Problem Set 7 Solutions

ECS 20 (Winter 2019)

Patrice Koehl
koehl@cs.ucdavis.edu

February 25, 2019

Exercise 1

a) Let a be a natural number strictly greater than 1. Show that $\gcd(a, a-1) = 1$.

b) Use the result of part a) to solve the Diophantine equation $a + 3b = ab$ where a and b are two positive integers.

a) We do a proof by contradiction. Let a be a natural number strictly greater than 1 and let us suppose that $gcd(a, a-1) = k$ with $k > 1$.
Then there exist two positive integers m and n, such that $a = mk$ and $a - 1 = nk$.
Then

$$a - (a-1) = mk - nk = (m-n)k$$

and at the same time

$$a - (a-1) = 1$$

Therefore $(m-n)k = 1$, i.e. k is a divisor of 1, but $k > 1$ (our hypothesis): we have reached a contradiction. Therefore, $gcd(a, a-1) = 1$

b) We want to solve the equation $a + 3b = ab$, were a and b are positive integers.
We look at three cases:

i) $b = 0$. The equation becomes $a = 0$.

ii) $b = 1$. The equation becomes $a + 2 = a$, which does not have a solution

ii) $b > 1$.
From $a + 3b = ab$, we get $3b = ab - a = a(b-1)$. Therefore $b - 1$ divides $3b$. From part a), we know that $gcd(b, b-1) = 1$. According to Gauss's theorem, we have $(b-1)/3$, meaning that $b = 2$ or $b = 4$
Replacing in the original equation, we get $a = 6$ in the first case, and $a = 4$ in the second case.

The set of solutions is therefore $\{(0,0), (6,2), (4,4)\}$.

Exercise 2

a) Let a, b, and c be three integers. Show that the equation $ax + by = c$ has at least one solution if and only if $\gcd(a, b)/c$.

b) A group of men and women spent \$100 in a store. Knowing that each man spent \$8, and each woman spent \$5, can you find how many men and how many women are in the group?

a) Let a, b, and c be three integers. We need to prove a biconditional $p \leftrightarrow q$, where p and q are the two propositions:

   p: The equation $ax + by = c$ has at least one solution (x_1, y_1)

   and

   $q : \gcd(a, b)/c$

   Proving $p \leftrightarrow q$ is equivalent to proving $p \rightarrow q$ and $q \rightarrow p$. We will use direct proofs for both implications.

   a) $p \rightarrow q$
   Hypothesis: p is true, namely, the equation $ax+by = c$ has at least one solution (x_1, y_1). Therefore $ax_1 + by_1 = c$.
   Let $g = \gcd(a, b)$: g divides a and g divides b. Therefore, there exists two integers k and l such that $a = gk$ and $b = gl$. Replacing in the equation above, we get:
   $gkx_1 + gly_1 = c$
   which we rewrite as:
   $g(kx_1 + ly_1) = c$
   Since $kx_1 + ly_1$ is an integer, g divides c, namely q is true.

   b) $q \rightarrow p$
   Hypothesis: q is true, namely $\gcd(a, b)/c$.
   Let $g = \gcd(a, b)$. Since g/c, there exists an integer m such that $c = mg$.
   Also, based on Bezout's identity, there exists two integers k and l such that $g = ka + lb$.
   Multiplying this equation by m, we get $mg = kma + lmb$, i.e. $c = kma + lmb$. We have therefore found a pair (x_1, y_1) with $x_1 = km$ and $y_1 = lm$ such that $ax_1 + by_1 = c$: p is true.

   In conclusion, $p \leftrightarrow q$ ia true.

b) Let n be the number of men, and let m be the number of women. From the text of the problem, we know that

$$7n + 6m = 100$$

   We notice first that $\gcd(7, 6) = 1$; since 1 divides 100, from a) we deduce that there is a solution to the problem.

Since $\gcd(7, 6) = 1$, according to Bezout we know that there are two integers u_0 and v_0 such that:

$$7u + 6v = 1$$

We can choose for example $u_0 = 1$ and $v_0 = -1$. Multiplying the equation above by 100, we get:

$$7(100u_0) + 6(100v_0) = 100$$

whose solutions are therefore $n_0 = 100u_0 = 100$ and $m_0 = 100v_0 = -100$. All solutions are of the form $n = n_0 - 6k = 100 - 6k$ and $m = m_0 + 7k = -100 + 7k$ where k is an integer, and $n \geq 0$ and $m \geq 0$. Since $n \geq 0$, $k \leq 16$. Since $m \geq 0$, $k \geq 15$. There are therefore 2 solutions for $k = 15$ and 16: $S = \{(10, 5), (4, 12)\}$.

