Modular Arithmetic.

The following problems are intended to give you some practice and familiarity with modular arithmetic computations, and to make you comfortable with the Euclid's Algorithm and the notion of multiplicative inverses modulo m.

1. Calculate the smallest non-negative $x \in \mathbb{N}$ for each of the following expressions:

   (a) $x = 21 \mod 12$

   $x =$

   Recall to compute $a \bmod b$, we divide a by b to write $a = b\lfloor \frac{a}{b} \rfloor + r$. The answer is $x = r$.

   We can express 21 as $12 \times 1 + 9$, so the remainder 9 is the solution. The equivalence class of $9 \bmod 12$ is $\{... - 15,\ -3,\ 9,\ 21,\ 33...\}$, obtained by adding integer multiples of 12 to 9. (Note that in this case it might have been easier to notice that 21 was 3 less than a multiple of 12: $21 = 12 \times 2 + (-3)$. To convert a fully simplified negative answer like this to an answer in the range $0 \le x < 12$, simply add the modulus 12: $-3 + 12 = 9$).

   (b) $x = -27 \mod 4$

   Recall to compute $a \bmod b$, we divide a by b to write $a = b\lfloor \frac{a}{b} \rfloor + r$. The answer is $x = r$.

   We can express -27 as $4 \times (-7) + 1$, so the remainder 1 is the solution. The equivalence class of $1 \bmod 4$ is $\{... - 7,\ -3,\ 1,\ 5,\ 9...\}$, obtained by adding integer multiples of 4 to 1.

   (c) $x = 7 \mod 64$

   $x =$

   Recall to compute $a \bmod b$, we divide a by b to write $a = b\lfloor \frac{a}{b} \rfloor + r$. The answer is $x = r$.

   We can express 7 as $64 \times 0 + 7$, so the remainder 7 is the solution. The equivalence class of $7 \bmod 64$ is $\{... - 121,\ -57,\ 7,\ 71,\ 135...\}$, obtained by adding integer multiples of 64 to 7.

   (d) $x = 101 \mod 2$

   $x =$

   Recall to compute $a \bmod b$, we divide a by b to write $a = b\lfloor \frac{a}{b} \rfloor + r$. The answer is $x = r$.

   We can express 101 as $2 \times 50 + 1$, so the remainder 1 is the solution. The equivalence class of $1 \bmod 2$ is simply all of the odd integers.

   (e) $x = 55 \mod 5$

   $x =$

   Recall to compute $a \bmod b$, we divide a by b to write $a = b\lfloor \frac{a}{b} \rfloor + r$. The answer is $x = r$.

   We can express 55 as $5 \times 11 + 0$, so the remainder 0 is the solution. The equivalence class of $0 \bmod 5$ is $\{... - 10,\ -5,\ 0,\ 5,\ 10...\}$, obtained by adding integer multiples of 5 to 0.

   (f) $x = 63 \mod 13$

   $x =$

   Recall to compute $a \bmod b$, we divide a by b to write $a = b\lfloor \frac{a}{b} \rfloor + r$. The answer is $x = r$.

   We can express 63 as $13 \times 4 + 11$, so the remainder 11 is the solution. The equivalence class of $11 \bmod 13$ is $\{... - 15,\ -2,\ 11,\ 24,\ 37...\}$, obtained by adding integer multiples of 13 to 11. (Note that in this case it might have been easier to notice that 63 was 2 less than a multiple of 13: $63 = 13 \times 5 + (-2)$. To convert a fully simplified negative answer like this to an answer in the range $0 \le x < 13$, simply add the modulus 13: $-2 + 13 = 11$).

   (g) $x = -25 \mod 7$

   $x =$

   Recall to compute $a \bmod b$, we divide a by b to write $a = b\lfloor \frac{a}{b} \rfloor + r$. The answer is $x = r$.

   We can express -25 as $7 \times (-4) + 3$, so the remainder 3 is the solution. The equivalence class of $3 \bmod 7$ is $\{... -11,\ -4,\ 3,\ 10,\ 17...\}$, obtained by adding integer multiples of 7 to 3.

