Number Theory with

python
PROGRAMMING

Divisibility
Lecture 1

Justin Stevens

Outline

Perfect Cube Pattern I

Example 1. Find a pattern in the sequence of perfect cubes, $1, 8, 27, 64, 125, 216, 343, 512, 729$.

Solution. We try taking differences of consecutive terms to help:

$$8 - 1 = 7, \ 27 - 8 = 19, \ 64 - 27 = 37.$$

SS We write these differences in a table:

1		8		27		64		125		216		343		512		729
	7		19		37		61		91		127		169		217	

Try taking differences again, and see if you get closer to a pattern!

Perfect Cube Pattern II

Example. Find a pattern in the sequence of perfect cubes, $1, 8, 27, 64, 125, 216, 343, 512, 729$.

1		8		27		64		125		216		343		512		729
	7		19		37		61		91		127		169		217	

We try taking differences of consecutive terms in the first row to give

$$19 - 7 = 12, \; 37 - 19 = 18, \; 61 - 37 = 24.$$

We write these in a row directly below:

1		8		27		64		125		216		343		512		729
	7		19		37		61		91		127		169		217	
		12		18		24		30		36		42		48		

Can we do this one more time?

Perfect Cubes Pattern III

Example. Find a pattern in the sequence of perfect cubes, $1, 8, 27, 64, 125, 216, 343, 512, 729$.

Taking the difference of consecutive terms one more time gives

$$18 - 12 = 6, \ 24 - 18 = 6, \ 30 - 24 = 6.$$

We write the final differences in the third row:

1		8		27		64		125		216		343		512		729
	7		19		37		61		91		127		169		217	
		12		18		24		30		36		42		48		
			6		6		6		6		6		6			

Why are all the terms at the bottom 6?

Perfect Cubes Pattern IV

The cubes are given by $f(n) = n^3$. Can we find a formula for the first difference?

Let the first difference, $D_1(n) = f(n+1) - f(n)$:

$$\begin{aligned} D_1(n) = f(n+1) - f(n) &= (n+1)^3 - n^3 \\ &= \left(n^3 + 3n^2 + 3n + 1\right) - n^3 \\ &= \mathbf{3n^2 + 3n + 1}. \end{aligned}$$

Plugging in $n = 1, n = 2$, and so forth gives the first row in our table above.

$D_2(n)$ is the difference of consecutive first differences. Can we find a formula?

Perfect Cubes Pattern V

We see that $D_2(n) = D_1(n+1) - D_1(n)$. Expanding gives

$$
\begin{aligned}
D_1(n+1) - D_1(n) &= \left(3\,(n+1)^2 + 3\,(n+1) + 1\right) - \left(3n^2 + 3n + 1\right) \\
&= \left(\left(3n^2 + 6n + 3\right) + (3n+3) + 1\right) - \left(3n^2 + 3n + 1\right) \\
&= \left(3n^2 + 9n + 7\right) - \left(3n^2 + 3n + 1\right) \\
&= \mathbf{6n + 6}.
\end{aligned}
$$

Plugging in $n = 1, n = 2$, and so forth gives the second row in our table.

Finally, $D_3(n)$ is the difference of consecutive second differences. Can we find a formula?

Perfect Cubes Pattern VI

We see that $D_3(n) = D_2(n+1) - D_2(n)$. Expanding gives

$$\begin{aligned}
D_3(n) = D_2(n+1) - D_2(n) &= (6(n+1)+6) - (6n+6) \\
&= (6n+12) - (6n+6) \\
&= \mathbf{6}.
\end{aligned}$$

Therefore, the third difference is always a constant 6. If we extend this method to any cubic polynomial, after three differences, the sequence will always be constant.

The method of finite differences tells us that for a sequence of integers, if $D_k(n)$ is constant, then the sequence is given by a degree k polynomial.

Finite Differences Puzzles

Example 2. Find a polynomial formula, $p(n)$ beginning with $n = 1$ for the sequence $13, 17, 23, 31, 41, 53, 67, 83, 101$.

Example 3. Find a formula for the sum of the first n perfect squares.

Prime Number Sequence Solution I

Example. Find a polynomial formula, $p(n)$ beginning with $n = 1$ for the sequence $13, 17, 23, 31, 41, 53, 67, 83, 101$.

