Mathematical Enrichment

Sat Feb 1st, 2020

Kevin Hutchinson : Number Theory

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

www.irmo.ie

Selection Test. H1.26 Feb 8th 10 – 1 pm. (10 questions)

EGMO Test

Recall m n What amounts l can we measure.

We saw: Let $g = \gcd(m,n) = (m,n)$

Then l is measurable $\iff$ l is a multiple of g

$\Updownarrow$

$l = sm + tn$ for some integers s, t

I.p. If $(m,n) = 1$, then we can write

$1 = sm + tn$ for some s, t integers.

Example 437 986 Find the gcd and express it as $s \cdot 437 + t \cdot 986$

Euclid's algorithm

$$\begin{aligned}
986 &= 2 \cdot \underline{437} + \underline{112} && (1)\\
437 &= 3 \cdot \underline{112} + \underline{101} && (2)\\
112 &= 1 \cdot \underline{101} + \underline{11} && (3)\\
101 &= 9 \cdot \underline{11} + \underline{2} && (4)\\
11 &= 5 \cdot \underline{2} + 1 && (5)
\end{aligned}$$

gcd

$$1 \underset{(5)}{=} 11 - 5\cdot \underline{2} \underset{(4)}{=} 11 - 5\cdot(101 - 9\cdot 11) = 46\cdot 11 - 5\cdot 101$$

$$\underset{(3)}{=} 46\cdot(112 - 101) - 5\cdot 101 = 46\cdot 112 - 51\cdot 101$$

$$\underset{(2)}{=} 46\cdot 112 - 51\cdot(437 - 3\cdot 112) = 199\cdot 112 - 51\cdot 437$$

$$\underset{(1)}{=} 199(986 - 2\cdot 437) - 51\cdot 437 = \underline{199\cdot 986 - 449\cdot 43}$$

✓.

Theorem If $(m,n) = 1$ then there exist integers s, t with $1 = sm + tn$

Note converse is true. Why? Easy.

IMO 1959 $\dfrac{21n+4}{14n+3}$ is always "irreducible".

Solution (1.)

$$\underline{21n+4} = 1\cdot(14\underline{n+3}) + (7\underline{n+1})$$

$$14n+3 = 2\cdot(7\underline{n+1}) + 1$$

$\Rightarrow$ gcd $= 1$.

(2) $1 = 3\cdot(14n+3) - 2\cdot(21n+4)$

$\boxed{3c}$ $\boxed{5c}$

↑

1	2	3	4	5	6	7	8	9	10	11
x	x	✓	x	✓	✓	x	✓	✓	✓	✓

↑

3 in a row

n obtainable $\Rightarrow$ $n+3$ obtainable..

$\boxed{5c}$ $\boxed{8c}$

20	21	22	23	24	25	26	27	28	29	30	31	32
✓	✓	X	✓	✓	✓	✓	X	✓	✓	✓	✓	✓

5 in a row.

m is obtainable if $m \geq 28$.

<u>General problem</u> Given $m, n \geq 1$ with $(m,n) = 1$

What amounts l can be expressed as

$sm + tn$ for some nonnegative integers s, t

ie $s, t \geq 0$

We <u>know</u> every $l = sm + tn$, but with s or t possibly <u>negative</u>.

<u>Problem</u> Suppose $l = s_0 m + t_0 n$. for some s_0, t_0 integers (possibly negative).

Find all other solutions $l = sm + tn$.

Before we do this, an important

<u>Lemma</u> If $(m,n) = 1$ "relatively prime" and if $m \mid na$ then $m \mid a$.

<u>Proof</u>: We know $1 = s \cdot m + t \cdot n$ for some integers s, t.

$\Rightarrow \quad a = sma + t\underline{na}$

m divides this and this.

Example of $m \mid ab$ but $m \nmid a$, $m \nmid b$.

$6 \mid 3 \cdot 4$ but $6 \nmid 3$ $6 \nmid 4$.

Recall p is prime if only divisors are $1, p$

Lemma If p is prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.

Proof: If $p \mid a$, ✓

Otherwise $(a, p) = 1$.

By previous Lemma $p \mid b$.

Corollary p prime, $p \mid a_1 a_2 \cdots a_n$

then $p \mid a_i$ for some i.

Proof: Use Lemma and proof by induction on n

Back to: Suppose $(m, n) = 1$

$$l = s_0 m + t_0 n$$

We can find lots of other s and t s:

$$l = \overbrace{(s_0 - rn)}^{s} m + \overbrace{(t_0 + rm)}^{t} n$$

for any integer r

Is this all possible solution ?

Yes! : If $\ell = sm + tn$ for ~~an~~ s, t integers then

$$s = s_0 - rn \quad \text{and} \quad t = t_0 + rm$$

for some integer r.

Proof: We have

$$sm + tn = \ell = s_0 m + t_0 n$$

$$(s_0 - s)m = (t - t_0)n$$

So $m \mid (t - t_0)n \Rightarrow m \mid t - t_0$ (since $(m,n) = 1$ (Lemma).)

i.e. $t - t_0 = rm$ for some integer r

i.e. $\boxed{t = t_0 + rm}$

$$(s_0 - s)m = \underbrace{rm}_{t - t_0} n \Rightarrow s_0 - s = rn$$

$$\Rightarrow \boxed{s = s_0 - rn}$$

15c 8c Do 31

$$2 \cdot 8 - 3 \cdot 5 = 1$$

$$62 \cdot 8 - 93 \cdot 5 = 31$$

$$62 - 5r \qquad -93 + 8r$$

$r = 12$: $62 - 60 = +2$, $\quad -93 + 96 = +3$ $\Rightarrow \boxed{2 \cdot 8 + 3 \cdot 5 = 31.}$

$$54 \cdot 8 - 81 \cdot 5 = 27$$

$54 - 5r$ $\qquad$ $-81 + 8r$

$5r \geq 55$ $\leftarrow$ need $r \geq 11$

this becomes negative.

Back to stamps $\boxed{m}$ $\boxed{n}$ $\qquad (m,n) = 1.$

Let $l \geq 1$ be any integer.

When is l obtainable.

We can write $l = sm + tn$ for some s, t

I can add or subtract multiples of n to s.

So we can arrange that $0 \leq s \leq n-1.$

If $t \geq 0$, l is obtainable.

Otherwise $t \leq -1$ and in this case

$$l \leq (n-1)m - n$$

$\therefore$ If $l > (n-1)m - n = \boxed{mn - m - n}$

it is obtainable

But $mn - m - n = (n-1)m + (-1) \cdot n$

is not obtainable.

all other sols $\quad (n-1) - rn \qquad -1 + rm$

negative if $r > 0$ $\qquad$ negative if $r \leq 0$.

<u>Conclusion</u> $mn - m - n$ not obtainable.

Every larger number is.

$3, 5 \qquad 3\cdot 5 - 3 - 5 = 7$

$5, 8 \qquad 5\cdot 8 - 5 - 8 = 27$

<u>Exercises</u> on gcds.

1. Let $g = \gcd(2^8+1, 2^{32}+1)$

   Express g as $s\cdot(2^8+1) + t\cdot(2^{32}+1)$

   (Use algebra!).

2. Suppose $(m,n) = 1$

   Show $(m^2-n^2, 2mn) = 1$ or 2.

3. Suppose $m,n \geq 1$ with $(m,n) = d$.

   $a > 1$

   Show $(a^m - 1, a^n - 1) = a^d - 1$