   (h) $x = -61 \mod 10$

   Recall to compute $a \bmod b$, we divide a by b to write $a = b\lfloor \frac{a}{b} \rfloor + r$. The answer is $x = r$.

   We can express -61 as $10 \times (-7) + 9$, so the remainder 9 is the solution. The equivalence class of $9 \bmod 10$ is $\{... - 11,\ -1,\ 9,\ 19...\}$, obtained by adding integer multiples of 10 to 9. (Note that in this case it might have been easier to notice that -61 was 1 less than a multiple of 10: $-61 = 10 \times (-6) + (-1)$. To convert a fully simplified negative answer like this to an answer in the range $0 \le x < 10$, simply add the modulus 10: $-1 + 10 = 9$).

   (i) $x = 20 \mod 1$

   $x =$ Recall to compute $a \bmod b$, we divide a by b to write $a = b\lfloor \frac{a}{b} \rfloor + r$. The answer is $x = r$.

   We can express 20 as $1 \times 20 + 0$, so the remainder 0 is the solution. All integers are in the equivalence class $0 \bmod 1$, because all integers are perfect multiples of 1.

   (j) $x = 89 \mod 5$

   $x =$

   Recall to compute $a \bmod b$, we divide a by b to write $a = b\lfloor \frac{a}{b} \rfloor + r$. The answer is $x = r$.

   We can express 89 as $5 \times 17 + 4$, so the remainder 4 is the solution. The equivalence class of $4 \bmod 5$ is $\{... - 6,\ -1,\ 4,\ 9...\}$, obtained by adding integer multiples of 5 to 4. (Note that in this case it might have been easier to notice that 89 was 1 less than a multiple of 5: $89 = 5 \times 18 + (-1)$. To convert a fully simplified negative answer like this to an answer in the range $0 \le x < 5$, simply add the modulus 5: $-1 + 5 = 4$).

   (k) $x = -32 \mod 6$

   Recall to compute $a \bmod b$, we divide a by b to write $a = b\lfloor \frac{a}{b} \rfloor + r$. The answer is $x = r$.

   We can express -32 as $6 \times (-6) + 4$, so the remainder 4 is the solution. The equivalence class of $4 \bmod 6$ is $\{... - 8,\ -2,\ 4,\ 10,\ 16...\}$, obtained by adding integer multiples of 6 to 4. (Note that in this case it might have been easier to notice that -32 was 2 less than a multiple of 6: $-32 = 6 \times (-5) + (-2)$. To convert a fully simplified negative answer like this to an answer in the range $0 \le x < 6$, simply add the modulus 6: $-2 + 6 = 4$).

   (l) $x = 34 \mod 16$

   $x =$

   Recall to compute $a \bmod b$, we divide a by b to write $a = b\lfloor \frac{a}{b} \rfloor + r$. The answer is $x = r$.

   We can express 34 as $16 \times 2 + 2$, so the remainder 2 is the solution. The equivalence class of $2 \bmod 16$ is $\{... - 30,\ -14,\ 2,\ 18,\ 34...\}$, obtained by adding integer multiples of 16 to 2.

   (m) $x = 79 \mod 4$

   $x =$

   Recall to compute $a \bmod b$, we divide a by b to write $a = b\lfloor \frac{a}{b} \rfloor + r$. The answer is $x = r$.

   We can express 79 as $4 \times 19 + 3$, so the remainder 3 is the solution. The equivalence class of $3 \bmod 4$ is $\{... - 5,\ -1,\ 3,\ 7,\ 11...\}$, obtained by adding integer multiples of 4 to 3. (Note that in this case it might have been easier to notice that 79 was 1 less than a multiple of 4: $79 = 4 \times 20 + (-1)$. To convert a fully simplified negative answer like this to an answer in the range $0 \le x < 4$, simply add the modulus 4: $-1 + 4 = 3$).

   (n) $x = -37 \mod 5$

   Recall to compute $a \bmod b$, we divide a by b to write $a = b\lfloor \frac{a}{b} \rfloor + r$. The answer is $x = r$.

