithmetic, we revisit our friend Euclid and learn about induction.

9.1 Euclid's Lemma

> "If two numbers by multiplying one another make some number, and any prime number measure the product, it will also measure one of the original numbers."
> - Euclid's Elements, Book VII, Proposition 30"

In other words, if prime $p \mid ab$ for integers a, b, then $p \mid a$ or $p \mid b$. The proof of Euclid's Lemma requires Bezout's Theorem, which will come later in this course!

Another key factor in the proof of the Fundamental Theorem of Arithmetic is the method of **mathematical induction**.

Definition (Induction)
In order to prove a statement $P(x)$ is true for all positive integers $x \geq a$, it suffices to show this in two parts:

1. *The base case:* $P(a)$ is true.
2. *The inductive step:* For all positive integers $k \geq a$, $P(k)$ being true implies $P(k+1)$ is also true.

This is a domino effect where one domino knocks down the next.

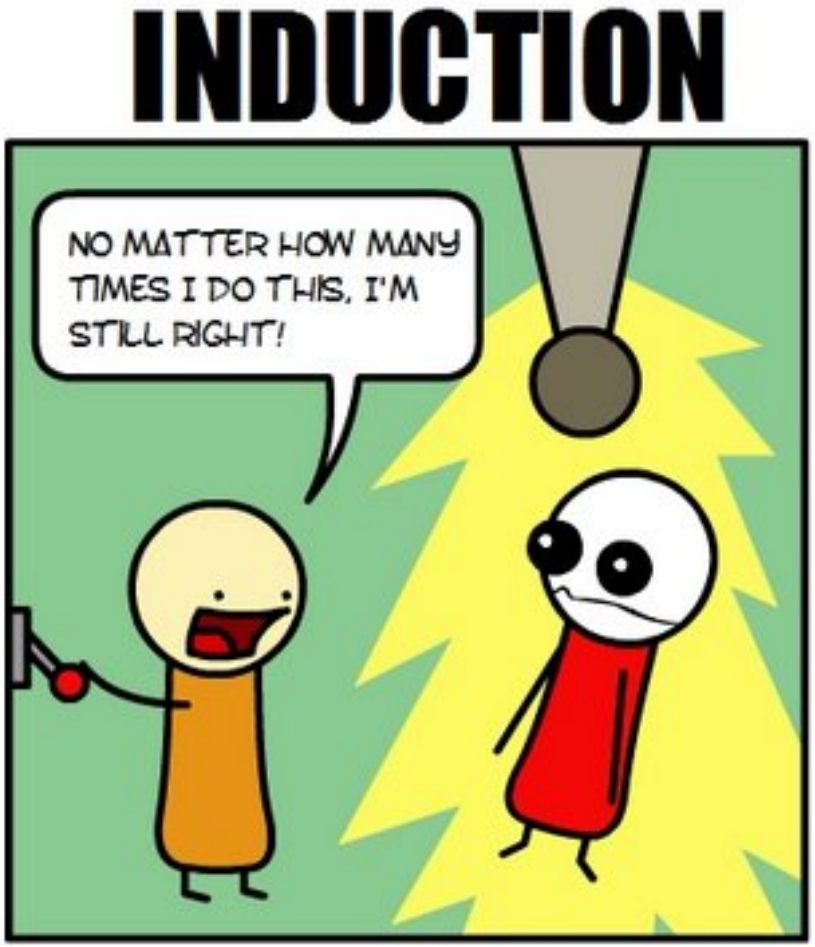


Figure 5: Source: Something Of That Ilk

For instance, suppose I wish to show the identity

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

holds for all $n \geq 1$. I begin by showing the identity holds for $n = 1$: $1 = \frac{1 \cdot 2}{2}$. I then show that if the identity is true for $n = k$, then it is also true for $n = k + 1$. The inductive *hypothesis* is that $1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}$. We use this to show the identity holds for $n = k + 1$. Indeed, note that

$$\begin{aligned}(1 + 2 + 3 + \cdots + k) + k + 1 &= \frac{k(k+1)}{2} + k + 1 \\ &= (k+1)\left(\frac{k}{2} + 1\right) \\ &= \frac{(k+1)(k+2)}{2}.\end{aligned}$$

Definition (Strong Induction)

Replace the inductive step with: If $P(a), P(a+1), P(a+2), P(a+3), \cdots, P(k-1), P(k)$ being true *implies* that $P(k+1)$ is also true.

