Abstract algebra Exam 1

Question 1

Let $a = 6409$ and $b = 3536$.
Using the Euclidean algorithm, find the greatest common divisor (a, b) of a and b and express (a, b) as a linear combination of a and b with integer coefficients.
Use your results to factor a and b as products of primes.

The Euclidean algorithm for (a, b) goes as follows:

$$6409 = 1(3536) + 2873,$$

$$3536 = 1(2873) + 663,$$

$$2873 = 2652 + 221 = 4(663) + 221,$$

$$663 = 3(221) + 0.$$

So the required g.c.d., which is the last non-zero remainder, is 221.

Putting $a = 6409$, 3536, $c = 2873$, $d = 663$ and $e = 221$, we have:

$$a = b + c, \text{ so } c = a - b,$$

$$b = c + d, \text{ so } d = b - c,$$

$$c = 4d + e, \text{ so } e = c - 4d,$$

$$d = 3e.$$

Then we have:

$$e = c - 4d = c - 4(b - c) = 5c - 4b = 5(a - b) - 4b = 5a - 9b.$$

Check:

$$5a - 9b = 5(6409) - 9(3536) = 32045 - 31824 = 221.$$

Now we have:

$$221 = 13(17).$$

Dividing a and b first by 17 and then by 13, we get the required prime factorizations:

$$a = 6409 = 13(493) = (13)(17)(29),$$

$$b = 3536 = 13(272) = (13)(17)(16) = 2^4(13)(17).$$

Question 2

For each of the following equations, determine, with proof, if it is solvable and for each solvable equation find all integer solutions; if an equation is not solvable prove that it is not solvable:

- $4x = 3 \mod 13$.

  This is solvable, with a unique solution, since we have:
  $(4, 13) = (4, 13 - 3(4)) = (4, 1) = 1 = (4 - 4(1), 1) = (0, 1) = 1$.
  We have working $\mod 13$:

  $$x = \frac{3}{4} = \frac{3+13}{4} = \frac{16}{4} = 4.$$

  Check: $4(4) = 16 = 13 + 3 = 3 \mod 13$.

- $16x = 1 \mod 23$.

  This is solvable, with a unique solution, since we have:
  $(16, 23) = (16, 23 - 2(16)) = (16, -5) = (16, 5) = (16 - 3(5), 5) = (1, 5) = (1, 5 - 5(1)) = (1, 0) = 1$.
  We have working $\mod 23$:

  $$x = \frac{1}{16} = \frac{1+23}{16} = \frac{24}{16} = \frac{3}{2} = \frac{3+23}{2} = \frac{26}{2} = 13.$$

  Check: $16(13) = 208 = 1 + 207 = 1 + 23(9) = 1 \mod 23$.

- $40x = 81 \mod 15$.

  We have:

  $(40, 15) = (40-3(15), 15) = (-5, 15) = (5, 15) = (5, 15-3(5)) = (5, 0) = 5$.

  But $81 = 80 + 1 = 16(5) + 1$ so 81 is not divisible by 5, so there are no solutions to this equation, since we know that the equation $ax = c \mod b$ has solutions if and only if (a, b) divides c.
  Here $a = 40, b = 15, (a, b) = 5$ and $c = 81$.

Question 3

For each of the following polynomial equations, determine with proof if it is solvable and for each solvable equation find all integer solutions; if an equation is not solvable prove that it is not solvable: also use your results to factor the given polynomial, if possible.

- $f(x) = x^2 + x + 1 = 0 \mod 5$. We have, working $\mod 5$:

  $f(0) = 0+0+1 = 1, \quad f(1) = 1+1+1 = 3, \quad f(2) = 4+2+1 = 7 = 5+2 = 2,$

  $f(3) = 9+3+1 = 13 = 10+3 = 2(5)+3 = 3, \quad f(4) = 16+4+1 = 21 = 20+1 = 4(5)+1 = 1.$

  Since we have tested all possible values, this equation has no solutions $\mod 5$.

  Alternatively, we might note that if $x^2 + x + 1 = 0$, we have $x^3 - 1 = (x-1)(x^2+x+1) = 0$, so $x^3 = 1$.
  Modulo 5, the cubes are:

  $$0^3 = 0, \quad 1^3 = 1, \quad 2^3 = 8 = 5 + 3 = 3,$$

  $$3^3 = 27 = 25 + 2 = 5(5) + 2 = 2, \quad 4^3 = 64 = 60 + 4 = 5(12) + 4 = 4.$$

  So the only solution of $x^3 = 1 \mod 5$ is $x = 1$.
  But this is not a solution of $f(x) = 0$, since $f(1) = 1 + 1 + 1 = 3 \mod 5$.
  So there are no solutions to $f(x) = 0$.