Exercise 3

a) Let a and b be two natural numbers. Show that if $\gcd(a, b) = 1$ then $\gcd(a, b^2) = 1$.

Let a and b be two natural numbers such that $\gcd(a, b) = 1$. According to Bezout's identity, there exist two integers k and l such that $ak + bl = 1$. Multiplying by b, we get $abk + b^2 l = b$.

Let $g = \gcd(a, b^2)$. By definition of gcd, there exists two integers u and v such that $a = ug$ and $b^2 = vg$. Replacing in the equation above, we get $gubk + gvl = b$. Hence, g divides b. Since g also divides a, g is a common divisor of a and b. Since $\gcd(a, b) = 1$, the only possibility is $g = 1$, therefore $\gcd(a, b^2) = 1$, which concludes the proof.

b) Let a and b be two natural numbers. Show that if $\gcd(a, b) = 1$ then $\gcd(a^2, b^2) = 1$.

Let a and b be two natural numbers such that $\gcd(a, b) = 1$. According to question a), we know that $\gcd(a, b^2) = 1$, which we can rewrite as $\gcd(b^2, a)$. Applying again the property of a) to b^2 and a, we get $\gcd(b^2, a^2) = 1$, therefore $\gcd(a^2, b^2) = 1$.

Exercise 4

Let n be a natural number such that the remainder of the division of 5218 by n is 10, and the remainder of the division of 2543 by n is 11. What is n?

We note first that n divides $5218 - 10 = 5208$ and n divides $2543 - 11 = 2532$. Therefore n divides the $\gcd(5208, 2532) = 3 \times 2^2 = 12$. Therefore $n = 2, 3, 4, 6, or 12$ (we can exclude 1!). We can exclude $2, 3, 4$ and 6 as 10 and 11 should both be smaller than n. We notice that $5218 = 12*434+10$, and $2543 = 211 \times 12 + 11$. The answer is $n = 12$.

Exercise 5

Find all $(x, y) \in \mathbb{N}^2$ that satisfy the system of equations:

$$\begin{cases} x^2 - y^2 = 2340 \\ \gcd(x, y) = 6 \end{cases}$$

Let x and y be two natural number and let $g = \gcd(x, y)$. By definition of gcd, there exists two integers u and v such that $x = gu$ and $y = gv$. Since $g = 6$, $x = 6u$ and $y = 6v$. Replacing in the first equation of the system, we get:

$$x^2 - y^2 = 36(u^2 - v^2) = 2340$$

Therefore,

$$(u - v)(u + v) = 65$$

Since $65 = 1 \times 5 \times 13$, the possible solutions for $u - v$ and $u + v$ are $S = \{(1, 65), (5, 13), (13, 5), (65, 1)\}$. Let us look at all 4 cases:

a)

$$\begin{cases} u - v = 1 \\ u + v = 65 \end{cases}$$

Then $u = 33$ and $v = 32$, i.e. $x = 198$ and $y = 192$.

b)

$$\begin{cases} u - v = 5 \\ u + v = 13 \end{cases}$$

Then $u = 9$ and $v = 4$, i.e. $x = 54$ and $y = 24$.

c)

$$\begin{cases} u - v = 13 \\ u + v = 5 \end{cases}$$

Then $u = 9$ and $v = -4$, i.e. $x = 54$ and $y = -24$. This is not a solution as x and y need to be natural numbers.

d)

$$\begin{cases} u - v = 65 \\ u + v = 1 \end{cases}$$

Then $u = 33$ and $v = -32$, i.e. $x = 198$ and $y = -192$. This is not a solution as x and y need to be natural numbers.

.

Therefore the only solutions are $S = \{(198, 192), (54, 24)\}$.

Exercise 6

Let n be a natural number. We define $A = n - 2$ and $B = n^2 - 6n + 13$. Show that $\gcd(A, B) = \gcd(A, 5)$.

Let us define $g1 = \gcd(A, B)$ and $g2 = \gcd(A, 5)$. We will show that $g1 \leq g2$ and $g2 \leq g1$.

a) Let us show that $g1 \leq g2$.

   We first notice that by definition, $g1/A$ and $g1/B$. Therefore, $g1$ divides any combinations of A and B. Now let us notice that:

$$A^2 = n^2 - 4n + 4$$

   Therefore

$$B = A^2 - 2n + 9 = A^2 - 2A + 5$$

   As $g1$ divides $B - A^2 + 2A$, $g1$ divides 5. Therefore $g1$ divides A and $g1$ divides 5, $g1 \leq g2$.

a) Let us show that $g2 \leq g1$.

