1. 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.

2. Baby Fermat

Assume that a does have a multiplicative inverse $\pmod{m}$. Let us prove that its multiplicative inverse can be written as $a^k \pmod{m}$ for some $k \geq 0$.

- Consider the sequence $a, a^2, a^3, \ldots \pmod{m}$. Prove that this sequence has repetitions.
- Assuming that $a^i \equiv a^j \pmod{m}$, where $i > j$, what can you say about $a^{i-j} \pmod{m}$?
- Prove that the multiplicative inverse can be written as $a^k \pmod{m}$. What is k in terms of i and j?

3. Extended Euclid

In this problem we will consider the extended Euclid's algorithm.

1. Note that $x \bmod y$, 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:
   $gcd(2328, 440)$
   $= gcd(440, 128)$ $[128 \equiv 2328 \bmod 440 \equiv 2328 - 5 \times 440]$
   $= gcd(128, 56)$ $[56 \equiv 440 \bmod 128 \equiv 440 - \underline{\quad\quad} \times 128]$
   $= gcd(56, 16)$ $[16 \equiv 128 \bmod 56 \equiv 128 - \underline{\quad\quad} \times 56]$
   $= gcd(16, 8)$ $[8 \equiv 56 \bmod 16 \equiv 56 - \underline{\quad\quad} \times 16]$
   $= gcd(8, 0)$ $[0 \equiv 16 \bmod 8 \equiv 16 - 2 \times 8]$
   $= 8.$
   (Fill in the blanks)

2. 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:
   8
   $= 1 \times 8 + 0 \times 0 = 1 \times 8 + (16 - 2 \times 8)$
   $= 1 \times 16 - 1 \times 8$
   $=$ ____ $\times 56 +$ ____ $\times 16$ [Hint: Remember, $8 = 56 - 3 \times 16$. Substitute this into the above line...]

   $=$ ____ $\times 128 +$ ____ $\times 56$ [Hint: Remember, $16 = 128 - 2 \times 56$]

   $=$ ____ $\times 440 +$ ____ $\times 128$

   $=$ ____ $\times 2328 +$ ____ $\times 440$

3. 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.
4. What does this imply, in this case, about the multiplicative inverse of 17, in arithmetic mod 38?

4. Product of Two

Suppose that $p > 2$ is a prime number and S is a set of numbers between 1 and $p-1$ such that $|S| > \frac{p}{2}$. Prove that any number $1 \leq x \leq p-1$ can be written as the product of two (not necessarily distinct) numbers in S, mod p.