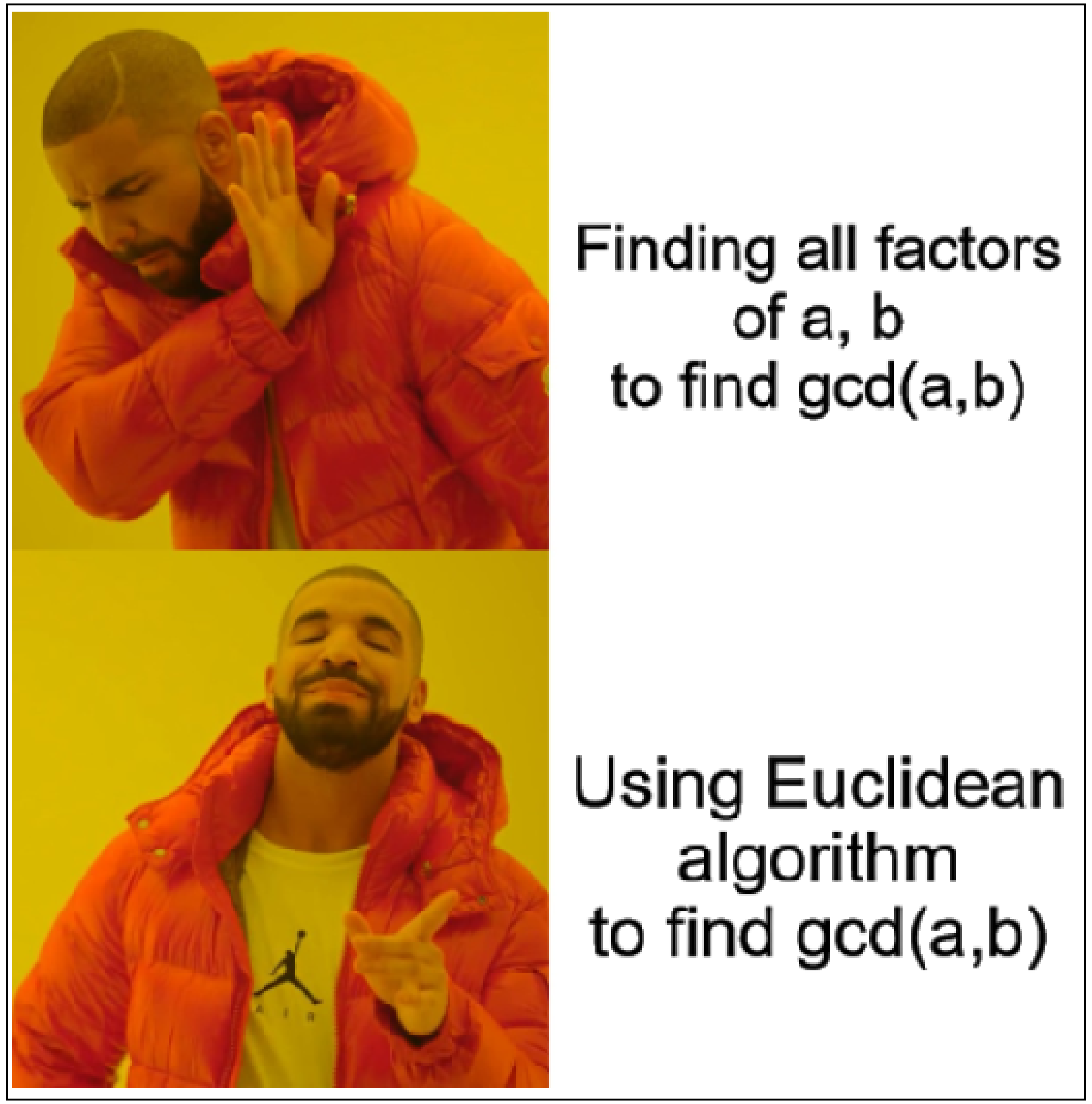
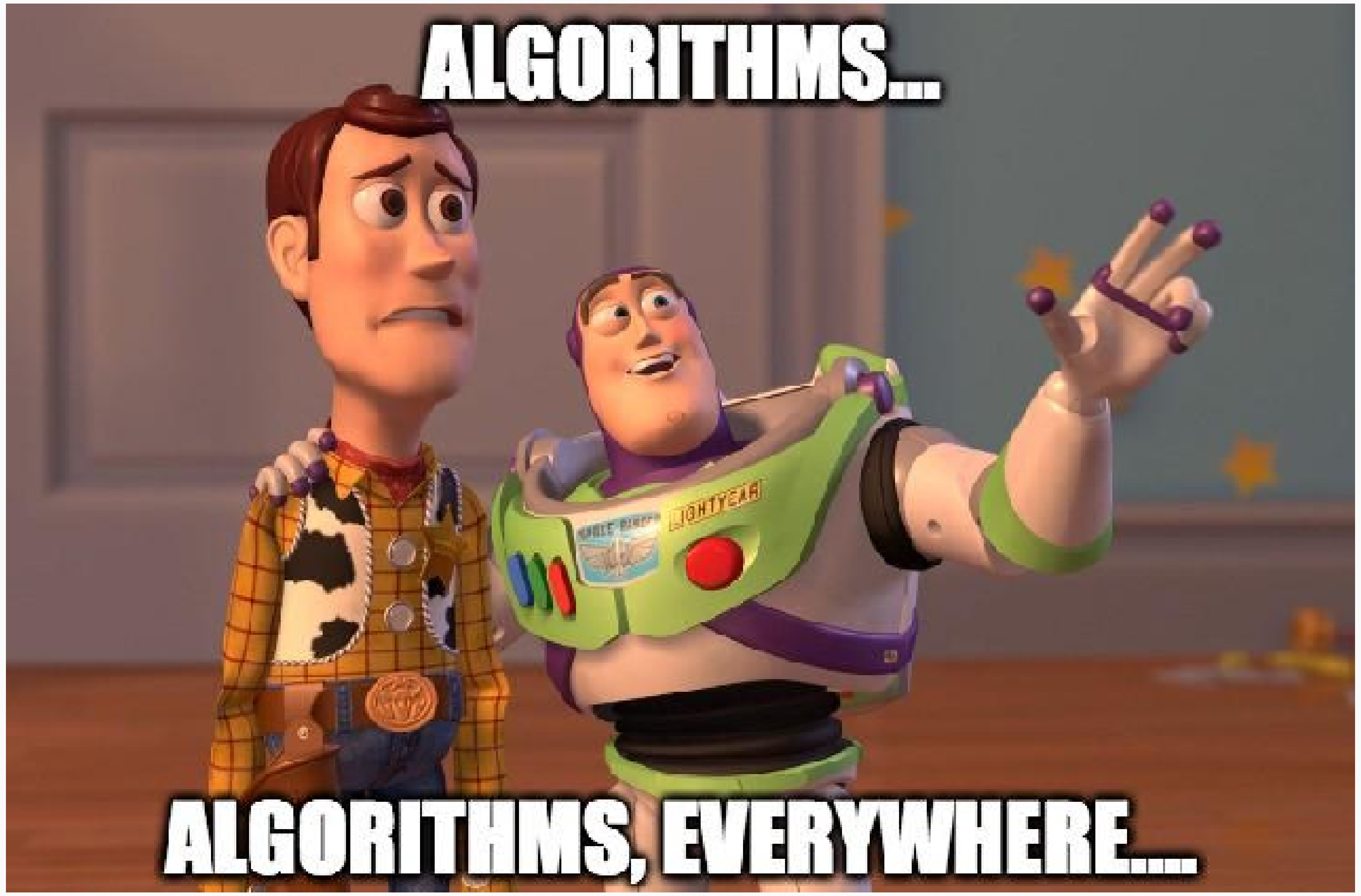
Instructions: We'll use the same whiteboard process until, as a whole class, we decide to use some other process.

