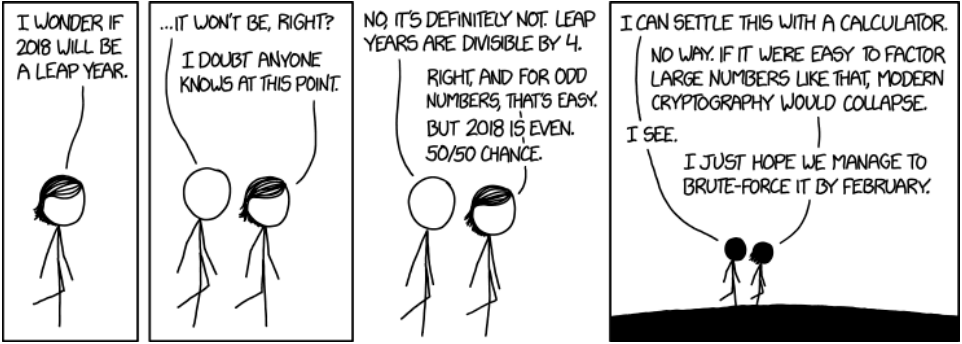
Discrete Mathematics

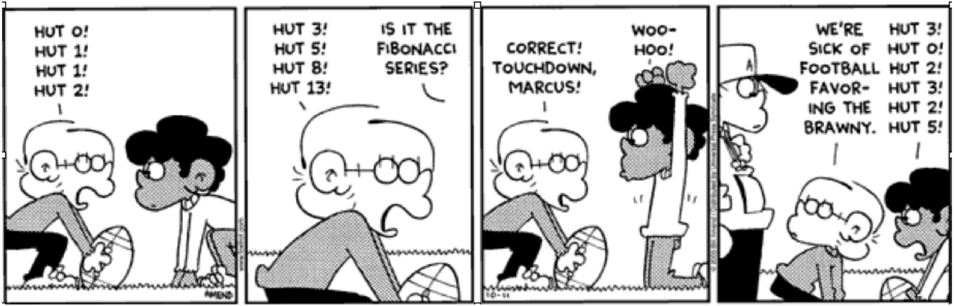
MATH1064, Lecture 12

Jonathan Spreer



Extra exercises for Lecture 12

Section 2.4: Problems 1–8, 25



Divisibility

Definition

If $n, d \in \mathbb{Z}$, then n is divisible by d if and only if there exists some $k \in \mathbb{Z}$ such that $n = kd$.

We write $d \mid n$. We also say "d divides n", or "d is a divisor of n".

Examples:

If n is not divisible by d, we write $d \nmid n$.

Examples:

Divisibility

Lemma

For all $a, b, m \in \mathbb{Z}$, if a and b are divisible by m, then $a + b$ is divisible by m.
Symbolically: $\forall a, b, m \in \mathbb{Z},\ (m \mid a) \wedge (m \mid b) \to m \mid (a + b)$.

Proof. Assume that $m \mid a$ and $m \mid b$. Then there exist $k, \ell \in \mathbb{N}$ such that $a = km$ and $b = \ell m$.

Then $a + b = km + \ell m = (k + \ell)m$. Because $k, \ell \in \mathbb{Z}$ we have $k + \ell \in \mathbb{Z}$, and so $m \mid (a + b)$ also. $\square$

Disproof by counterexample (see Lecture 6)

Key idea: To disprove a statement $\forall x, P(x)$ – that is, to show that the statement is false – we simply need to show one example of an x for which $P(x)$ is false. This x is called a counterexample.

Example

Disprove the following statement:
For all $a, b, m \in \mathbb{Z}$, if ab is divisible by m, then either a or b is divisible by m.

Counterexample. Let $m = 4$ and $a = b = 6$. Then $ab = 36$ is divisible by 4, but neither $a = 6$ nor $b = 6$ is divisible by 4.

Finding all divisors

Can we make a list of all divisors of $n = 6$?

We have found: 1, -1, 2, -2, 3, -3, 6, -6

Can we be sure there are no others?

We need to know when we can stop searching.
We will prove:

Lemma (Bounds for divisors)

Let $n, d \in \mathbb{Z}$. If $|n| \geq 1$ and $d \mid n$, then $0 < |d| \leq |n|$.

Lemma (Bounds for divisors)

Let $n, d \in \mathbb{Z}$. If $|n| \geq 1$ and $d \mid n$, then $0 < |d| \leq |n|$.

Side note: Do we really need the extra condition $|n| \geq 1$? What would happen if $n = 0$?

If $n = 0$, then every integer $d \in \mathbb{Z}$ divides n (as $0 = 0 \cdot d$).

So the statement "If $d \mid n$, then $|d| \leq |n|$" is false for $n = 0$.

Proof of lemma: Suppose $n, d \in \mathbb{Z}$ with $|n| \geq 1$ and $d \mid n$.
Then there is some $k \in \mathbb{Z}$ such that $n = kd$.

To show that $0 < |d|$, use a proof by contradiction.
If $|d| \leq 0$ then $|d| = 0$ (absolute values cannot be negative).
Therefore $d = 0$ and so $n = kd = k \cdot 0 = 0$.
But then $|n| = 0$, contradicting our assumption that $|n| \geq 1$.
Therefore $0 < |d|$.

We now prove a special case of the lemma:
we additionally assume that $n, d \in \mathbb{N}$.
(Often it is a good strategy to prove a special case first, and then try to reduce the general case to the special case.)

If $n, d \in \mathbb{N}$, we have $n \geq 1$ and $d \geq 1$. Since $n = kd$, we also have $k \geq 1$. Now:

$$1 \leq k \qquad \text{multiplied by } d \text{ gives} \qquad d \leq kd = n,$$

since multiplying both sides of an inequality by a positive number preserves the inequality.