Solution. We use the method of finite differences:

$$
\begin{array}{ccccccccccccccccc}
13 & & 17 & & 23 & & 31 & & 41 & & 53 & & 67 & & 83 & & 101 \\
& 4 & & 6 & & 8 & & 10 & & 12 & & 14 & & 16 & & 18 & \\
& & 2 & & 2 & & 2 & & 2 & & 2 & & 2 & & 2 & &
\end{array}
$$

The sequence is quadratic since there are two differences before the terms are constant. Let $p(n) = an^2 + bn + c$. Can you find a, b, and c?

Prime Number Sequence Solution II

Example. Find a polynomial formula, $p(n)$, beginning with $n = 1$ for the sequence $13, 17, 23, 31, 41, 53, 67, 83, 101$.

Substituting $p(1) = 13$, $p(2) = 17$, $p(3) = 23$ into $p(n) = an^2 + bn + c$:

$$\begin{cases} a + \ b + c = 13 \\ 4a + 2b + c = 17 \\ 9a + 3b + c = 23. \end{cases}$$

Solving gives $(a, b, c) = (1, 1, 11)$, so the nth term in the sequence is

$$p(n) = \boxed{n^2 + n + 11}.$$

Surprisingly, for $n = 1$ through 9, $n^2 + n + 11$ is always prime. It isn't always prime, however, since $10^2 + 10 + 11 = 121 = 11^2$. We'll explore this more in a future lecture!

Summations

Summation Notation: For a function $f(j)$, we write the sum of the values of $f(j)$ from 1 to n as

$$\sum_{j=1}^{n} f(j) = f(1) + f(2) + f(3) + \cdots + f(n).$$

j is the index of the summation and can be replaced by any variable.

The value 1 is the starting point of our sum and the value n is the stopping place.

For instance, $\displaystyle\sum_{j=1}^{4} j^2 = 1^2 + 2^2 + 3^2 + 4^2 = 30$.

Sum of First n Squares Solution I

Example. Find a formula for the sum of the first n squares.

Solution. We begin by coloring the perfect squares blue:

$$\textcircled{0} \quad 1 \quad\quad 5 \quad\quad 14 \quad\quad 30 \quad\quad 55 \quad\quad 91 \quad\quad 140 \quad\quad 204$$
$$\quad 1 \quad\quad 4 \quad\quad 9 \quad\quad 16 \quad\quad 25 \quad\quad 36 \quad\quad 49 \quad\quad 64$$

We now use the method of finite differences:

$$\textcircled{0} \quad 1 \quad\quad 5 \quad\quad 14 \quad\quad 30 \quad\quad 55 \quad\quad 91 \quad\quad 140 \quad\quad 204$$
$$\quad 1 \quad\quad 4 \quad\quad 9 \quad\quad 16 \quad\quad 25 \quad\quad 36 \quad\quad 49 \quad\quad 64$$
$$\quad\quad 3 \quad\quad 5 \quad\quad 7 \quad\quad 9 \quad\quad 11 \quad\quad 13 \quad\quad 15$$
$$\quad\quad\quad 2 \quad\quad 2 \quad\quad 2 \quad\quad 2 \quad\quad 2 \quad\quad 2$$

We therefore expect the polynomial to be cubic. Let the sum of the first n squares be $p(n) = an^3 + bn^2 + cn + d$.

Sum of First n Squares II

Example. Find a formula for the sum of the first n squares.

$$\boxed{0} \quad 1 \quad 5 \quad 14 \quad 30 \quad 55 \quad 91 \quad 140 \quad 204$$

Since the sum starts at 0, $p(0) = 0 \implies d = 0$.

Since $p(1) = 1, p(2) = 5, p(3) = 14$, we have the system of equations:

$$\begin{cases} a + b + c = 1 \\ 8a + 4b + 2c = 5 \\ 27a + 9b + 3c = 14. \end{cases}$$

Solving gives $a = \frac{1}{3}, b = \frac{1}{2}, c = \frac{1}{6}$. Therefore,

$$p(n) = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n = \frac{n(n+1)(2n+1)}{6}.$$

Outline

Definition

Definition. For two integers n and d, **d divides n**, written **$d \mid n$**, if and only if there exists an integer q such that $n = dq$. This is equivalent to saying **n is a multiple of d** or n is divisible by d.