   We can express -37 as $5 \times (-8) + 3$, so the remainder 3 is the solution. The equivalence class of $3 \bmod 5$ is $\{... - 7,\ -2,\ 3,\ 8...\}$, obtained by adding integer multiples of 5 to 3. (Note that in this case it might have been easier to notice that -37 was 2 less than a multiple of 5: $-37 = 5 \times (-7) + (-2)$. To convert a fully simplified negative answer like this to an answer in the range $0 \le x < 5$, simply add the modulus 5: $-2 + 5 = 3$).

   (o) $x = 17 \mod 3$

   $x =$

   Recall to compute $a \bmod b$, we divide a by b to write $a = b\lfloor \frac{a}{b} \rfloor + r$. The answer is $x = r$.

   We can express 17 as $3 \times 5 + 2$, so the remainder 2 is the solution. The equivalence class of $2 \bmod 3$ is $\{... - 4,\ -1,\ 2,\ 5,\ 8...\}$, obtained by adding integer multiples of 3 to 2. (Note that in this case it might have been easier to notice that 17 was 1 less than a multiple of 3: $17 = 3 \times 6 + (-1)$. To convert a fully simplified negative answer like this to an answer in the range $0 \le x < 3$, simply add the modulus 3: $-1 + 3 = 2$).

   (p) $x = -45 \mod 47$

   Recall to compute $a \bmod b$, we divide a by b to write $a = b\lfloor \frac{a}{b} \rfloor + r$. The answer is $x = r$.

   We can express -45 as $47 \times (-1) + 2$, so the remainder 2 is the solution. The equivalence class of $2 \bmod 47$ is $\{... - 92,\ -45,\ 2,\ 49,\ 96...\}$, obtained by adding integer multiples of 47 to 2.

2. Decide whether each of the following statements are true or false. The expression $a \equiv b \mod 5$ reads "a is equivalent to b modulo m".

   (a) $10 \equiv 2 \mod 5$
   - True
   - False

   Recall $a \equiv b \bmod m$ iff m divides $a - b$.
   $10 - 2 = 7$, which is not divisible by 5, so $10 \not\equiv 2 \bmod 5$

   (b) $42 \equiv 7 \mod 5$
   - True
   - False

   Recall $a \equiv b \bmod m$ iff m divides $a - b$.
   $42 - 7 = 35$, which is divisible by 5, so $42 \equiv 7 \bmod 5$

   (c) $18 \equiv -4 \mod 11$
   - True
   - False

   Recall $a \equiv b \bmod m$ iff m divides $a - b$.
   $18 - (-4) = 22$, which is divisble by 11, so $18 \equiv -4 \bmod 11$

   (d) $12 \equiv -6 \mod 5$
   - True
   - False

   Recall $a \equiv b \bmod m$ iff m divides $a - b$.
   $12 - (-6) = 18$, which is not divisble by 5, so $12 \not\equiv -6 \bmod 5$

   (e) $28 \equiv 14 \mod 7$
   - True
   - False

   Recall $a \equiv b \bmod m$ iff m divides $a - b$.
   $28 - 14 = 14$, which is divisble by 7, so $28 \equiv 14 \bmod 7$

   (f) $-37 \equiv 37 \mod 6$
   - True
   - False

   Recall $a \equiv b \bmod m$ iff m divides $a - b$.
   $-37 - 37 = -74$, which is not divisble by 6, so $-37 \not\equiv 37 \bmod 6$. Note that it is *not* in general true that $a \equiv -a \bmod m$!

   (g) $44 \equiv -44 \mod 8$
   - True
   - False

   $44 - (-44) = 88$, which is divisble by 8, so $44 \equiv -44 \bmod 8$. Note that it is *not* in general true that $a \equiv -a \bmod m$! (Why does it work here?)

   (h) $-17 \equiv -29 \mod 4$
   - True
   - False

   $-17 - (-29) = 12$, which is divisible by 4, so $-17 \equiv -29 \bmod 4$.

3. In the notes, you learn that x has a multiplicative inverse $\mod m$ if and only if the greatest common divisor of x and m is 1. For each of the following questions, first decide if x has a multiplicative inverse $\mod m$, then calculate y to be the inverse of x in base m (if one exists), or give y such that $xy = 0 \mod m$. In all cases report the smallest such y that is bigger than 0.