  Alternatively we use the quadratic formula, working mod 5:

  $$x = \frac{1}{2}\left(-1 \pm \sqrt{1-4}\right) = \frac{1}{2}\left(-1 \pm \sqrt{-3}\right) = 3\left(-1 \pm \sqrt{3}\right).$$

  But the squares mod 5 are:

  $0^2 = 0, \quad 1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 9 = 5+4 = 4, \quad 4^2 = 16 = 15+1 = 3(5)+1 = 1.$

  Since 3 is not a square mod 5, there are no solutions.

  Equivalently, we can complete the square:

  $x^2+x+1 = x^2-4x+1 = (x^2-4x+4)-3 = (x-2)^2-3, \quad (x-2)^2 = 3.$

  Since, as shown above, 3 is not a square, mod 5, there are no solutions.

- $g(x) = x^2 + 5x + 3 = 0 \mod 13$.

  We use the quadratic formula, working mod 13:

  $$x = \frac{1}{2}\left(-5 \pm \sqrt{25-12}\right) = \frac{1}{2}\left(-5 \pm \sqrt{13}\right) = \frac{1}{2}\left(-5 \pm \sqrt{0}\right) = \frac{-5}{2} = \frac{-5+13}{2} = \frac{8}{2} = 4.$$

  There is only one solution, $x = 4$, so the quadratic must be a perfect square:

  $$g(x) = (x-4)^2.$$

  Check:

  $$(x-4)^2-(x^2+5x+3) = x^2-8x+16-x^2-5x-3 = -13x+13 = 13(1-x) = 0, \mod 13.$$

  Alternatively we complete the square, working mod 13:

  $$x^2+5x+3 = x^2-8x+3 = x^2-8x+16-16+3 = (x-4)^2-13 = (x-4)^2.$$

- $h(x) = x^3 - 1 = 0 \mod 7$.

  Clearly $x = 1$ is a solution so we factor:

  $$h(x) = (x-1)(x^2+x+1) = (x-1)m(x), \text{ where } m(x) = x^2+x+1.$$

  We use the quadratic formula for the roots of $m(x) = 0$, working mod 7:

  $$x = \frac{1}{2}\left(-1 \pm \sqrt{1-4}\right) = \frac{8}{2}\left(-1 \pm \sqrt{-3}\right) = 4\left(-1 \pm \sqrt{4}\right)$$
  $$= 4\left(-1 \pm 2\right) = -4 \pm 8 = 3 \pm 1 = 4 \text{ or } 2.$$

  So we have the roots 1, 2 and 4 for the equation $h(x) = 0$ and the factorization:

  $$h(x) = x^3 - 1 = (x-1)(x-2)(x-4).$$

  Check, mod 7 we have:

  $$(x-1)(x-2)(x-4) = (x^2-3x+2)(x-4) = x^3-3x^2+2x-4x^2+12x-8$$
  $$= x^3 - 7x^2 + 14x - 8 = x^3 - 1 + 7(-x^2+2x-1) = x^3 - 1.$$

Question 4

Given positive integers a, b, c and d, put $(a, b) = p$ and $(c, d) = q$.
Prove that pq divides (ac, bd).
Give an example to show that (ac, bd) can be equal to pq and another example to show that (ac, bd) can be more than pq.

Since $p = (a, b)$ we have $a = pr$ and $b = ps$, for some integers r and s.
Since $q = (c, bd$ we have $c = qt$ and $d = qu$, for some integers t and u.
These relations give:

$$ac = (pq)(rt), \quad bd = pq(su).$$

So, since rt and su are integers, we see that pq is a common divisor of ac and bd, so by a theorem proved in class, the number pq must divide the g.c.d. of ac and bd, so pq divides (ac, bd), as required.

If $a = b = c = d = 1$, then $p = 1$, $q = 1$ and $(ac, bd) = (1, 1) = 1$, so $pq = (ac, bd)$.

If $a = d = 1$ and $b = c = 2$, then $p = 1$, $q = 1$ and $(ac, bd) = (2, 2) = 2$, so $pq < (ac, bd)$.

Question 5

- Find all integer solutions x of the following system:

$$37x = 7 \mod 13$$
$$9x = 5 \mod 11$$

- Also find the number of integer solutions x of the system with $|x| < 1000$.

