CS 70 Discrete Mathematics and Probability Theory
Summer 2018 Sinho Chewi and Vrettos Moulos

DIS 2C

1 Extended Euclid

In this problem we will consider the extended Euclid's algorithm. The bolded numbers below keep track of which numbers appeared as inputs to the gcd call. Remember that we are interested in writing the GCD as a linear combination of the original inputs, so we don't want to accidentally simplify the expressions and eliminate the inputs.

(a) Note that x mod y, by definition, is always x minus a multiple of y. So, in the execution of Euclid's algorithm, each newly introduced value can always be expressed as a "combination" of the previous two, like so:

$$\begin{aligned}
\gcd(2328, 440) &= \gcd(440, 128) && [\mathbf{128} = 1 \times \mathbf{2328} + (-5) \times \mathbf{440}] \\
&= \gcd(128, 56) && [\mathbf{56} = 1 \times \mathbf{440} + ____ \times \mathbf{128}] \\
&= \gcd(56, 16) && [\mathbf{16} = 1 \times \mathbf{128} + ____ \times \mathbf{56}] \\
&= \gcd(16, 8) && [\mathbf{8} = 1 \times \mathbf{56} + ____ \times \mathbf{16}] \\
&= \gcd(8, 0) && [\mathbf{0} = 1 \times \mathbf{16} + (-2) \times \mathbf{8}] \\
&= 8.
\end{aligned}$$

(Fill in the blanks)

(b) Now working back up from the bottom, we will express the final gcd above as a combination of the two arguments on each of the previous lines:

$$\begin{aligned}
8 &= 1 \times \mathbf{8} + 0 \times \mathbf{0} = 1 \times \mathbf{8} + (1 \times \mathbf{16} + (-2) \times \mathbf{8}) \\
&= 1 \times \mathbf{16} - 1 \times \mathbf{8} \\
&= ____ \times \mathbf{56} + ____ \times \mathbf{16}
\end{aligned}$$

[*Hint*: Remember, $\mathbf{8} = 1 \times \mathbf{56} + (-3) \times \mathbf{16}$. Substitute this into the above line.]

$$= \_\_\_\_ \times \mathbf{128} + \_\_\_\_ \times \mathbf{56}$$

[*Hint*: Remember, $\mathbf{16} = 1 \times \mathbf{128} + (-2) \times \mathbf{56}$.]

$$\begin{aligned}
&= ____ \times \mathbf{440} + ____ \times \mathbf{128} \\
&= ____ \times \mathbf{2328} + ____ \times \mathbf{440}
\end{aligned}$$

(c) In the same way as just illustrated in the previous two parts, calculate the gcd of 17 and 38, and determine how to express this as a "combination" of 17 and 38.

(d) What does this imply, in this case, about the multiplicative inverse of 17, in arithmetic mod 38?

Solution:

(a) -3

-2

-3

(b) $1 \times \mathbf{16} - 1 \times (1 \times \mathbf{56} + (-3) \times \mathbf{16}) = -1 \times \mathbf{56} + 4 \times \mathbf{16}$

$-1 \times \mathbf{56} + 4 \times (1 \times \mathbf{128} + (-2) \times \mathbf{56}) = 4 \times \mathbf{128} - 9 \times \mathbf{56}$

$4 \times \mathbf{128} - 9 \times (1 \times \mathbf{440} + (-3) \times \mathbf{128}) = -9 \times \mathbf{440} + 31 \times \mathbf{128}$

$-9 \times \mathbf{440} + 31 \times (1 \times \mathbf{2328} + (-5) \times \mathbf{440}) = 31 \times \mathbf{2328} - 164 \times \mathbf{440}$

(c) $\gcd(17, 38) = 1 = 13 \times 38 - 29 \times 17$; also, more simply, $-4 \times 38 + 9 \times 17$, but the algorithm produces the former.

(d) It is equal to -29, which is equal to 9.

2 Fibonacci GCD

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

Solution:

Proceed by induction.

Base Case: We have $\gcd(F_1, F_0) = \gcd(1, 0) = 1$, which is trivially true.

Inductive Hypothesis: Assume we have $\gcd(F_k, F_{k-1}) = 1$ for some $k \geq 1$.

Inductive Step: Now we need to show that $\gcd(F_{k+1}, F_k) = 1$ as well.

We can show that:

$$\gcd(F_{k+1}, F_k) = \gcd(F_k + F_{k-1}, F_k) = \gcd(F_k, F_{k-1}) = 1$$

Note that the second expression comes from the definition of Fibonacci numbers. The last expression comes from Euclid's GCD algorithm, in which $\gcd(x, y) = \gcd(y, x \bmod y)$, since

$$F_k + F_{k-1} \equiv F_{k-1} \pmod{F_k}$$

Therefore the statement is also true for $n = k + 1$.