While the notation may be confusing now, after we see strong induction in action, it will make more sense!

Theorem

Every integer at least 2 is either prime itself or is the unique product of primes.

Proof. We prove the Fundamental Theorem of Arithmetic. There are two parts for the proof: showing the existance of a prime factorization, and the uniqueness of the prime factorization. We begin with the existance part.

We use the method of strong induction. We desire to show that all positive integers greater than or equal to 2 are either prime or can be expressed as the product of primes. To begin with, as a base case, 2 itself is prime.

Furthermore, using the strong induction hypothesis, assume that we have proven the the existance of a prime factorization for all integers y with $2 \leq y \leq k$. We then prove the existance for $k+1$. We have two cases to consider: either $k+1$ is prime, or it is the product of two numbers a, b with $2 \leq a, b < k+1$.

If $k+1$ itself is prime, then this satisfies the first condition of the Fundamental Theorem of Arithmetic. Otherwise, $k+1 = ab$.

By the strong induction hypothesis, both a and b are the product of primes. Therefore, $k+1$ is also the product of primes.

By the method of strong induction, we have proved the existance of a prime factorization. We now go about proving uniqueness.

For the uniqueness part, we again use the method of strong induction. As a base case, 2 indeed has a unique prime factorization. For the strong induction hypothesis, assume that all integers y with $2 \leq y \leq k$ have a unique prime factorization. We then prove that $k+1$ also has a unique

prime factorization. Assume for the sake of contradiction that it does not and that two possible prime factorizations exist:

$$k+1 = p_1 p_2 p_3 \cdots p_s = q_1 q_2 q_3 \cdots q_r.$$

I wil show that this is impossible.

We see that $p_1 \mid q_1 q_2 q_3 \cdots q_r$. By Euclid's Lemma, we must have $p_1 \mid q_j$ for some $1 \leq j \leq r$. However, since they are primes, this implies that $p_1 = q_j$. We cancel out this similar term to get

$$\frac{k+1}{p_1} = p_2 p_3 \cdots p_s = q_1 q_2 q_3 \cdots q_{j-1} q_{j+1} \cdots q_r.$$

By the strong induction hypothesis, $\frac{k+1}{p_1} = \frac{k+1}{q_j}$ has a unique prime factorization. This implies that the two products above contain the same exact primes with the same multiplicity (although, they may be slightly rearranged)! Similarly, since $p_1 = q_j$, the original two numbers are exactly identical, and $k+1$ has a unique prime factorization. $\square$

What does Gauss' proof of the Fundamental Theorem of Arithmetic imply? It allows us to write numbers in their prime factorization. For instance, $120 = 2^3 \cdot 3 \cdot 5$ and $182 = 2 \cdot 7 \cdot 13$.

9.2 Canonical Prime Factorization

The preferred method for writing the prime factorization of a positive integer n is

$$n = \prod_{j=1}^{k} p_j^{e_j} = p_1^{e_1} p_2^{e_2} \cdots p_j^{e_j}.$$

The $\prod$ symbol is similar to the $\sum$ symbol, except we multiply all the terms!

Writing prime factorizations this way makes it easier to compute the greatest common divisor and least common multiple of two terms. It also allows us to do other problems involving least common multiples, sum of divisors, product of divisors, and number of divisors!

