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 $x \bmod y$, 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:

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

(Fill in the blanks)

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

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

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:

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

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

$$= \underline{\qquad} \times \mathbf{128} + \underline{\qquad} \times \mathbf{56}$$

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

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

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

**Solution:**

(a) Bijection, because there exists the inverse function $g(y) = 2^{-1}y \pmod{n}$. Since $n$ is odd, $\gcd(2,n) = 1$, so the multiplicative inverse of 2 exists.

(b) Not necessarily a bijection. For example, $n = 5, f(0) = f(1) = 0$.

(c) Bijection, because the multiplicative inverse is unique.

(d) Definitely not a bijection. For example, if $n = 3$, $f(1) = f(2) = 1$.

## 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 $a, a^2, a^3, \dots \pmod{m}$. 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 $j$?

**Solution:**

(a) There are only $m$ possible values mod $m$, and so after the $m$-th term we should see repetitions.

The Pigeonhole principle applies here - we have $m$ boxes that represent the different unique values that $a^k$ can take on $\pmod{m}$. Then, we can view $a, a^2, a^3, \cdots$ as the objects to put in the $m$ boxes. As soon as we have more than $m$ objects (in other words, we reach $a^{m+1}$ in our sequence), the Pigeonhole Principle implies that there will be a collision, or that at least two numbers in our sequence take on the same value $\pmod{m}$.

(b) We will temporarily use the notation $a^*$ for the multiplicative inverse of $a$ to avoid confusion. If we multiply both sides by $(a^*)^j$ in the third line below, we get

$$\begin{aligned}
a^i &\equiv a^j && \pmod{m}, \\
a^{i-j}\underbrace{a\cdots a}_{j\text{ times}} &\equiv \underbrace{a\cdots a}_{j\text{ times}} && \pmod{m}, \\
a^{i-j}\underbrace{a\cdots a}_{j\text{ times}}\cdot\underbrace{a^*\cdots a^*}_{j\text{ times}} &\equiv \underbrace{a\cdots a}_{j\text{ times}}\cdot\underbrace{a^*\cdots a^*}_{j\text{ times}} && \pmod{m}, \\
a^{i-j} &\equiv 1 && \pmod{m}.
\end{aligned}$$

(c) We can rewrite $a^{i-j} \equiv 1 \pmod{m}$ as $a^{i-j-1}a \equiv 1 \pmod{m}$. Therefore $a^{i-j-1}$ is the multiplicative inverse of $a \pmod{m}$.

## 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 $b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.

Show that for any $a$ relatively prime to $b$, the following holds:

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

**Solution:**

(a) Since $p$ is prime, all the numbers from 1 to $p-1$ are relatively prime to $p$.

So, $\phi(p) = p-1$.

(b) The only positive integers less than $p^k$ which are not relatively prime to $p^k$ are multiples of $p$.

Why is this true? This is so because the only possible prime factor which can be shared with $p^k$ is $p$. Hence, if any number is not relatively prime to $p^k$, it has to have a prime factor of $p$ which means that it is a multiple of $p$.

The multiples of $p$ which are $\leq p^k$ are $1\cdot p, 2\cdot p, \ldots, p^{k-1}\cdot p$. There are $p^{k-1}$ of these.

The total number of positive integers less than or equal to $p^k$ is $p^k$.

So $\phi(p^k) = p^k - p^{k-1} = p^{k-1}\cdot(p-1)$.

(c) From Fermat's Little Theorem, and part (a),

$a^{\phi(p)} \equiv a^{p-1} \equiv 1 \pmod p$

(d) From the property of the totient function and part (b):

$$
\begin{aligned}
\phi(b) &= \phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}) \\
&= \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \dots \phi(p_k^{\alpha_k}) \\
&= p_1^{\alpha_1 - 1}(p_1 - 1) \cdot p_2^{\alpha_2 - 1}(p_2 - 1) \dots p_k^{\alpha_k - 1}(p_k - 1)
\end{aligned}
$$

This shows that, for every $p_i$, which is a prime factor of $b$, we can write $\phi(b) = c \cdot (p_i - 1)$, where $c$ is some constant. Since $a$ and $b$ are relatively prime, $a$ is also relatively prime with $p_i$. From Fermat's Little Theorem:

$a^{\phi(b)} \equiv a^{c \cdot (p_i - 1)} \equiv (a^{(p_i - 1)})^c \equiv 1^c \equiv 1 \mod p_i$

Since we picked $p_i$ arbitrarily from the set of prime factors of $b$, this holds for all such $p_i$.