The Chinese Remainder Theorem applies, since we have:

$$(11, 13) = (11, 13 - 11) = (11, 2) = (11 - (5)(2), 2)$$
$$= (1, 2) = (1, 2 - 2(1)) = (1, 0) = 1,$$

$(37, 13) = (37-3(13), 13) = (-2, 13) = (2, 13) = (2, 13-6(2)) = (2, 1) = (2-2(1), 1) = (0, 1) = 1,$

$(9, 11) = (9-11, 11) = (-2, 11) = (2, 11) = (2, 11-5(2)) = (2, 1) = (2-2(1), 1) = (0, 1) = 1.$

- The first subproblem is:

$$37x_1 = 7 \mod 13, \quad x_1 = 0 \mod 11,$$

So $x_1 = 11s$, with s an integer and we need:

$$37(11)(s) = 7 \mod 13,$$
$$s = \frac{7}{(37)(11)} = \frac{7}{(37 - 3(13))(11 - 13)} = \frac{7}{(-2)(-2)} = \frac{7 + 13}{4} = 5 \mod 13.$$
$$x_1 = 11s = 55.$$

- The second subproblem is:

$$37x_2 = 0 \mod 13, \quad 9x_2 = 5 \mod 11,$$

So $x_2 = 13t$, with t an integer and we need:

$$9(13)(t) = 5 \mod 11,$$
$$t = \frac{5}{(9)(13)} = \frac{5}{(9 - (11))(13 - 11)} = \frac{5}{(-2)(2)} = \frac{5 + 11}{-4} = -4 = 7 \mod 11.$$
$$x_2 = 13t = 91.$$

Then by the Chinese Remainder Theorem, the required solution is:

$$x = x_1 + x_2 = 55 + 91 = 146 \mod (11)(13)$$

$$= 146 \mod 143 = (146 - 143) \mod 143 = 3 \mod 143.$$

Check $x = 3$ should be a solution:

$$37(3) - 7 = 111 - 7 = 104 = 8(13) = 0 \mod 13,$$

$$9(3) - 5 = 27 - 5 = 22 = 2(11) = 0 \mod 11.$$

So the general solution is:

$$x = 3 + 143z, \text{ where } z \in \mathbb{Z}.$$

Finally we need:

$$|3 + 143z| < 1000,$$

$$-1000 < 3 + 143z < 1000,$$

$$-1003 < 143z < 997.$$

Now we have $6(143) = 852$, $7(143) = 1001$ and $8(143) = 1144$, so we have:

$$-8(143) < -1003 < -7(143), \quad , 6(143) < 997 < 7(143).$$

So we need $-7 \leq z \leq 6$.
So there are exactly fourteen solutions given by $-1001 + 3 + 143y = -998 + 143y$, for y from 0 to 13.
Specifically the set of solutions is:

$$\{-998, -855, -712, -569, -426, -283, -140, 3, 146, 289, 432, 575, 718, 861\}.$$

Alternatively, we first solve one equation and then insert in the other:

$$37x = 7 \mod 13,$$

$$x = \frac{7}{37} = \frac{7 - 13}{37 - 3(13)} = \frac{-6}{-2} = 3 \mod 13.$$

So $x = 3 + 13u$, for some integer u.
Putting this in the second equation, we need:

$$0 = 9x - 5 \mod 11 = 9(3 + 13u) - 5 \mod 11$$

$$= 22 + 117u = 22 + 117u - 11(2 + 10u) \mod 11 = 7u \mod 11.$$

So $u = 0 \mod 11$, so $u = 11z$, for z an integer and the solution is $x = 3 + 13(11)z = 3 + 143z$, for z integral, as before.

Question 6

Consider the following addition and multiplication tables for a ring:

$+$	$\underline{x}$	$\underline{z}$	$\underline{y}$	$\underline{w}$
x	z	x	w	y
z	x	z	y	w
y	w	y	x	z
w	y	w	z	x

$\cdot$	$\underline{x}$	$\underline{z}$	$\underline{y}$	$\underline{w}$
x	z	z	x	x
z	z	z	z	z
y	x	z	y	w
w	x	z	w	y

Show that this ring is really the ring $\mathbb{Z}_4$ in disguise.
Hint: begin by identifying the additive and multiplicative identities.