For instance, 7 divides 63 since $63 = 7 \cdot 9$. This is equivalent to saying $7 \mid 63$, 63 is a multiple of 7, or 63 is divisible by 7. We will use these equivalent statements interchangeably throughout the course.

A few basic facts of divisibility are that 0 is divisible by every integer, 1 divides every integer, and integers always divide themselves.

Example. Calculate $296 \div 8$, $1651 \div 13$, and $57542 \div 42$.

Division Solution I

Example. Calculate $296 \div 8$, $1651 \div 13$, and $57542 \div 42$.

Solution. Using long division, we get:

$$\begin{array}{r} 13 \\ 35 \\ 26 \\ \hline 91 \end{array}$$

$$\begin{array}{r} 24 \\ 56 \\ \hline \end{array}$$

$$\begin{array}{r} 42 \\ 155 \\ 126 \\ \hline 294 \end{array}$$

$8)\overline{296}$ $13)\overline{1651}$ $42)\overline{5754}$

0 0 0

Therefore $8 \mid 296$, $13 \mid 1651$, and $42 \mid 5754$.

Another way of thinking of long division is *grouping terms*. How does that work here?

Dividing a Sum of Sequence

In the previous problem, we broke the dividend into three parts:
$1651 = 1300 + 260 + 91$. Note that 13 divides both the sum and every
individual term in the sum. This leads us to our first property of divisibility.

Theorem. If d divides every integer in the sequence $n_1, n_2, \cdots, n_k$,
then $d \mid n_1 + n_2 + \cdots + n_k$.

Proof. Since $d \mid n_j$ for every $1 \leq j \leq k$, there exists an integer q_j such that
$n_j = q_j d$:

$$n_1 + n_2 + \cdots + n_k = q_1 d + q_2 d + \cdots + q_k d$$

$$= d \left(\sum_{j=1}^{k} q_j \right).$$

Therefore, $d \mid n_1 + n_2 + \cdots + n_k$.

Divisibility Puzzles

Example 4. I bring several rolls of dimes (10¢) and quarters (25¢) to the store. Show that the price of any object I buy must be divisible by 5¢ given that I pay with exact change.

Example 5. Show that if d divides n, then d divides cn for all integers c.

Rolls of Dimes and Quarters

Example. I bring several rolls of dimes (10¢) and quarters (25¢) to the store. Show that the price of any object I buy must be divisible by 5¢ given that I pay with exact change.

Solution. Let the number of dimes I pay with be d and quarters be q. Therefore, the total price (in cents) is

$$P = 10d + 25q = 5\left(2d + 5q\right).$$

Therefore, the total price is divisible by 5¢.

We say that the price of any object is a **linear combination** of 10 and 25.

Definition. A linear combination of two integers n_1 and n_2 is of the form $n_1 c_1 + n_2 c_2$ where c_1 and c_2 are integers.

Theorem. If $d \mid n_1$ and $d \mid n_2$, then $d \mid n_1 c_1 + n_2 c_2$ for integers c_1 and c_2.

Multiplying by a Constant

Example. Show that if d divides n, then d divides cn for all integers c.

Solution. By the definition of divisibility, since d divides n, $n = dq$ for some integer q. Therefore when we multiply n by a constant,

$$cn = c(dq) = d(cq).$$

Hence, d divides cn for all integers c.

Outline

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.

Lucky Seven

Example 6. Choose **one** number below and determine if it is divisible by 7.

- 1729
- $2,718,281$
- $16,180,339$

Taxicab Number

Example. Does 7 divide 1729?

"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

$$1729 \quad \rightarrow \quad 172 - 2 \cdot 9 = 154$$
$$154 \quad \rightarrow \quad 15 - 2 \cdot 4 = 7$$

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

Can you find the two ways Ramanujan referenced?

Euler's Number

Example. Does 7 divide 2718281?

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

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

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

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

Example. Does 7 divide 16180339?

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

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

Explanation of Lucky Seven I

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

$$N = 10a + x.$$

For instance, if $N = 1729$, then $a = 172$ and $x = 9$.

