

1. Recursive Calls Calculate the greatest common divisor (gcd) of the following pairs of numbers using the Euclidean algorithm.

[Hasty refresher: starting with a pair of input values, keep repeating the operation “Replace the larger value with its remainder modulo the smaller value” over and over, until one of the values becomes zero. At that point, the other value is the gcd of the original two inputs (as well as of every pair of values along the way).

In pseudocode: $\text{gcd}(x, y) \rightarrow$ if $y = 0$ then return x else return $\text{gcd}(y, x \bmod y)$].

1. 208 and 872
2. 1952 and 872
3. $1952 \times n + 872$ and 1952

2. Baby Fermat

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

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

3. 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 .

4. 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:

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

(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:

$$\begin{aligned} &8 \\ &= 1 \times 8 + 0 \times 0 = 1 \times 8 + (16 - 2 \times 8) \\ &= 1 \times 16 - 1 \times 8 \\ &= \text{ ____ } \times 56 + \text{ ____ } \times 16 \quad [\text{Hint: Remember, } 8 = 56 - 3 \times 16. \text{ Substitute this into the above line...}] \\ &= \text{ ____ } \times 128 + \text{ ____ } \times 56 \quad [\text{Hint: Remember, } 16 = 128 - 2 \times 56] \\ &= \text{ ____ } \times 440 + \text{ ____ } \times 128 \\ &= \text{ ____ } \times 2328 + \text{ ____ } \times 440 \end{aligned}$$

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?