Problem Set 7 Solutions

ECS 20 (Fall 2016)

Patrice Koehl
koehl@cs.ucdavis.edu

October 31, 2016

Exercise 1

e) -2002 divided by 89: Quotient = -23; Remainder = 45; Check : -23*89+45 = -2002.

f) 0 divided by 19: Quotient = 0; Remainder = 0; Check : 0*17+0 = 0.

g) 1,234,567 divided by 101: Quotient = 12223; Remainder = 44; Check : 12223*101+44 = 1,234,567.

h) -100 divided by 103: Quotient = -1; Remainder = 3; Check : -1*103+3 = -100.

Exercise 2

a) Let us suppose that $gcd(a, a-1) = k$ where k>1.
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 $a + 2b = 2ab$, were a and b are positive integers.
We look at two cases:

i) $a = 0$. The equation becomes $2b = 0$, therefore $b = 0$.

ii) $a \neq 0$.
From $a + 2b = 2ab$, we get $a = 2ab - 2b = 2b(a - 1)$. Because $a \neq 0$, $b \neq 0$ and $a \neq 1$.
From $a = 2b(a-1)$, we get that $a-1$ divides a. From part a), we know that $gcd(a, a-1) = 1$. Thus, there is only one possibility, $a - 1 = 1$ and therefore $a = 2$.
Replacing in the original equation, we get $2 + 2b = 4b$, hence $b = 1$.

The set of solutions is therefore $\{(0, 0), (2, 1)\}$.

Exercise 3

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, $p \leftrightarrow q$.

Exercise 4

Let a, b and n be three integers such that $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$.

Since $\gcd(a, n) = 1$, according to Bezout's identity, there exists two integers k and l such that $ka + ln = 1$. Multiplying by b, we get $kab + lnb = b$.

Let $g = \gcd(ab, n)$. There exist two integers u and v such that $ab = ug$ and $n = vg$. Replacing in the equation above, we get $kgu + lvgb = b$, or $g(ku + lvb) = b$. Hence, g divides b. Since g also divides n, g is a common divisor of b and n. Since $\gcd(b, n) = 1$, the only possibility is $g = 1$, and therefore $\gcd(ab, n) = 1$, which concludes the proof.

Exercise 5

We consider the equation $3x^2 + 5y^2 = 19$. Let us follow the hint:
Since $5 \equiv 0 (\text{mod } 5)$, $5y^2 \equiv 0 (\text{mod } 5)$. Hence $3x^2 + 5y^2 \equiv 3x^2 (\text{mod } 5)$.

Let us write $x = 5q+r$, with $0 \leq r \leq 4$. Then $x^2 = 25q^2+10q+r^2$, and therefore $x^2 \equiv r^2 (\text{mod } 5)$, and $3x^2 \equiv 3r^2 (\text{mod } 5)$. For $r = 0, 1, 2, 3, 4$, we get $3x^2 \equiv 0, 3, 2, 2, 3 (\text{mod } 5)$, respectively.
On the other hand, $19 \equiv 4 (\text{mod } 5)$. Therefore we cannot have $3x^2 + 5y^2 \equiv 19 (\text{mod } 5)$, and the equation does not have any solution.

Exercise 6

We can divide all integers larger than 3 into three sets: those that have the form $3k$, those that have the form $3k + 1$ and those that have the form $3k + 2$, where $k \in \mathbb{Z}$.

a) If n is in form of $3k$, then it is not a prime as it is a multiple of 3.

b) If n is in form of $3k + 1$, then $2n + 1 = 6k + 2 + 1 = 3(2k + 1)$, is not a prime, as it is a multiple of 3.

c) If n is in form of $3k + 2$, then $4n + 1 = 12k + 9 = 3(4k + 3)$, is not a prime, as it is a multiple of 3.

Therefore, if n is greater than 3, n, $2n + 1$ and $4n + 1$ cannot all be prime.

Exercise 7

The three primes 3, 5, and 7 verify the property.

Exercise 8

We need to prove an implication of the form $p \rightarrow q$, where:
p: n is a positive integer such that the sum of its divisors is $n + 1$
q: n is prime
We will use an indirect proof, namely we will show that $\neg q \rightarrow \neg p$.

Hypothesis: $\neg q$ is true, i.e. n is not prime.
As n is not a prime, there is at least one positive integer m other than 1 and n itself that divides n. Therefore, the sum of all divisors is $S > 1 + n + m > n + 1$. Therefore $S \neq n + 1$ and $\neg p$ is true.
We can conclude that $\neg q \rightarrow \neg p$ is true, therefore $p \rightarrow q$ is true.

Extra Credit

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 $\text{gcd}(a,b) = 6$: NO. In this case, we do not have new solutions.

3) $g = 9$. The equation becomes $\text{lcm}(a,b) = b$. Since $\text{lcm}(a,b).\,\text{gcd}(a,b) = ab$, 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.