   (a) $x = 3, m = 5$.

   What is $gcd(x, m)$? Review the definition and existence conditions of an inverse modulo m in the notes.
   - x has an inverse $\mod m$.
   - x does not have an inverse $\mod m$.

   Yes, $gcd(x, m) = gcd(3, 5) = 1$

   $y =$

   What is $gcd(x, m)$? Review the definition and existence conditions of an inverse modulo m in the notes.

   Since 3 and 5 are small values, we can use guess-and-check to see that 2 is the multiplicative inverse ($3 \times 2 = 6 \equiv 1 \bmod 5$). This answer is unique mod5, so other numbers in the equivalence class (7, 12, 17, etc) would also work.

   (b) $x = 3, m = 6$.

   Review the definition and existence conditions of an inverse modulo m in the notes.
   - x has an inverse $\mod m$.
   - x does not have an inverse $\mod m$.

   No, $gcd(x, m) = gcd(3, 6) = 3$. The numbers are not coprime, so no inverse exists.

   $y =$

   What is $gcd(x, m)$? Review the definition and existence conditions of an inverse modulo m in the notes.

   We want to find y such that $3y \equiv 0 \bmod 6$. By trial and error we find that 2 works ($3 \times 2 = 6 \equiv 0 \bmod 6$). Any multiple of 2 would also work.

   (c) $x = 15, m = 4$.

   Review the definition and existence conditions of an inverse modulo m in the notes.
   - x has an inverse $\mod m$.
   - x does not have an inverse $\mod m$.

   Yes, $gcd(x, m) = gcd(15, 4) = 1$, so an inverse exists.

   $y =$

   What is $gcd(x, m)$? Review the definition and existence conditions of an inverse modulo m in the notes.

   We know $15^{-1} \bmod 4 = (15 \bmod 4)^{-1} \bmod 4 = 3^{-1} \bmod 4$. From trial and error we can see that 3 works ($3 \times 3 = 9 \equiv 1 \bmod 4$). Quickly verifying, we see that $15 \times 3 = 45 \equiv 1 \bmod 4$. Anything in the same equivalence class (7, 11, 15, etc) would also work.

   (d) $x = 3, m = 4$.

   Review the definition and existence conditions of an inverse modulo m in the notes.
   - x has an inverse $\mod m$.
   - x does not have an inverse $\mod m$.

   Yes, $gcd(x, m) = gcd(3, 4) = 1$, so an inverse exists.

   $y =$

   What is $gcd(x, m)$? Review the definition and existence conditions of an inverse modulo m in the notes.

   From above, we found $3^{-1} \bmod 4 = 3$, or anything equivalent to $3 \bmod 4$.

   (e) $x = 12, m = 16$.

   Review the definition and existence conditions of an inverse modulo m in the notes.
   - x has an inverse $\mod m$.
   - x does not have an inverse $\mod m$.

   No, $gcd(x, m) = gcd(12, 16) = 4$. The numbers are not coprime, so no inverse exists.

   $y =$

   What is $gcd(x, m)$? Review the definition and existence conditions of an inverse modulo m in the notes.

   We want to find y such that $12y \equiv 0 \bmod 16$, so $12y$ must be a multiple of 16. To find the smallest such y, solve $12y = lcm(12, 16) = 48$. This gives us $y = 4$. Any multiple of 4 would also work.

4. Euclid's algorithm is a fast algorithm for computing the greatest common divisor of two integers. Here is an example. To compute $gcd(16, 10)$:

$$\begin{aligned} 16 &= 10 \times 1 + 6 && && (1)\\ 10 &= 6 \times 1 + 4 && \text{(notice this is a recursive call of } gcd(10,6)\text{)} && (2)\\ 6 &= 4 \times 1 + 2 && \text{(notice this is a recursive call of } gcd(6,4)\text{)} && (3)\\ 4 &= 2 \times 2 + 0 && \text{(notice this is a recursive call of } gcd(4,2)\text{)} && (4) \end{aligned}$$