Looking at the addition and multiplication tables we see that z behaves as an additive identity, since $z+u=u+z=z$ and $zu=uz=z$ for all u.
Looking at the multiplication table we see that y behaves as multiplicative identity, since $yu=uy=u$ for all u.
So we put $z=0$ and $y=1$. Then from the addition table, we see that:

$$2=1+1=y+y=x, \quad 3=1+2=y+x=w.$$

Substituting $w=3$, $x=2$, $y=1$ and $z=0$, the tables now read:

$+$	$\underline{2}$	$\underline{0}$	$\underline{1}$	$\underline{3}$
2	0	2	3	1
0	2	0	1	3
1	3	1	2	0
3	1	3	0	2

$\cdot$	$\underline{2}$	$\underline{0}$	$\underline{1}$	$\underline{3}$
2	0	0	2	2
0	0	0	0	0
1	2	0	1	3
3	2	0	3	1

By inspection these are the addition and multiplication tables for $\mathbb{Z}_4$, so we are done.

Question 7

For x in $\mathbb{Z}$ put $f(x) = 5x \mod 20$.
Prove that the map f is a ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_{20}$.
Also determine the image of the map f and its kernel. For any integers x and y, we have, working mod 20:

$$f(x+y) - (f(x) + f(y)) = 5(x+y) - (5x + 5y) = 0,$$

$$f(xy) - (f(x)f(y)) = 5(xy) - (5x)(5y) = 5xy - 25xy = 20(-xy) = 0.$$

These formulas prove that f is a homomorphism of rings.
The kernel is all $x \in \mathbb{Z}$ with $f(x) = 0$, so is all $x = 0$ with $5x = 0 \mod 20$, so $5x = 20k$, for some integer k, or $x = 4k$.
So the kernel is all integer mutliples of 4.
Check: $f(4k) = 5(4k) = 20k = 0, \mod 20$.

Finally the image of f is all numbers of the form $5u \mod 20$, with u an integer.
But if $u \to u + 4$, we see that $f(u+4) = f(u) + f(4) = f(u) + 0 = f(u)$.
So only $u = 0, 1, 2, 3$ can give distinct images.
So the image of f in $\mathbb{Z}_{20}$ is the set:

$$\{f(0), f(1), f(2), f(3)\} = \{0, 5, 10, 15\} \subset \mathbb{Z}_{20}.$$

Question 8

Let $\mathbb{A} = \mathbb{Z}_2 \times \mathbb{Z}_6$, $\mathbb{B} = \mathbb{Z}_3 \times \mathbb{Z}_4$ and $\mathbb{C} = \mathbb{Z}_{12}$.
Decide, with proof, which of the rings $\mathbb{A}$, $\mathbb{B}$, or $\mathbb{C}$ are isomorphic to each other.

In $\mathbb{C} = \mathbb{Z}_{12}$ the only solutions to the equation $6x = 0$ are the six even numbers, mod 12, since we need $6x = 12k$, for k an integer, so $x = 2k$.

In $\mathbb{A}$, if $x = (p, q) \in \mathbb{A}$, with $p \in \mathbb{Z}_2$ and $q \in \mathbb{Z}_6$, then $6x = (6p, 6q) = (0, 0)$, so there are twelve solutions of the equation $6x = 0$, namely every element of $\mathbb{A}$.
So $\mathbb{A}$ and $\mathbb{C}$ are not isomorphic.
Finally consider the map: $\mathbb{C} \to \mathbb{B}$, defined for any $x \in \mathbb{Z}_{12}$.

$$g(x) = (x \mod 3, x \mod 4).$$

Since $12k = 0 \mod 3$ and $12k = 0 \mod 4$, for any integer k, this map is well-defined.
If $g(x) = g(y)$, then 3 divides $x - y$ and 4 divides $x - y$, so 12 divides $x - y$, so $x = y \mod 12$, so g is one-to-one.
Since both $\mathbb{B}$ and $\mathbb{C}$ have twelve elements, by the pigeonhole principle, g is bijective.
Finally we have, for any integers x and y mod 12:

$$g(x+y)-(g(x)+g(y)) = (x+y, x+y)-((x, x)+(y, y)) = (x+y, x+y)-(x+y, x+y) = (0, 0),$$

$$g(xy) - (g(x)g(y)) = (xy, xy) - (x, x)(y, y) = (xy - xy, xy - xy) = (0, 0).$$

So g is a ring homomorphism, and is bijective, so is an isomorphism.
If $\mathbb{A}$ and $\mathbb{B}$ were isomorphic, then all three rings would be isomorphic, which is false.
So only $\mathbb{B}$ and $\mathbb{C}$ are isomorphic amongst the given rings and we are done.