CS 70 Discrete Mathematics and Probability Theory
Summer 2019 James Hulett and Elizabeth Yang

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:

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

(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?

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 Mechanical Chinese Remainder Theorem

In this problem, we will solve for x 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 $0 \leq b_2 < 30$ 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 $0 \leq b_3 < 30$ 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 $0 \leq b_5 < 30$ 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.

Solution:

(a) (Note that students can use Extended Euclid for bigger numbers like mod 11.) In order to make sure that $b_2 \equiv 0 \pmod 3$, we just need to make b_2 a multiple of 3–so we can start with just $b_2 = 3$. However, we now need to make sure we satisfy $b_2 \equiv 1 \pmod 2$, so we multiply

this by $3^{-1} \pmod 2$. Since $3 \equiv 1 \pmod 2$, this is just 1. Thus, we so far have $b_2 = 3 \cdot 1$. We now need to make sure b_2 is a multiple of 5 (ie, is equivalent to zero mod 5), so we multiply our current value for b_2 by 5. But now we again need to make sure that b_2 is still equivalent to 1 mod 2, so we multiply by $5^{-1} \pmod 2$, which will again just be 1. Finally, we get $b_2 = 3 \cdot 1 \cdot 5 \cdot 1 = 15$.

(b) Similar to the previous part, we make b_3 just be $2 \cdot (2^{-1} \pmod 3) \cdot 5 \cdot (5^{-1} \pmod 3)$. We have that $2^{-1} \equiv 2 \pmod 3$ and $5^{-1} \equiv 2^{-1} \equiv 2 \pmod 3$, so $b_3 = 2 \cdot 2 \cdot 5 \cdot 2 = 40$. Reducing this to a number modulo 30, we get $b_3 = 10$.

(c) As before, we get $b_5 = 2 \cdot (2^{-1} \pmod 5) \cdot 3 \cdot (3^{-1} \pmod 5)$. Plugging in $2^{-1} \equiv 3 \pmod 5$ and $3^{-1} \equiv 2 \pmod 5$, we get $b_5 = 2 \cdot 3 \cdot 3 \cdot 2 = 36$. Since we want a number modulo 30, we reduce this to $b_5 = 6$.

(d) We went through all the above steps to ensure that $b_2 \equiv 1 \pmod 2$ and has no remainder for $\pmod 3$ and $\pmod 5$, $b_3 \equiv 1 \pmod 3$ and has no remainder for $\pmod 2$ and $\pmod 5$, $b_5 \equiv 1 \pmod 5$ and has no remainder for $\pmod 2$ and $\pmod 3$. So by multiplying coefficients before b_i and adding them together enables us to manipulate the remainders of x in terms of $\pmod 2$, $\pmod 3$, $\pmod 5$ separately without affecting the remainders of others. We can write $x = b_2 + 2b_3 + 3b_5$. This ensures that when we take x modulo 2, we end up getting $x \equiv b_2 + 2b_3 + 3b_5 \equiv 1 + 2(0) + 3(0) \equiv 1 \pmod 2$ as we expected–and similar statements can be made for the other two moduli. Evaluating this numerically, we get that $x = 15 + 2(10) + 3(6) = 53$. Reducing this to a number mod 30, we get $x = 23$.

3 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 $n = 3$, $f(1) = f(2) = 1$.

4 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?

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 $a \pmod m$.