We want to prove that if 7 divides $N = 10a + x$, then 7 divides $a - 2x$.

To do so, we multiply N by an integer. Can you find this number?

Explanation of Lucky Seven II

Example. Show that if 7 divides $N = 10a + x$, then 7 divides $a - 2x$.

Solution. 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 also divides $5N = 50a + 5x$. Therefore,

$$7 \mid 50a + 5x.$$

Furthermore, by the linear combination theorem, $7 \mid 49a + 7x$. Hence, 7 must divide their difference:

$$7 \mid \Big((50a + 5x) - (49a + 7x) \Big) \implies 7 \mid a - 2x.$$

Therefore, we have proven the divisibility rule for 7.

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 $+4x$.

Example. Is 1734579 divisible by 11?

Rule for 11

Example. Is 1734579 divisible by 11?

Solution. We begin numbering the digits. We start with the rightmost digit and label 9 as 0. Then 7 is labeled as 1, 5 is labeled as 2, 4 is labeled as 3 and so forth.

We make all of the even digits red and all of the odd digits blue:

$$1734579.$$

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

$$E = 1 + 3 + 5 + 9 = 18, O = 7 + 4 + 7 = 18.$$
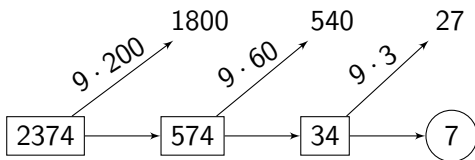
Since $E - O = 18 - 18 = 0$ is divisible by 11, so is the original number.

Outline

Division Algorithm I

When the concept of division is first introduced in primary school, quotients and remainders are used. For instance, if we divide 2374 by 9:

$$
\begin{array}{r}
18 \\
\overline{57} \\
54 \\
\overline{34} \\
9\overline{)2374} \\
27 \\
\overline{7}
\end{array}
$$

Therefore, $2374 = 9 \cdot 263 + 7$. Here's another way of looking at the division:

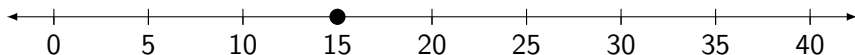# Division Algorithm II

Theorem. For positive integers n and d, to divide n by d, there exists a unique quotient and remainder q and r such that

$$n = dq + r, \quad 0 \le r < d.$$

When $r = 0$ in the division algorithm, we have $n = dq$, therefore $d \mid n$.

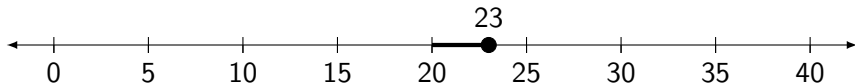For example, $15 = 5 \cdot 3 + 0$. We can see this on the number line:

Note that 15 lies on the tick. What happens when a number lies between two ticks?

Division Algorithm III

Theorem. For positive integers n and d, to divide n by d, there exists a unique quotient and remainder q and r such that

$$n = dq + r, \quad 0 \le r < d.$$

For example, if $n = 23$ and $d = 5$, we can see this on a number line:
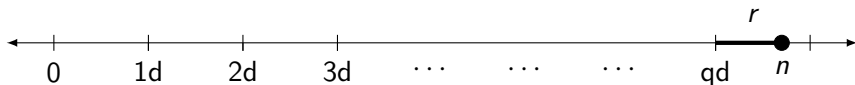

Therefore, $23 = 5 \cdot 4 + 3$, hence $q = 4$ and $r = 3$.

Division Algorithm IV

Theorem. For positive integers n and d, to divide n by d, there exists a unique quotient and remainder q and r such that

$$n = dq + r, \quad 0 \le r < d.$$

If $d \nmid n$, then n will always lie between two ticks on the number line!

Otherwise, n lies on one of the ticks and $r = 0$.

Now, how do we prove that the quotient and remainder are unique?

Division Algorithm V

Theorem. For positive integers n and d, to divide n by d, there exists a **unique** quotient and remainder q and r such that

$$n = dq + r, \quad 0 \le r < d.$$

Assume for the sake of contradiction there are two distinct representations:

$$n = dq_1 + r_1 = dq_2 + r_2, \quad 0 \le r_1, r_2 < d.$$

Rearranging these equations gives

$$d(q_1 - q_2) = r_2 - r_1.$$

From the inequalities above, $|r_2 - r_1| < d$. Therefore, $r_2 - r_1 = 0$, implying $r_2 = r_1$ and $q_2 = q_1$. Hence, the representation is unique.