One change: I did two more examples of Euclidean algorithm on the first two panels and reversed those after problem 1 panel.





And, I introduce two memes about the topic: The one on the left, found online (it's not really very helpful). The one above, handmade!

Euclidean algorithm

$a = 40 \qquad b = 15$

$$\begin{array}{ccccc} a & & b & & r \\ 40 & = & 15 \cdot 2 & + & 10 \\ 15 & = & 10 \cdot 1 & + & 5 \\ 10 & = & 5 \cdot 2 & + & 0 \end{array}$$

gcd

Next equation: b , r become new a, b

↑

same

once we have 0 remainder, we go back one equation and grab r as the GCD.

One more example

$a = 651 \qquad b = 294$

$$651 = 294 \cdot 2 + 63$$

$$294 = 63 \cdot 4 + 42$$

$$63 = 42 \cdot 1 + 21 \quad \text{gcd}$$

$$42 = 21 \cdot 2 + 0$$

1

5005 = 2 * (2093) + 819

2093 = 2 * (819) + 455

819 = 1 * (455) + 364

455 = 1 * (364) + 91

364 = 4 * (91) + 0

So the GCD (5005, 2093) = 91

Cian

Reversing Euclidean algorithm example

Using $a=40,\ b=15$ calculations:

Express first as a combo of later "a" and "b". Then we will replace them with earlier "a" and "b's.

$$40 = 15\cdot 2 + 10$$

$$15 = 10\cdot 1 + 5 \longrightarrow \overset{\text{gcd}}{5} = 15 - \overset{r}{10}$$

$$= 15 - (\overset{a}{40} - 2\cdot \overset{b}{15})$$

$$= 3\cdot 15 - 40$$

want to express as a combo of 40, 15

At each step we replace the "r" of the previous equation with a linear combination of the "a" and "b" of that equation.

One more reversing example reversing a=651 b=294 calculation.

gcd

$$
\begin{aligned}
21 &= 63 - \overset{r}{42} \\
&= 63 - (\overset{a}{294} - 4 \cdot \overset{b}{63}) \\
&= 5 \cdot \overset{r}{63} - 294 \\
&= 5 \cdot (651 - 2 \cdot 294) - 294 \\
&= 5 \cdot 651 - 11 \cdot 294
\end{aligned}
$$

Before moving on to replacing the next "r", make sure to clean up the equation by gathering all terms together.

