Alexander Garcia
24 February 2017

1. Question 1

   (a) $-17 \ mod \ 4 = 3$

   $1 = a *_4 -17(mod \ 4)$

   $1 = a *_4 3$

   $(3a)(mod \ 4) = 1$

   $a = 3$

   In this case, m must equal 4, since it is the modulo of the original value for "b". The equation can then be easily solved for a, which could be 3.

   (b) $-17 \div 4 = -5 \ rem \ 3$

   This follows from the definition of the modulo operator, where when $a \ mod \ b$, this means that $a = bq + r$, where r is always a positive integer. Since r must be positive, we obtain the value -20 from bq, giving us the smallest positive r. Therefore, $a = 3$.

   (c) $a \equiv -17 \ (mod \ 4)$

   $4|(a + 17)$

   $a = 3$

Alexander Garcia

24 February 2017

2. Question 2

$a \equiv b\ (mod\ m)$

$m \mid a - b$	Definition of congruency
$\exists c, mc = a - b$	Definition of the "divisible" operator
$p = gcd(a, m); q = gcd(b, m)$	Assignment of gcd operations
$\frac{a}{p} = \frac{mc}{p} + \frac{b}{p}$	Rewriting of "divisible" operator. Here, $\frac{a}{p}$ and $\frac{m}{p}$ are both integers.
$\frac{b}{p} = \frac{-a}{p} + \frac{mc}{p}$	Reorganization of expression

Since the two parts of the equation that make up $\frac{b}{p}$ are both integers, $\frac{b}{p}$ must be an integer. Therefore, $p \mid b$. In addition, $p \leq q$, since q is the largest number that can divide b.

$\frac{a}{q} = \frac{mc}{q} + \frac{b}{q}$ Rewriting of "divisible" operator. Here, $\frac{mc}{q}$ and $\frac{b}{q}$ are both whole numbers.

Again, the two parts making up $\frac{a}{q}$ are integers, so $\frac{a}{q}$ must be an integer. This time, however, $q \leq p$, for the same reason that $p \leq q$. The only possible conclusion then, is that $p = q$.

$\therefore gcd(a, m) = gcd(b, m)$

Alexander Garcia

24 February 2017

3. Question 3

(a)

$gcd(124, 323) = d, d \in \mathbb{Z}$	Representation of gcd
$d = sa + tb$	Bezout's Theorem
Now begin stepping through the given algorithm	
Representation of gcd	Reformatting of representation
$323 = 2 * 124 + 75$	$75 = 323 - (2 * 124)$
$124 = 1 * 75 + 49$	$49 = 124 - (1 * 75)$
$75 = 1 * 49 + 26$	$26 = 75 - *1 * 49)$
$49 = 1 * 26 + 23$	$23 = 49 - (1 * 26)$
$26 = 1 * 23 + 3$	$3 = 26 - (1 * 23)$
$23 = 7 * 3 + 2$	$2 = 23 - (7 * 3)$
$3 = 1 * 2 + 1$	$1 = 3 - (1 * 2)$
$2 = 2 * 1$	$gcd(124, 323) = 1$

These two numbers are relatively prime since their gcd $= 1$. We must now go "backwards" through these steps and find the coefficients associated with the two numbers (s, t) to make $124s + 323t = 1$ true.

$1 = 3 - (1 * 2)$	Starting premise
$2 = 23 - (7 * 3)$	Starting premise
$1 = 3 - 1 * (23 - 7 * 3)$	$8 * 3 - 1 * 23$
$8 * (26 - 1 * 23) - 1 * 23$	$8 * 26 - 9 * 23$
$8 * 26 - 9 * (49 - 1 * 26)$	$17 * 26 - 9 * 49$
$17 * (75 - 1 * 49) - 9 * 49$	$17 * 75 - 26 * 49$
$17 * 75 - 26 * (124 - 1 * 75)$	$43 * 75 - 26 * 124$
$43 * (323 - 2 * 124) - 26 * 124$	$43 * 323 - 112 * 124$

The final item in the table contains both of the original numbers, and the expression is equal to 1 the whole way down. Therefore, the Bezout Coefficients of 124,323 are -112, 43 respectively.

Alexander Garcia

24 February 2017

(b) This calculation is done through the same steps as part (a).

$gcd(3457, 4669) = d, d \in Z$	Representation of gcd
$4669 = 1 * 3457 + 1212$	$1212 = 4669 - 1 * 3457$
$3457 = 2 * 1212 + 1033$	$1033 = 3457 - 2 * 1212$
$1212 = 1 * 1033 + 179$	$179 = 1212 - 1 * 1033$
$1033 = 5 * 179 + 138$	$138 = 1033 - 5 * 179$
$179 = 1 * 138 + 41$	$41 = 17901 * 138$
$138 = 3 * 41 + 15$	$15 = 138 - 3 * 41$
$41 = 2 * 15 + 11$	$11 = 41 - 2 * 15$
$15 = 1 * 11 + 4$	$4 = 15 - 1 * 11$
$11 = 2 * 4 + 3$	$4 = 11 - 2 * 4$
$4 = 1 * 3 + 1$	$1 = 4 - 1 * 3$
$3 = 3 * 1$	$gcd(3457, 4669) = 1$

Now repeat the steps from before, going backwards to find the Bezout Coefficients.

All expressions in the table are equal to 1.

$1 = 4 - 1 * (11 - 2 * 4)$	$3 * 4 - 1 * 11$
$3 * (15 - 1 * 11) - 1 * 11$	$3 * 15 - 4 * 11$
$3 * 15 - 4 * (41 - 2 * 15)$	$11 * 15 - 4 * 41$
$11 * (138 - 3 * 41) - 4 * 41$	$11 * 138 - 37 * 41$
$11 * 138 - 37 * (179 - 1 * 138)$	$48 * 138 - 37 * 179$
$48 * (1033 - 5 * 179) - 37 * 179$	$48 * 1033 - 277 * 179$
$48 * 1033 - 277 * (1212 - 1 * 1033)$	$325 * 1033 - 277 * 1212$
$325 * (3457 - 2 * 1212) - 277 * 1212$	$325 * 3457 - 927 * 1212$
$325 * 3457 - 927 * (4669 - 1 * 3457)$	1252 * 3457 - 927 * 4669 = 1

Bazout Coefficients: $s = 1252, t = -927$

Alexander Garcia

24 February 2017

4. Question 4

We begin with a proof by contradiction

Assume there are a finite number of primes of form $q = 3k + 2$

$Q = \{q_1, q_2, q_3, \dots q_n\}$ Q is the set of ALL primes of the form $2k + 1$
$N = 3(q_1 * q_2 * \cdots * q_n) + 2$ $3 \nmid N \wedge q_i \nmid N, q_i \in Q$

It is known that $\nexists q_i \in Q \; S.T. \; q_i|N$, since $q_i|N - 2$. If $q_i|N$, then $q_i|2$, which cannot be true, since q_i is an odd prime.

$N = odd * even + even \rightarrow N = odd \quad 2 \nmid N$

According to the Fundamental Theorem of Arithmtic, any integer (in this case N), can be represented uniquely as a product of primes. According to the initial assumption, N is not divisible by any $q_i \in Q$. Then if N is the produt of primes of the form $p_i = 3k + 1$, N would have the form $3k + 1$.

$N = 3k + 1, k \in Z$
However, the premise was that N is of the form $3k + 2$
Therefore, $\exists p, p = 3k + 2 \wedge p \notin Q$

Because Q was defined to be the set of ALL prime numbers of the form 3k+2, we have a contradiction.

$\therefore |Q| = \infty$