Questions and Solutions for ASSIGNMENT 2, MAT1026: PROOF

Question 1: Use Euclid's algorithm to calculate the highest common factor g of the numbers (89,55), and of the numbers (3132,7200). For the numbers (89,55) find integers x and y such that $g = 55x + 89y$.

Solution:

$89 = 55 \cdot 1 + 34$
$55 = 34 \cdot 1 + 21$
$34 = 21 \cdot 1 + 13$
$21 = 13 \cdot 1 + 8$
$13 = 8 \cdot 1 + 5$
$8 = 5 \cdot 1 + 3$
$5 = 3 \cdot 1 + 2$
$3 = 2 \cdot 1 + 1$
$2 = 1 \cdot 2 + 0$

and so $g = 1$. In order to find x and y we work backward:

$$\begin{aligned} 1 = 3 - 2 &= 3 - (5 - 3) = 2 \cdot 3 - 5 = 2(8 - 5) - 5 = 2 \cdot 8 - 3 \cdot 5 \quad (1) \\ &= 2 \cdot 8 - 3(13 - 8) = 5 \cdot 8 - 3 \cdot 13 = 5(21 - 13) - 3 \cdot 13 \\ &= 5 \cdot 21 - 8 \cdot 13 = 5 \cdot 21 - 8(34 - 21) = \\ &= 13 \cdot 21 - 8 \cdot 34 = 13(55 - 34) - 8 \cdot 34 = \\ &= 13 \cdot 55 - 21 \cdot 34 = 13 \cdot 55 - 21(89 - 55) = \\ &= 34 \cdot 55 - 21 \cdot 89, \end{aligned}$$

so that $y = -21$ and $x = 34$. Remark: So the Fibonacci numbers turn up as the canonical worst case of Euclid's algorithm!

For the numbers 7200 and 3132 we have

$7200 = 3132 \cdot 2 + 936$
$3132 = 936 \cdot 3 + 324$
$936 = 324 \cdot 2 + 288$
$324 = 288 \cdot 1 + 36$
$288 = 36 \cdot 8 + 0$
and so $g = 36$.

Question 2: Given positive integers a, b their product is a multiple of both and therefore they have a *least common multiple* usually denoted by

$l(a,b)$. By denoting by $g(a,b)$ their *highest common factor*, prove that $l(a,b) \cdot g(a,b) = ab$.

Solution: Put $g = g(a,b) = sa + tb$. Since ab/g is a common multiple of a and b $ab/g \geq l(a,b)$. Now let $l(a,b) = ma = nb$. Then

$$snb = sma = m(g - tb) = mg - mtb,$$

and $b|mg$. Then $b \leq mg$ and $ab \leq amg = l(a,b)g$, that is $ab/g \leq l(a,b)$. Hence, $ab = l(a,b)g = l(a,b) \cdot g(a,b)$.

A different (more compact and more beautiful) proof can be obtained by using the fundamental theorem of arithmetic.

Question 3: Find the solutions within the set of natural numbers of the Diophantine equation $11x - 7y = 3$. Does the Diophantine equation $15x - 5y = 2$ possess solutions within the set of natural numbers? Give reasons for your answer.

Solution: We know that the linear Diophantine equation $ax - by = n$ is soluble in natural numbers x, y iff n is a multiple of $g(a,b)$, the greatest common factor of (a,b). Thus in the case of $11x - 7y = 3$ we have that $g(11,7) = 1$ and therefore the equation is always soluble in integers and in particular for the integer 3. The solution set is given by $x = x_0 + n7, y = y_0 + n11$, where n is any integer and x_0, y_0 is any particular solution, for example we can take $x_0 = 6, y_0 = 9$.

Regarding the other equation, namely $15x - 5y = 2$ we can infer immediately that it has not solutions within the set of natural numbers because the number 2 is not a multiple of $g(15,5) = 5$.

Question 4: Show by contraposition that if $a \geq 2$ and $a^m + 1$ is a prime number, with m any natural number, then a must be even.

Solution: Assume $a \geq 2$ is odd, then $a^m + 1$ is even for every natural number m and therefore it cannot be a prime.

Question 5: If $m > 1$ and $a^m - 1$ is prime then show that $a = 2$ and m is prime. [That is $a^m - 1$ has the form $2^p - 1$ with p a prime which is a Mersenne prime].

Solution: If $a > 2$ then

$$a^m - 1 = (a-1)(a^{m-1} + a^{m-2} + \cdots + 1)$$

which is a composite number, hence $a = 2$. On the other hand if m is a composite number, namely $m = rs$ with both $r, s > 1$ then

$$a^m - 1 = [(a^r)^s - 1] = (a^r - 1)[(a^r)^{s-1} + (a^r)^{s-2} + \cdots + 1]$$

which is composite; hence m is prime.