Always double check the final combo works. Yep!

2

$$
\begin{aligned}
91 &= 455 - 364 \\
&= 455 - (819 - 455) \\
&= 455 \cdot 2 - 819 \\
&= (2093 - 819 \cdot 2) \cdot 2 - 819 \\
&= 2093 \cdot 2 - 819 \cdot 5 \\
&= 2093 \cdot 2 - (5005 - 2093 \cdot 2) \cdot 5 \\
&= 2093 \cdot 12 - 5005 \cdot 5
\end{aligned}
$$

-Nick

Use the online Euclidean algorithm solver for this. I have the solution by hand, but it's not in easily scannable format.

4

a) 5x+10y=1234; Not possible, 5 * an integer + 10 * an integer will always result in an answer ending in either 0 or 5

b) 5x-4y=2; x=2 and y=2

c) 5x-4y=1234; x=250 and y=4

I found which multiple of 4 could be added to 1234 to give a number ending in 0 or 5, which then told me what to multiply by 5

Oh, I like this idea. The first time I read it, I thought it was something complicated but it's not. We could also use negative y, y=-1, because 1234=1230+4 would be easier. Then x=1230/5.

Is there another way we can obtain an integer solution to c?

Michael

Theorem 1

Theorem 1: The linear Diophantine equation $ax + by = c$ has a solution if and only if $\gcd(a, b)$ divides c.

proof: Prove the easy direction.

If there's a solution, then $ax_0 + by_0 = c$ for some x_0, y_0.

Since $\gcd | a, b$, $\gcd | ax_0 + by_0 = c$ as well.

To prove the other direction, assume $\gcd(a,b) | c$. By definition of divisibility, we have $c = \gcd(a,b) \cdot k$ for some k. By the GCD as a linear combination result, we have $\gcd(a,b) = ax_0 + by_0$. Multiplying both sides by k and rearranging terms, we obtain

$$(ax_0 + by_0)k = a(x_0 \cdot k) + b(y_0 \cdot k) = c.$$

Oops.. When I scanned the solution, I did not include the last line. Oh well.

5 a, b

5 a. Use your result from problem 2 to solve the following Diophantine equation:

$$2093 \cdot x + 5005 \cdot y = 9191$$

$101\left(91 = 12 \cdot 2093 - 5 \cdot 5005\right)$ $\quad 9191 = \underbrace{1212}_{x} \cdot 2093 + \underbrace{(-505)}_{y} \cdot 5005$

b. Check that $x = 1322$ and $y = -551$ is a possible solution. Are your x and y values different than these?

✓

Yes.

5 c, d

c. Show that for any k, $x = 1322 + 5005 \cdot k$ and $y = -551 - 2093 \cdot k$ also works as solution.

$(1322 + \cancel{5005k})\,2093 + (-551 - \cancel{2093k})\,5005 =$

$1322 \cdot 2093 - 551 \cdot 5005 = 9191$

why did this work?

d. Show that $x = 1322 + 55 \cdot k$ and $y = -551 - 23 \cdot k$ also works.

$1322 \cdot 2093 + \underbrace{\cancel{55 \cdot 2093 \cdot k}} - 551 \cdot 5005 \underbrace{\cancel{- 23 \cdot 5005 \cdot k}} = 9191$

$\underbrace{55}_{b/d} \cdot \overbrace{23 \cdot 91}^{a}$ $\qquad$ $\underbrace{23}_{a/d} \cdot \overbrace{55 \cdot 91}^{b}$

Extra problem (in case all the others are taken): Use the gcd as a linear combination idea to solve the Diophantine equation x*159-y*204=57.

If you want to skip/get stuck: Someone, of course, did an online solver: https://www.math.uwaterloo.ca/~snburris/cgi-bin/linear-query (now how on Earth is this thing coded?)

Room 1 numbers: 265631, 88183

gcd(265631,88183)=541; 541=244(88183)-81(265631)

Both of the numbers given have large prime factors. If we were to try to find their prime factorization and look for common divisors using the prime factorization, it wouldn't be efficient.

Numbers with large prime factors are used in RSA, an encryption system, and factoring being hard is the reason why RSA is secure.

2nd part of the question: Write 912,667 as a linear combination of 265631 and 88183.

912667=88183(411628)-265631(136647)

Room 2 numbers: 249401, 82519

Both of the numbers given have large prime factors. If we were to try to find their prime factorization and look for common divisors using the prime factorization, it wouldn't be efficient.

Numbers with large prime factors are used in RSA, an encryption system, and factoring being hard is the reason why RSA is secure.

2nd part of the question: Write 824,729 as a linear combination of 249401 and 82519.

gcd(249401, 82519) = 461

461 = 249401*(45) + 82519*(-136)

1789*461 = 249401*(45*1789) + 82519*(-136*1789)

Last page