DIS 2C

Tuesday, June 26, 2018 10:48 AM

Topics : foundations of modular arithmetic

Review

- a^{-1} exists in $\mathbb{Z}/m\mathbb{Z} \Leftrightarrow \gcd(a, m) = 1$

  analogy : 0 doesn't have a multiplicative inverse in $\mathbb{R}$

(Extended) Euclid's algorithm

- ① $\gcd(x, y) \equiv \gcd(y, \underbrace{x \bmod y}_{<y})$ ← assume $x > y$

  ② $\gcd(x, 0) = x$

  keep doing ①, you'll get ② at the end — this is Euclid's Algorithm

- $x \equiv y \pmod m$

  $\Leftrightarrow y = x + km$ for some $k \in \mathbb{Z}$

  notice that there's no mod on the second line.

  This is a common strategy to "bring everything back to $\mathbb{Z}$".

Q1

Euclid's algorithm : given x, y, output $\gcd(x, y)$.

Extended Euclid's Algorithm : During each step of Euclid's algorithm, do more stuff. Thus, by running almost the same algorithm, you get $\gcd(x, y)$ as a integer linear combination of x and y.
i.e. $\gcd(x, y) = ax + by$ for some $a, b \in \mathbb{Z}$.

(a) What is $\gcd(2328, 440)$?

On the side, write down the newly introduced value as an integer combination of the previous two inputs.

Sol: $\gcd(2328, 440) = \gcd(440, \underbrace{128}_{\equiv 2328 \pmod{440}})$ $\qquad 128 = 1 \times 2328 + (-5) \times 440$

new input !

$= \gcd(128, 56)$ $\qquad 56 = 1 \times 440 + (-3) \times 128$

$= \gcd(56, 16)$ $\qquad 16 = 1 \times 128 + (-2) \times 56$

$= \gcd(16, 8)$ $\qquad \Rightarrow 8 = 1 \times 56 + (-3) \times 16$

$= \gcd(8, 0)$ $\qquad 0 = 1 \times 16 + (-2) \times 8$

$= 8$

(b) What is gcd(2328, 440) as an integer linear combination of 2328 and 440?

On the right side above, we have a set a equations, "describing" 8, 2328, and 440. Keep substituting to get the answer.

Sol:

$$\begin{aligned}
8 &= 1\times 8 + 0\times 0 \\
&= 1\times 8 + (1\times 16 + (-2)\times 8) \\
&= 1\times 16 - 1\times 8 \\
&= 1\times 16 - 1\times(1\times 56 + (-3)\times 16) \\
&= -1\times 56 + 4\times 16 \\
&= -1\times 56 + 4\times(1\times 128 + (-2)\times 56) \\
&= 4\times 128 - 9\times 56 \\
&= 4\times 128 - 9\times(1\times 440 + (-3)\times 128) \\
&= -9\times 440 + 31\times 128 \\
&= -9\times 440 + 31\times(1\times 2328 + (-5)\times 440) \\
&= 31\times 2328 - 164\times 440
\end{aligned}$$

Or, start from yellow arrow, substitute $\boxed{\text{one}}$ number at a time, in backwards order

$$\begin{aligned}
8 &= 1\times 56 + (-3)\times 16 \\
&= 1\times 56 + (-3)\times(1\times 128 + (-2)\times 56) \\
&= 1\times 56 + (-3)\times 128 + 6\times 56 \\
&= 7\times 56 + (-3)\times 128 \\
&= 7\times(1\times 440 + (-3)\times 128) + (-3)\times 128 \\
&= 7\times 440 + (-21)\times 128 + (-3)\times 128 \\
&= 7\times 440 + (-24)\times 128 \\
&= 7\times 440 + (-24)\times(1\times 2328 + (-5)\times 440) \\
&= 7\times 440 + (-24)\times 2328 + 120\times 440 \\
&= 127\times 440 - 24\times 2328
\end{aligned}$$

(c) Express gcd(17, 38) as a "combination" of 17 and 38.

Sol:

$4 = 1\times 38 + (-2)\times 17$

$\Rightarrow 1 = 1\times 17 + (-4)\times 4$

$0 = 1\times 4 + (-4)\times 1$

$\gcd(17,38) = \gcd(38,17) = \gcd(17,4) = \gcd(4,1) = \gcd(1,0) = 1$

$$\begin{aligned}
\gcd(17,38) = 1 &= 1\times 17 + (-4)\times 4 \\
&= 1\times 17 + (-4)\times(1\times 38 + (-2)\times 17) \\
&= 1\times 17 + (-4)\times 38 + 8\times 17 \\
&= -4\times 38 + 9\times 17
\end{aligned}$$

(d) What is 17^{-1} in mod 38?

Sol: 9.

$1 = 9\times 17 + 4\times 38$

$\Rightarrow 9\times 17 \equiv 1 \pmod{38}$

$\Rightarrow 17^{-1} \equiv 9 \pmod{38}$

$\boxed{\text{Concept}}$ 1 $\to$ $y = \underbrace{x}_{9\times 17} + \underbrace{km}_{4\times 38}$

$\Rightarrow x \equiv y \pmod m$

Q2.

Prove that $\gcd(F_n, F_{n-1}) = 1$, where $F_0 = 0$ and $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$.

Pf: [Nice recurrence relation. So try induction.]

$P(n)$: $\gcd(F_n, F_{n-1}) = 1$.

Base case: WTS $P(1)$ is true.

$\gcd(F_1, F_0) = \gcd(1, 0) = 1$

Thus, $P(1)$ holds.

IS: Assume $P(n)$. WTS $P(n+1)$.

$$\begin{aligned}
\gcd(F_{n+1}, F_n) &= \gcd(F_n + F_{n-1}, F_n) && \text{by defn of } F_n \\
&= \gcd(F_n, F_{n-1}) && \text{by } \gcd(x,y) = \gcd(y, x \bmod y) \\
&= 1 && \text{by IH}
\end{aligned}$$

$\Rightarrow P(n+1)$ holds

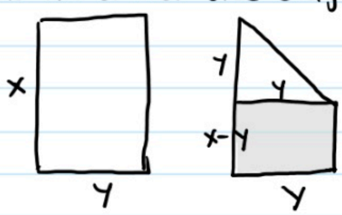
Conclusion: By principle of induction, the original statement holds.

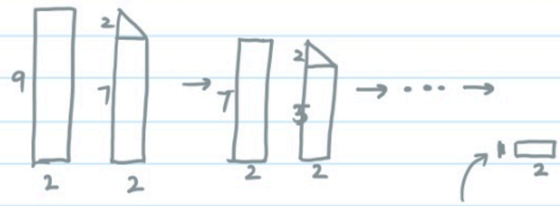
Q3.

Describe a method to find the GCD of the width and height of the paper, with scissors and no rulers

Sol : [The only way we've learned to find $\gcd(x,y)$ for $x>y$ is Euclid's algorithm; namely, $\gcd(x,y) = \gcd(y, x \bmod y)$.
Certainly, we can't really do "mod" using paper, but what's $x \bmod y$? You can think of it as keep subtracting y from x, until we get something that's smaller than y.
Note: However, (almost) never think of mod as an operation!]

Fold the smaller side diagonally onto the larger side.





$\mathrm{mod}(9,2) = \mathrm{mod}(2, 9 \bmod 2)$
$= \mathrm{mod}(2, 1)$

Throw away the square.

Repeat until we've left with a square.

This is the same as Euclid's algorithm.