This is gives us $d \leq n$. But $n, d \in \mathbb{N}$, so $|d| = d$ and $|n| = n$.
Therefore $|d| \leq |n|$.

So we have proved the lemma in the special case $n, d \in \mathbb{N}$.

We return now to the general case, where $n, d \in \mathbb{Z}$.
All that remains is to prove $|d| \leq |n|$.

Our technique will be to apply our special case argument to the absolute values $|n|$ and $|d|$.

As before, there is some $k \in \mathbb{Z}$ such that $n = kd$.
Taking absolute values gives $|n| = |kd| = |k| \cdot |d|$.
That is: $|d|$ divides $|n|$.

From the statement of the lemma we have $|n| \geq 1$, and from our earlier argument we have $|d| > 0$. Therefore $|d|, |n| \in \mathbb{N}$.

But... we already know the lemma is true for natural numbers (our special case from before)!
Since $|d|, |n| \in \mathbb{N}$, $|n| \geq 1$ and $|d|$ divides $|n|$, our special case argument tells us that $|d| \leq |n|$. $\square$

The key steps in this proof were to:

- prove $0 < |d|$ by contradiction;
- prove $|d| \leq |n|$ in the special case where $n, d \in \mathbb{N}$;
- reduce the general case $n, d \in \mathbb{Z}$ to an instance of our special case.

So... can we make a list of all divisors of $n = 6$?

We found: ± 1, ± 2, ± 3, ± 6.

Can we be sure there are no others?

Yes! Because we now know that if $d \mid 6$ then $|d| \leq 6$.

Division with remainder

For dividing by 11, we can write:

$576 = 51 \cdot 11 + 15$ (The proposed remainder is bigger than 11!)

$576 = 52 \cdot 11 + 4$

$-576 = (-52) \cdot 11 - 4$ (The proposed remainder is negative!)

$-576 = (-53) \cdot 11 + 7$

For dividing by 18, we can write:

$576 = 32 \cdot 18 = 32 \cdot 18 + 0$

The Quotient-Remainder Theorem

Given any integer n and positive integer d,
there exist unique integers q and r such that

$$n = qd + r \qquad \text{and} \qquad 0 \leq r < d.$$

We call q the quotient, and r the remainder.

Division by 7

Write down your favourite 3-digit number.
Then write it twice in succession.

Example: 123123.

Now divide your 6-digit number by 7. What is your remainder:

1. remainder $= 1$
2. remainder $= 2$
3. remainder $= 3$
4. remainder $= 4$
5. remainder $= 5$
6. remainder $= 6$
7. remainder $= 0$

Applications of the QRT

Is there a square which ends with the digit 7?

Let's look at the first few squares:

$1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2, 10^2, 11^2, 12^2, 13^2, 14^2, 15^2, 16^2, \ldots$

Let's write down the last digits:

1, 4, 9, 6, 5, 6, 9, 4, 1, 0, 1, 4, 9, 6, 5, 6, ...

The pattern seems to repeat!

Let $n \in \mathbb{Z}$.

By the quotient-remainder theorem, we can write $n = 10q + r$, where $0 \leq r < 10$. Then:

$$\begin{aligned} n^2 &= (10q + r)^2 \\ &= 100q^2 + 20qr + r^2 \\ &= 10(10q^2 + 2qr) + r^2 \end{aligned}$$

So the only part that affects the last digit is r^2.

There are only 10 choices for r: it must be one of 0,1,...,9.
This explains why the sequence repeats with period 10:
$\ldots, 1,\ 4,\ 9,\ 6,\ 5,\ 6,\ 9,\ 4,\ 1,\ 0,\ \ldots$

We also see that the only digits that will be the last digit of any square are $0, 1, 4, 5, 6, 9$, but not $2, 3, 7, 8$.

Question: Is 288768324567698358 a square?

Modular arithmetic is a fancy way of writing down arguments like this in a more elegant, concise form. It can answer questions like:

– Is 438345 divisible by 9?

– For which positive integers n is $n^2 - 5$ a power of 2?

If n and m leave the same remainder after division by d,
we say that they are congruent modulo d.

We write: $n \equiv m \pmod{d}$

If $n \equiv m \pmod{d}$, then $m \equiv n \pmod{d}$.
So the relationship is symmetric.

Facts:

- If $n = qd + r$, then $n \equiv r \pmod{d}$
- $n \equiv m \pmod{d}$ if and only if $d \mid (n - m)$
- $n \equiv 0 \pmod{d}$ if and only if $d \mid n$

Question time!

Facts:

- If $n = qd + r$, then $n \equiv r \pmod d$
- $n \equiv m \pmod d$ if and only if $d \mid (n - m)$
- $n \equiv 0 \pmod d$ if and only if $d \mid n$

a) $7 \equiv 31 \pmod 6$ — true or false?

b) $-2 \equiv 8 \pmod 5$ — true or false?

c) $-27 \equiv 27 \pmod{10}$ — true or false?

To analyse the sequence of the last digits of the squares, we showed:

If $n \equiv r \pmod{10}$, then $n^2 \equiv r^2 \pmod{10}$.

This is just a special instance of a more general result!

If $a \equiv b \pmod{d}$ and $n \equiv m \pmod{d}$, then

1. $an \equiv bm \pmod{d}$, and
2. $a + n \equiv b + m \pmod{d}$

Is $a - n \equiv b - m \pmod{d}$?

True! $a - n \equiv b - m \pmod{d}$. Prove this!

If $ac \equiv bc \pmod{d}$, is $a \equiv b \pmod{d}$?

Come up with a proof or a counterexample and post it on the discussion board.