So $gcd(16, 10) = 2$, the last non-zero remainder. We can also back substitute to find x, y such that

$$2 = 16x + 10y = gcd(16, 10).$$

Here is how:

$$\begin{aligned} \text{Rearrange (3) to get an expression}&\\ \text{for gcd(16,10):}\quad 2 &= 6 - 4 \times 1\\ \text{rearrange (2) to get } 4 = (10 - 6 \times 1)&\\ \text{and substitute:}\quad 2 &= 6 - (10 - 6 \times 1) \times 1\\ \text{simplify:}\quad 2 &= -10 + 6 \times 2\\ \text{now rearrange (1) to get}&\\ 6 = (16 - 10 \times 1) \text{ and substitute:}\quad 2 &= -10 + (16 - 10 \times 1) \times 2\\ \text{simplify:}\quad 2 &= 16 \times 2 - 10 \times 3 \end{aligned}$$

So $x = 2$ and $y = -3$.

Now, we will practice running Euclid's algorithm. As we saw above, the ith step of Euclid's algorithm is of the form

$$a_i = b_i \times q_i + r_i,$$

where a_1 and b_1 are the two numbers for which we are trying to compute the greatest common divisor. The following questions will ask you to give the values for a_i, b_i, q_i, r_i for different steps i.

   (a) Run Euclid's algorithm to determine the greatest common divisor of $a = 8, b = 22$.

      i. In the first step of the algorithm, we have $a_1 = 22$ and $b_1 = 8$. Give the values for q_1 and r_1:
      $q_1 =$
      We're solving $22 = 8 \times q_1 + r_1$, so $q_1 = \lfloor \frac{22}{8} \rfloor = 2$.
      Review Euclid's algorithm in the notes.
      $r_1 =$
      Review Euclid's algorithm in the notes.
      We're solving $22 = 8 \times q_1 + r_1$, so $r_1 = 22 \bmod 8 = 6$.

      ii. What are a_2, b_2, q_2, and r_2?
      $a_2 =$
      Review Euclid's algorithm in the notes.
      By the algorithm, we're now trying to compute $gcd(8, 6)$, so $a_2 = 8$.
      $b_2 =$
      Review Euclid's algorithm in the notes
      By the algorithm, we're now trying to compute $gcd(8, 6)$, so $b_2 = 6$.
      $q_2 =$
      Review Euclid's algorithm in the notes.
      We're trying to solve $8 = 6 \times q_2 + r_2$, so $q_2 = \lfloor \frac{8}{6} \rfloor = 1$.
      $r_2 =$
      Review Euclid's algorithm in the notes.
      We're trying to solve $8 = 6 \times q_2 + r_2$, so $r_2 = 8 \bmod 6 = 2$.

      iii. What are a_3, b_3, q_3, and r_3?
      $a_3 =$
      Review Euclid's algorithm in the notes.
      By the algorithm, we're now trying to find $gcd(6, 2)$, so $a_3 = 6$.
      $b_3 =$
      Review Euclid's algorithm in the notes.
      By the algorithm, we're now trying to find $gcd(6, 2)$, so $b_3 = 2$.
      $q_3 =$
      Review Euclid's algorithm in the notes.
      We're trying to solve $6 = 2 \times q_3 + r_3$, so $q_3 = \lfloor \frac{6}{2} \rfloor = 3$.
      $r_3 =$
      Review Euclid's algorithm in the notes.
      We're trying to solve $6 = 2 \times q_3 + r_3$, so $r_3 = 2 \bmod 2 = 0$.

      iv. What is the greatest common divisor of 22 and 8?
      $gcd(22, 8) =$
      Review Euclid's algorithm in the notes.
      We've determined $gcd(22, 8) = gcd(2, 0)$, and by definition the greatest common denominator of x and 0 is x, so $gcd(22, 8) = 2$.

   (b) Now, follow the process demonstrated above to find x, y such that $8x + 22y = gcd(8, 22)$.

      i. We start by taking $r_2 = a_2 - b_2 \times q_2$. We then substitute some expression for b_2, and after simplifying end up with the expression $r_2 = \alpha \times b_1 + \beta \times a_1$. What are α, β?
      $\alpha =$
      Review Euclid's algorithm in the notes.
      $\alpha = 3$. For full explanation, see solution to β.
      $\beta =$
      Review Euclid's algorithm in the notes.
      $\beta = -1$. Recall that $a_2 = 8$, $b_2 = 6$, $q_2 = 1$, and $r_2 = 2$. We know

      $$2 = 8 - 6 \times 1 = 8 \times 1 + 6 \times (-1)$$

      Now let's try to express this in terms of $b_1 = 8$ and $a_1 = 22$.