10 Applications of the Fundamental Theorem of Arithmetic

10.1 GCD and LCM

For two positive integers a and b, we write out their prime factorizations:

$$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}.$$

Then,

$$\begin{aligned} \gcd(a,b) &= p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_k^{\min(a_k,b_k)} \\ \text{lcm}[a,b] &= p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_k^{\max(a_k,b_k)}. \end{aligned}$$

For instance, when $a = 2^6 \cdot 3^5 \cdot 7^2$ and $b = 2^9 \cdot 3^1$, then

$$\gcd(a,b) = 2^{\min(6,9)} \cdot 3^{\min(5,1)} \cdot 7^{\min(2,0)} = 2^6 \cdot 3^1 \cdot 7^0$$
$$\operatorname{lcm}[a,b] = 2^{\max(6,9)} \cdot 3^{\max(5,1)} \cdot 7^{\max(2,0)} = 2^9 \cdot 3^5 \cdot 7^2.$$

Note that $\gcd(a,b)\operatorname{lcm}[a,b] = 2^{6+9} \cdot 3^{1+5} \cdot 7^2 = ab$. This is true in general be cause $\min(a_j, b_j) + \max(a_j, b_j) = a_j + b_j$.

10.2 Jail Puzzle

Problem

The cells in a jail are numbered from 1 to 100 and their doors are activated from a central button. The activation opens a closed door and closes an open door. Starting with all the doors closed the button is pressed 100 times. When it is pressed the k-th time the doors that are multiples of k are activated. Which doors will be open at the end?

10.3 Least Common Multiple Problems

Problem (AIME 1998)

For how many values of k is 12^{12} the least common multiple of 6^6, 8^8, and k?

Problem

Let $[r, s]$ denote the least common multiple of positive integers r and s. Find the number of ordered triples a, b, c such that $[a, b] = 1000, [b, c] = 2000, [c, a] = 2000$.

10.4 AIME 1998

We find the prime factorizations of these numbers. We have

$$12^{12} = 2^{24} \cdot 3^{12}, 6^6 = 2^6 \cdot 3^6 \text{ and } 8^8 = 2^{24}.$$

Let $k = 2^{k_1} 3^{k_2}$. We then rewrite the equation as

$$\text{lcm}[2^6 \cdot 3^6, 2^{24}, 2^{k_1} 3^{k_2}] = 2^{24} \cdot 3^{12}.$$

Since none of the first two terms have a factor of 3^{12}, we must have $k_2 = 12$.

On the other hand, the second term has a factor of 2^{24}. Therefore, we must have $0 \leq k_1 \leq 24$, giving $\boxed{25}$ possible values of k.

10.5 AIME 1987

Notice that $1000 = 2^3 \times 5^3, 2000 = 2^4 \times 5^3$. Since we are working with least common multiples, set

$$a = 2^{a_1}5^{a_2}, b = 2^{b_1}5^{b_2}, c = 2^{c_1}5^{c_2}.$$

By looking at the exponent of 2, we see that $v_2([a,b]) = 3$ and $v_2([b,c]) = v_2([c,a]) = 4$. If a_1 or b_1 were greater than 3, then the first equation would be false. Therefore, we must have $a_1, b_1 \leq 3$, and at least one of them must be equal to 3. Further, for the second two relations to be true, we must have $c_1 = 4$.

Now, we consider the powers of 5. We note that $v_5([a,b]) = 3, v_5([a,c]) = 3, v_5([b,c]) = 3$. This gives us four separate cases, whena ll of the numbers are 3 or when two of them are, while the third is less than 3:

$$(a_2, b_2, c_2) = (3,3,3), (3,3,x), (3,x,3), (x,3,3).$$

We know that $0 \leq x \leq 2$, therefore, there are 3 possibilities for each of the x's above. Hence, there are a total of $3 \cdot 3 + 1 = 10$ possibilities for the power of 5.

In conclusion, there is a total of $7 \cdot 10 = \boxed{70}$ ordered triples a, b, c which work.

11 Bezout's Identity

Bezout (1730-1783) was a French mathematician

References

[1] Clay Kitchings. *Gaussian Integers & Division Algorithm Project*.

[2] A-Star. *A-Star Winter Math Camp AMC 10/12 Handout*. Star League, 2015.

[3] Wikipedia. Euclid's elements.

[4] Justin Stevens. *Olympiad Number Theory Through Challenging Problems*. AoPS Featured Articles, 3rd edition, 2016.

[5] Iurie Boreico. *A-Star Summer Math Camp USAMO Number Theory*. Star League, 2013.

[6] Matthew Crawford. *Introduction to Number Theory*. Art of Problem Solving, 2nd edition.