   We first notice that by definition, $g2/A$ and $g2/5$. Since $B = A^2 - 2A + 5$, and $g2$ divides $A^2 - 2A + 5$, $g2$ divides B. Therefore $g2$ divides A and $g2$ divides B, $g2 \leq g1$.

In conclusion, $g1 = \gcd(A, B) = g2 = \gcd(A, 5)$.

Exercise 7

Let a and b be two natural numbers. Solve the equations $a^2 - b^2 = 13$.

We can rewrite the equation as

$$(a - b)(a + b) = 13$$

The solutions for $(a + b)$ and $(a - b)$ are therefore $S = \{(1, 13), (13, 1)\}$. Let us look at all 2 cases:

a)

$$\begin{cases} a - b = 1 \\ a + b = 13 \end{cases}$$

   Then $a = 7$ and $b = 6$.

b)

$$\begin{cases} a - b = 13 \\ a + b = 1 \end{cases}$$

   Then $a = 7$ and $b = -6$. Since b needs to be a natural number, this is not a solution.

The only solution is (7,6).

Extra Credit

Let a and b be two natural numbers. Solve $\gcd(a,b)+\text{lcm}(a,b)=b+9$.

We want to solve $\gcd(a,b)+\text{lcm}(a,b)=b+9$, where a and b are two natural numbers (i.e. positive non zero integers).
As written, the equation looks very complicated. Let us transform it to make it more tractable. Most terms in the equation can be written as multiples of $g=\gcd(a,b)$:
Since g is a divisor of a and b, there exists non-zero integers m and n such $a=mg$ and $b=ng$. We also know that $g.\text{lcm}(a,b)=ab$, then $g.\text{lcm}(a,b)=g.g.mn$ and therefore $\text{lcm}(a,b)=gmn$.
Replacing in the equation, we get: $g+gmn=gn+9$, which can be rewritten as $g(1+mn-n)=9$.

This shows that g divides 9. There are 3 possibilities for g: $g=1$, or $g=3$ or $g=9$:

1) $g=1$. The equation becomes $lcm(a,b)=b+8$, with $lcm(a,b)=ab$. Then $ab=b+8$, or $b(a-1)=8$. Then b is a divisor of 8, i.e. $b=1, b=2, b=4$ or $b=8$.

   - $b=1$: $a-1=8$ then $a=9$. $(9,1)$ is one solution of the equation.
   - $b=2$: $a-1=4$ then $a=5$. $(5,2)$ is another solution of the equation.
   - $b=4$: $a-1=2$ then $a=3$. $(3,4)$ is another solution of the equation.
   - $b=8$: $a-1=1$ then $a=2$. This would imply $gcd(a,b)=2$, which is in contradiction with $g=1$. This case does not yield any new solutions .

2) $g=3$. The equation becomes $\text{lcm}(a,b)=b+6$. $\text{lcm}(a,b)$ is a multiple of b: $\text{lcm}(a,b)=mb$, hence $b(m-1)=6$. Hence b divides 6, i.e. $b=1, b=2, b=3$ or $b=6$. Since $b\geq g$, we cannot have in this case $b=1$ or $b=2$. We need to check two cases:

   - If $b=3$, then the equation becomes $3+\text{lcm}(a,b)=3+9$, i.e. $\text{lcm}(a,b)=9$. Since $\text{lcm}(a,b)$ is a multiple of a, we find that a divides 9. We also know that a is a multiple of 3, as $g=3$ is a divisor of a. Then $a=3$ or $a=9$. We cannot have $a=3$ (since we would have $\text{lcm}(a,b)=3$), hence $a=9$. $(9,3)$ is another solution of the equation.
   - If $b=6$, the equation becomes $3+\text{lcm}(a,b)=6+9$, hence $\text{lcm}(a,b)=12$. As above, a is a multiple of 3 and a divides 12. If $a=3$ or $a=6$, the we would have $\text{lcm}(a,b)=6$ NO. If $a=12$, then $\gcd(a,b)=6$: NO. In this case, we do not have new solutions.

3) $g=9$. The equation becomes $\text{lcm}(a,b)=b$. Since $\text{lcm}(a,b).\gcd(a,b)=ab$, we get $9b=ab$, i.e. $a=9$ (we do not have to consider b=0, as we look for natural numbers). Since $\text{lcm}(a,b)=b$ is a multiple of a, there exists $k>0$ such that $b=9k$. All values of $k>0$ are possible.

In conclusion, the solutions are: $\{(9,1),(5,2),(3,4),(9,3),(9,9k)\}$ where all values of $(k>0)$ are possible.