      We're trying to find α and β such that

      $$2 = 8 \times \alpha + 22 \times \beta$$

      First we express a_2 and b_2 in terms of a_1 and b_1. We know $8 \times 2 + 6 = 22$, so $6 = 22 - 8 \times 2$.

      $$2 = 8 \times 1 + (22 - 8 \times 2) \times (-1)$$

      Combining like terms,

      $$2 = 8 \times (1 + 2) + 22 \times (-1) = 8 \times 3 + 22 \times (-1)$$

      Thus we have $\alpha = 3$ and $\beta = -1$.

      ii. What are x, y?
      $x =$
      $x = \alpha = 3$.
      Review Euclid's algorithm in the notes.
      $y =$
      Review Euclid's algorithm in the notes.
      $y = \beta = -1$.

   (c) Run Euclid's algorithm to determine the greatest common divisor of $x = 13, y = 21$.

      i. In the first step of the algorithm, we have $a_1 = 21$ and $b_1 = 13$. Give the values for q_1 and r_1:
      $q_1 =$
      Review Euclid's algorithm in the notes.
      $q_1 = \lfloor \frac{21}{13} \rfloor = 1$.
      $r_1 =$
      Review Euclid's algorithm in the notes.
      $r_1 = 21 \bmod 13 = 8$.

      ii. What are a_2, b_2, q_2, and r_2?
      $a_2 =$
      Review Euclid's algorithm in the notes.
      $a_2 = b_1 = 13$
      $b_2 =$
      Review Euclid's algorithm in the notes.
      $b_2 = r_1 = 8$.
      $q_2 =$
      $q_2 = \lfloor \frac{13}{8} \rfloor = 1$.
      Review Euclid's algorithm in the notes.
      $r_2 =$
      Review Euclid's algorithm in the notes.
      $r_2 = 13 \bmod 8 = 5$.

      iii. What are a_3, b_3, q_3, and r_3?
      $a_3 =$
      Review Euclid's algorithm in the notes.
      $a_3 = b_2 = 8$.
      $b_3 =$
      Review Euclid's algorithm in the notes.
      $b_3 = r_2 = 5$.
      $q_3 =$
      Review Euclid's algorithm in the notes.
      $q_3 = \lfloor \frac{8}{5} \rfloor = 1$.
      $r_3 =$
      Review Euclid's algorithm in the notes.
      $r_3 = 8 \bmod 5 = 3$.

      iv. What are a_4, b_4, q_4, and r_4?
      $a_4 =$
      Review Euclid's algorithm in the notes.
      $a_4 = b_3 = 5$.
      $b_4 =$
      Review Euclid's algorithm in the notes.
      $b_4 = r_3 = 3$.
      $q_4 =$
      Review Euclid's algorithm in the notes.
      $q_4 = \lfloor \frac{5}{3} \rfloor = 1$.
      $r_4 =$
      Review Euclid's algorithm in the notes.
      $r_4 = 5 \bmod 3 = 2$.

      v. What are a_5, b_5, q_5, and r_5?
      $a_5 =$
      Review Euclid's algorithm in the notes.
      $a_5 = b_4 = 3$.
      $b_5 =$
      Review Euclid's algorithm in the notes.
      $b_5 = r_4 = 2$.
      $q_5 =$
      Review Euclid's algorithm in the notes.
      $q_5 = \lfloor \frac{3}{2} \rfloor = 1$.
      $r_5 =$
      Review Euclid's algorithm in the notes.
      $r_5 = 3 \bmod 2 = 1$.

      vi. What are a_6, b_6, q_6, and r_6?
      $a_6 =$
      Review Euclid's algorithm in the notes.
      $a_6 = b_5 = 2$.
      $b_6 =$
      Review Euclid's algorithm in the notes.
      $b_6 = r_5 = 1$.
      $q_6 =$
      Review Euclid's algorithm in the notes.
      $q_6 = \lfloor \frac{2}{1} \rfloor = 2$.
      $r_6 =$
      Review Euclid's algorithm in the notes.
      $r_6 = 2 \bmod 1 = 0$.

      vii. What is the greatest common divisor of 13 and 21?
      $gcd(13, 21) =$
      Review Euclid's algorithm in the notes.
      $gcd(31, 21) = gcd(1, 0) = 1$.

