Extended GCD

egcd(a,b) = (d, x, y)

ax + by = d

a, 0

a·1 + 0·0 = a

a > b

v v

b a % b

```
def egcd(a:int, b:int) -> (int, int, int):
    if b == 0:
        return (a, 1, 0)
    else:
        d, x, y = egcd(b, a%b)
        return (d, y, x - ⌊a/b⌋ * y)
```

```
a>b
def gcd(a,b) -> int:
    if b==0:
        return a
    else:
        return gcd(b, a%b)
```

gcd(a,b) = gcd(b, a%b)

gcd(a,b) = d

∃x,y ∈ ℤ : ax + by = d

d = kdy + ld((x - ⌊a/b⌋ * y))

gcd(75,15)

75(1) + 15(-4) = 15

d = kdx + (a%b)y = bx + (a - ⌊a/b⌋b)y = bx + ay - ⌊a/b⌋by

a%b

d = bx + (a%b)y

kth, b, ∃q, r

r = a%b

qb ≡ 0 (mod b)

d = a(y) + b(x - ⌊a/b⌋ * y)

gcd(b, a%b) = d

a = kd = qb + r = qld + r

=> (k - ql)d = r = a%b

must also be div by d

(a%b) = (a/b)b

51, 19

quotient

51 = (2)·19 + (13) rem

a - fdiv(a,b) * b

a - qb = (a%b)

↑

⌊a/b⌋

Need to show converse

⌊17/3⌋ = ⌊5.66⌋ = 5

d = bx + (a%b)y

= bx +

CS 70 Discrete Mathematics and Probability Theory
Fall 2021 DIS 4A

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) Recall that our goal is to fill out the blanks in

$$8 = \_\_\_\_ \times \mathbf{2328} + \_\_\_\_ \times \mathbf{440}.$$

To do so, we work back up from the bottom, and express the 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?

2 Bijections

Let n be an odd number. Let $f(x)$ be a function from $\{0,1,\ldots,n-1\}$ to $\{0,1,\ldots,n-1\}$. In each of these cases say whether or not $f(x)$ is necessarily a bijection. Justify your answer (either prove $f(x)$ is a bijection or give a counterexample).

(a) $f(x) = 2x \pmod{n}$.

(b) $f(x) = 5x \pmod{n}$.

(c) n is prime and

$$f(x) = \begin{cases} 0 & \text{if } x = 0, \\ x^{-1} \pmod{n} & \text{if } x \neq 0. \end{cases}$$

(d) n is prime and $f(x) = x^2 \pmod{n}$.

3 Baby Fermat

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

(a) Consider the sequence $a, a^2, a^3, \ldots \pmod{m}$. Prove that this sequence has repetitions.
(**Hint:** Consider the Pigeonhole Principle.)

(b) Assuming that $a^i \equiv a^j \pmod{m}$, where $i > j$, what can you say about $a^{i-j} \pmod{m}$?

(c) Prove that the multiplicative inverse can be written as $a^k \pmod{m}$. What is k in terms of i and j?

4 Euler's Totient Function

Euler's totient function is defined as follows:

$$\phi(n) = |\{i : 1 \leq i \leq n, \texttt{gcd}(n,i) = 1\}|$$

In other words, $\phi(n)$ is the total number of positive integers less than or equal to n which are relatively prime to it. Here is a property of Euler's totient function that you can use without proof:

For m, n such that $\texttt{gcd}(m,n) = 1$, $\phi(mn) = \phi(m) \cdot \phi(n)$.

(a) Let p be a prime number. What is $\phi(p)$?

(b) Let p be a prime number and k be some positive integer. What is $\phi(p^k)$?

(c) Let p be a prime number and a be a positive integer smaller than p. What is $a^{\phi(p)} \pmod{p}$?
(Hint: use Fermat's Little Theorem.)

(d) Let b be a positive integer whose prime factors are $p_1, p_2, \ldots, p_k$. We can write $b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Show that for any a relatively prime to b, the following holds:

$$\forall i \in \{1, 2, \ldots, k\}, \;\; a^{\phi(b)} \equiv 1 \pmod{p_i}$$