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:

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

(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:

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

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

$$= \underline{\hspace{2em}}\times\mathbf{128}+\underline{\hspace{2em}}\times\mathbf{56}$$

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

$$\begin{aligned}
&= \underline{\hspace{2em}}\times\mathbf{440}+\underline{\hspace{2em}}\times\mathbf{128}\\
&= \underline{\hspace{2em}}\times\mathbf{2328}+\underline{\hspace{2em}}\times\mathbf{440}
\end{aligned}$$

(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?

2 Fibonacci GCD

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

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.

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.