Algorithm Component

```python
def QuotientRemainder(n, d):
    """Input integers n and d to divide n by d.
       Returns q and r such that n=dq+r."""
    q=0
    r=n
    while r>=d:
        r=r-d
        q=q+1
    return q, r
```

q	r	$r \geq d$?
0	23	T
1	18	T
2	13	T
3	8	T
4	3	F

Forms of Numbers

If we say a number is of the form $n = 3k + 1$, this means that the remainder when we divide n by 3 is 1. We could write out several possible values of n:

k	n
-2	-5
-1	-2
0	1
1	4
2	7
3	10

Another application of the division algorithm is even/odd numbers.

Definition. n is odd if $n = 2k + 1$ for some integer k. n is even if $n = 2k$ for some integer k. Two numbers are said to have the same parity if they are both odd or both even. Otherwise, they have opposite parity.

Division Algorithm Puzzles

Example 7. Show that every perfect square is of the form $3k$ or $3k+1$.

Example 8. Prove that if n is an integer, then $1 + (-1)^n (2n - 1)$ is a multiple of 4.

Perfect Square Remainders I

Example. Show that every perfect square is of the form $3k$ or $3k+1$.

Solution. The possible remainders when dividing a number by 3 are $0, 1, 2$. We list several perfect squares, and put checks by which form they are in.

n	n^2	3k	3k+1	3k+2
1	1	X	✓	X
2	4	X	✓	X
3	9	✓	X	X
4	16	X	✓	X
5	25	X	✓	X
6	36	✓	X	X

We hypothesize that when n is a multiple of 3, n^2 is of the form $3k$. Otherwise, n^2 is of the form $3k+1$.

We split our proof into cases based on the remainder when dividing n by 3.

Perfect Square Remainders II

Example. Show that every perfect square is of the form $3k$ or $3k + 1$.

- If $n = 3m$ for some integer m, then

$$n^2 = (3m)^2 = 9m^2 = 3\left(3m^2\right),$$

which is of the form $3k$ when $k = 3m^2$.

- If $n = 3m + 1$ for some integer m, then

$$n^2 = (3m + 1)^2 = 9m^2 + 6m + 1 = 3\left(3m^2 + 2m\right) + 1,$$

which is of the form $3k + 1$ when $k = 3m^2 + 2m$.

- If $n = 3m + 2$ for some integer m, then

$$n^2 = (3m + 2)^2 = 9m^2 + 12m + 4 = 3\left(3m^2 + 4m + 1\right) + 1,$$

which is of the form $3k + 1$ when $k = 3m^2 + 4m + 1$.

Multiples of Four I

Example. Prove that if n is an integer, then $1 + (-1)^n (2n - 1)$ is a multiple of 4.

Solution. Note that the sign of $(-1)^n$ depends on the parity of n. Therefore, we divide the proof into two cases: n even and n odd.

- n is even. Then, $n = 2k$ for some integer k.
  Substituting this into the expression gives:

$$
\begin{aligned}
1 + (-1)^n (2n - 1) &= 1 + (-1)^{2k} (2 \cdot 2k - 1) \\
&= 1 + 1 (4k - 1) \\
&= 4k.
\end{aligned}
$$

Since this a multiple of 4, our proof for the even case is complete.

Can you complete the proof for the odd case?

Multiples of Four II

Example. Prove that if n is an integer, then $1 + (-1)^n (2n - 1)$ is a multiple of 4.

- n is odd. Then, $n = 2k + 1$ for some integer k.
  Substituting this into the expression gives:

$$\begin{aligned}
1 + (-1)^n (2n - 1) &= 1 + (-1)^{2k+1} (2 \cdot (2k + 1) - 1) \\
&= 1 + (-1)(4k + 2 - 1) \\
&= 1 - (4k + 1) \\
&= -4k.
\end{aligned}$$

Since this is a multiple of 4, our proof for the odd case is complete.

Since every positive integer is either even or odd, our proof is complete.