Mathematics Enrichment UCD, Jan 11, 2020

Kevin Hutchinson (UCD Maths/Stats)

ucd.ie/mathstat/newsandevents/events/mathsenrichment/

www.irmo.ie

Olympiad problems (examples)

[Romania 1959] Prove that the fraction

$\frac{21n+4}{14n+3}$ is irreducible for every

natural number n.

↳ i.e. 1, 2, 3, 4, 5, ...

[Beijing China, 1990] Determine all numbers n such that $\frac{2^n+1}{n^2}$ is an integer

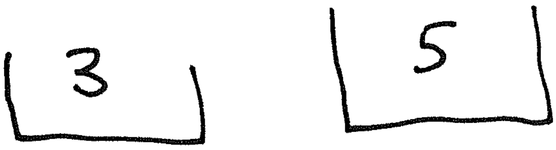
Problems in "Number Theory"

i.e. problems about whole numbers (integers)

(or their ratios — rational numbers)

Some number theory problems

Die Hard 3



measure exactly 4 litres.

mathematically:

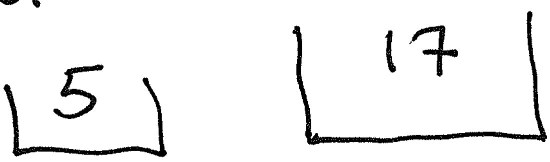
$$2 \cdot \underline{5} - 2 \cdot \underline{3} = 4$$ (Damian's solution)

$$3 \cdot \underline{3} - 1 \cdot \underline{5} = 4$$ (Andy's solution)

By the way: measure 1 litre:

$$2 \cdot \underline{3} - 1 \cdot \underline{5} = 1$$ (Andy).

How about



measure exactly 1 litre.

$$7 \cdot \underline{5} - 2 \cdot \underline{17} = 1$$

or

$$3 \cdot \underline{17} - 10 \cdot \underline{5} = 1$$

[Return to: find all possible solutions — there are infinitely many!]

$\lfloor 4 \rfloor$ $\lfloor 18 \rfloor$ measure 1?

Can't be done: 4, 18 both even

$\Rightarrow$ $x \cdot 4 \pm y \cdot 18$ will be

even also. $\therefore \neq 1$.

$\lfloor 6 \rfloor$ $\lfloor 15 \rfloor$ measure 1?

No: 3 divides both 6 and 15 $\Rightarrow$

3 must divide any combination of them.

3 is a common divisor of 6, 15.

Mathematical problem

Given $\lfloor m \rfloor$, $\lfloor n \rfloor$, what amounts

l can I measure (and find a recipe)?

i.e. the problem is to find integers x, y

such that $x\,\underline{m} + y \cdot n = \underset{(\text{from } m, n)}{l}$

Let us say l is "obtainable" if

such integers x, y exist.

Note 1 If d is a common divisor of m, n ~~th~~ and if l is obtainable then d divides l also ($d | l$).

Note 2 If l is obtainable

— i.e. there are integers x, y with

$$xm + yn = l \qquad (1)$$

— then so is any multiple tl of l (t integer).

Why? Multiply (1) by t:

$$(tx)m + (ty)n = tl$$

Note 3 If 1 is obtainable, then every integer is obtainable.

Let g be the largest common divisor of m, n

[We write $g = \gcd(m,n) = \operatorname{hcf}(m,n) = \underline{(m,n)}$.]

eg

$(3,5) = 1$

$(5,17) = 1$

$(4,18) = 2$

$(6,15) = 3$ etc.

If $g = (m, n)$ and if l is obtainable then l must be a multiple of g.

Is any multiple of g obtainable?

In part, <u>Is g always obtainable</u>?

<u>Answer</u> Yes, always

by "Euclid's Algorithm"

Euclid of Alexandria, ca 350 BC

<u>Basic principle</u>

<u>Theorem</u> Let a, b be any integers.

Suppose $b = ta + c$ where c, t integers

Then $(a, b) = (a, c)$

<u>Proof</u> Any common divisor of a, b is also a divisor of c since $c = b - ta$.

Likewise, any common divisor of a, c is also a ~~common~~ divisor of $b = ta + c$

"Toy" example

Find the gcd 21, 51

$$51 = 2 \cdot \underline{21} + \underline{9} \quad (1) \quad (21, 9)$$

$$21 = 2 \cdot \underline{9} + \boxed{\underline{3}} \quad (2) \quad (9, 3)$$

$3 | 9$ ✓

Furthermore, we can now find integers x, y with $x \cdot 21 + y \cdot 51 = 3$. (using (1) and (2)):

(2) gives $\quad 3 = 21 - 2 \cdot \underline{9}$

(1) gives $\quad 3 = 21 - 2 \cdot (51 - 2 \cdot 21)$

ie $\quad 3 = 5 \cdot 21 - 2 \cdot 51$

Example $\quad 703, \quad 1007$

Find gcd g and express it in the form $x \cdot 703 + y \cdot 1007$.

Solution:

$$1007 = 1 \cdot \underline{703} + \underline{304}$$
$$703 = 2 \cdot \underline{304} + \underline{95}$$
$$304 = 3 \cdot \underline{95} + \boxed{\underline{19}} \quad (19 | 95)$$

So $g = 19$.

Now

$$19 = 304 - 3 \cdot \underline{95}$$

$$= 304 - 3 \cdot (703 - 2 \cdot 304)$$

$$= 7 \cdot \underline{304} - 3 \cdot 703$$

$$= 7 \cdot (1007 - 703) - 3 \cdot 703$$

$$\boxed{19 = 7 \cdot 1007 - 10 \cdot 703}$$

<u>Theorem</u> $g = (m, n)$ is always "obtainable":
If g is the gcd of m, n then there exist integers x, y such that
$$g = xm + yn$$
(and we have an algorithm to find x, y)

<u>Exercises</u> (1) $\boxed{437}$ $\boxed{986}$

What amounts obtainable? Measure out the gcd.

(2) Do Romania 1959 problem above.

(3) I have lots of $\boxed{3c}$ and $\boxed{5c}$ stamps.

What amounts are obtainable:

$8 = 3 + 5$ ✓ $11 = 2 \cdot 3 + 5$ ✓

2 is not obtainable, 4 is not . .

Last theorem is <u>very</u> important.

Corollary to Theorem

Let $g = \gcd(m,n)$. Let d be any other common divisor. (By definition, $d < g$)

In fact, $d \mid g$

Proof: We have $g = xm + ny$

d divides both terms.