   (d) Now, follow the process demonstrated above to find x, y such that $13x + 21y = gcd(13, 21)$.

      i. We start by taking $r_5 = a_5 - b_5 \times q_5$. We then substitute some expression for b_5, and after simplifying end up with the expression $r_5 = \alpha \times b_4 + \beta \times a_4$. What are α, β?
      $\alpha =$
      Review Euclid's algorithm in the notes.
      $\alpha = 2$. For full solution, see solution to β.
      $\beta =$
      Review Euclid's algorithm in the notes.
      $\beta = -1$. We know

      $$r_5 = a_5 - b_5 \times q_5 \implies 1 = 3 - 2 \times 1$$

      Now we express $b_5 = 2$ in terms of $b_4 = 3$ and $a_4 = 5$:

      $$1 = 3 - (5 - 3) \times 1$$

      Combining like terms, we get

      $$1 = 3 \times 2 + 5 \times (-1)$$

      giving $\alpha = 2$ and $\beta = -1$.

      ii. We then substitute some expression for $b_4 = r_3$, and after simplifying we get $r_5 = \alpha \times b_3 + \beta \times a_3$. What are α, β?
      $\alpha =$
      Review Euclid's algorithm in the notes.
      $\alpha = -3$. For full solution, see solution to β.
      $\beta =$
      Review Euclid's algorithm in the notes.
      $\beta = 2$. We start with the expression we derived in the last step:

      $$1 = 3 \times 2 + 5 \times (-1)$$

      Now we express $b_4 = 3$ in terms of $b_3 = 5$ and $a_3 = 8$:

      $$1 = (8 - 5) \times 2 + 5 \times (-1)$$

      Combining like terms,

      $$1 = 5 \times (-3) + 8 \times 2$$

      giving $\alpha = -3$ and $\beta = 2$.

      iii. We then substitute some expression for $b_3 = r_2$, and after simplifying we get $r_5 = \alpha \times b_2 + \beta \times a_2$. What are α, β?
      $\alpha =$
      Review Euclid's algorithm in the notes.
      $\alpha = 5$. For full solution, see solution to β.
      $\beta =$
      Review Euclid's algorithm in the notes.
      $\beta = -3$. We start with the expression we found in the last step:

      $$1 = 5 \times (-3) + 8 \times 2$$

      Now we express $b_3 = 5$ in terms of $b_2 = 8$ and $a_2 = 13$:

      $$1 = (13 - 8) \times (-3) + 8 \times 2$$

      Combining like terms, we get

      $$1 = 8 \times 5 + 13 \times (-3)$$

      giving $\alpha = 5$ and $\beta = -3$.

      iv. We finally substitute some expression for $b_2 = r_1$, and after simplifying we get $r_5 = \alpha \times b_1 + \beta \times a_1$. What are α, β?
      $\alpha =$
      Review Euclid's algorithm in the notes.
      $\alpha = -8$. For full solution, see solution to β.
      $\beta =$
      Review Euclid's algorithm in the notes.
      $\beta = 5$. We start with the expression we derived in the last step:

      $$1 = 8 \times 5 + 13 \times (-3)$$

      We now express $b_2 = 8$ in terms of $b_1 = 13$ and $a_1 = 22$:

      $$1 = (22 - 13) \times 5 + 13 \times (-3)$$

      Combining like terms, we get

      $$1 = 13 \times (-8) + 22 \times 5$$

      giving $\alpha = -8$ and $\beta = 5$.

      v. What are x, y?
      $x =$
      Review Euclid's algorithm in the notes.
      $x = \alpha = -8$.
      $y =$
      Review Euclid's algorithm in the notes.
      $y = \beta = 5$.