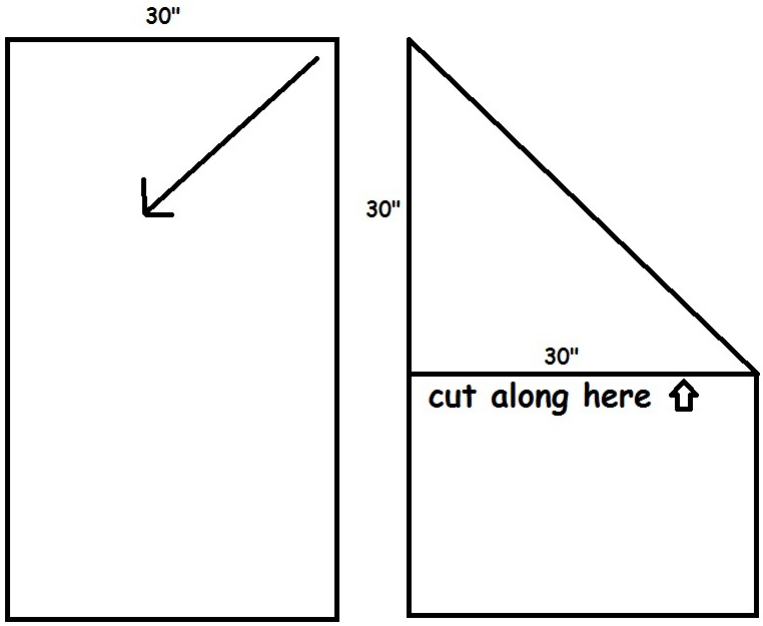
By the rule of induction, we can conclude that $\gcd(F_n, F_{n-1}) = 1$ for all $n \geq 1$, where $F_0 = 0$ and $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$.

3 Paper GCD

Given a sheet of paper such as this one, and no rulers, describe a method to find the GCD of the width and the height of the paper. You can fold or tear the paper however you want, and ultimately you should produce a square piece whose side lengths are equal to the GCD.

Solution:

We can fold the smaller side diagonally onto the larger side, and tear the paper from where the fold lands.



If we started with height and width equal to a and b, this gives us a piece of paper with side lengths $a-b$ and b (assuming that $a > b$). Note that if $a-b > b$, the next time we end up with side lengths $a-2b$ and b. So after a few steps we must reach a mod b and b, at which we start subtracting from b.

Continuing this method is similar to the Euclidean algorithm and therefore results in reaching 0 at some point. Right before reaching 0, we must have a square piece of paper whose side lengths are the GCD.

4 Mechanical Chinese Remainder Theorem

In this problem, we will solve for $x \in \mathbb{Z}/30\mathbb{Z}$ such that

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

(a) Find a number $b_2 \in \mathbb{Z}/30\mathbb{Z}$ such that $b_2 \equiv 1 \pmod 2$, $b_2 \equiv 0 \pmod 3$, and $b_2 \equiv 0 \pmod 5$.

(b) Find a number $b_3 \in \mathbb{Z}/30\mathbb{Z}$ such that $b_3 \equiv 0 \pmod 2$, $b_3 \equiv 1 \pmod 3$, and $b_3 \equiv 0 \pmod 5$.

(c) Find a number $b_5 \in \mathbb{Z}/30\mathbb{Z}$ such that $b_5 \equiv 0 \pmod 2$, $b_5 \equiv 0 \pmod 3$, and $b_5 \equiv 1 \pmod 5$.

(d) What is x in terms of b_2, b_3, and b_5? Evaluate this to get a numerical value for x.

Solution:

(a) In order to make sure that $b_2 \equiv 0 \pmod 3$, we just need to make b_2 a multiple of 3–so we can start with just $b_2 = 3$. However, we now need to make sure we satisfy $b_2 \equiv 1 \pmod 2$, so we multiply this by $3^{-1} \pmod 2$. Since $3 \equiv 1 \pmod 2$, this is just 1. Thus, we so far have $b_2 = 3 \cdot 1$. We now need to make sure b_2 is a multiple of 5 (ie, is equivalent to zero mod 5), so we multiply our current value for b_2 by 5. But now we again need to make sure that b_2 is still equivalent to 1 mod 2, so we multiply by $5^{-1} \pmod 2$, which will again just be 1. Finally, we get $b_2 = 3 \cdot 1 \cdot 5 \cdot 1 = 15$.

(b) Similar to the previous part, we make b_3 just be $2 \cdot (2^{-1} \pmod 3) \cdot 5 \cdot (5^{-1} \pmod 3)$. We have that $2^{-1} \equiv 2 \pmod 3$ and $5^{-1} \equiv 2^{-1} \equiv 2 \pmod 3$, so $b_3 = 2 \cdot 2 \cdot 5 \cdot 2 = 40$. Reducing this to a number modulo 30, we get $b_3 = 10$.

(c) As before, we get $b_5 = 2 \cdot (2^{-1} \pmod 5) \cdot 3 \cdot (3^{-1} \pmod 5)$. Plugging in $2^{-1} \equiv 3 \pmod 5$ and $3^{-1} \equiv 2 \pmod 5$, we get $b_5 = 2 \cdot 3 \cdot 3 \cdot 2 = 36$. Since we want a number modulo 30, we reduce this to $b_5 = 6$.

(d) We can write $x = b_2 + 2b_3 + 3b_5$. This ensures that when we take x modulo 2, we end up getting $x \equiv b_2 + 2b_3 + 3b_5 \equiv 1 + 2(0) + 3(0) \equiv 1 \pmod 2$ as we expected–and similar statements can be made for the other two moduli. Evaluating this numerically, we get that $x = 15 + 2(10) + 3(6) = 53$. Reducing this to a number mod 30, we get $x = 23$.