Matematiska Institutionen
KTH

Solutions to homework number 1 to SF2736, fall 2012.

Please, deliver this homework at latest on Tuesday, November 6.

The homework must be delivered individually, and, in general, just hand written notes are accepted. You are free to discuss the problems below with your class mates, but you are not allowed to copy the solution of another student.

1. (0.2p) Find all solutions to the equation $12x = 8$ in the ring Z_{128}.

   Solution. For a solution x, considered as an element in Z, it must hold that $12x = 8 + 128k$, for some integer k. This is an ordinary Diophantine equation, that we solve following the ordinary routines:

   $$12x = 8 + 128k \qquad \Longleftrightarrow \qquad 3x = 2 + 32k,$$

   for some integer k. Easy found solution is $x = -10$ and $k = -1$. If $x = x'$ and $k = k'$ is another solution then

   $$\begin{cases} -10 \cdot 3 &= 2 - 32 \\ x' \cdot 3 &= 2 + k'32 \end{cases} \qquad \Longrightarrow \qquad (x' + 10)3 = (k' + 1)32$$

   from which follows that

   $$x' + 10 = 32n,$$

   for some integer n, as 32 and 3 are coprime. It is easy to verify, simply by substituting this expression in the original equation that all these elements satisfy that equation for every integer n. This gives four distinct solutions of the original equation in the ring Z_{128}.

   Answer: The elements 22, 54, 86 and 118.

2. (a) (0.1p) Prove that the sum of any three consecutive integers is divisible by 3. (For example the sum of 7, 6 and 5 is 18, which is divisible by 3.)

   Solution. Three consecutive integers are always equal to $n - 1$, n and $n + 1$ for some integer n. Trivially, then

   $$(n - 1) + n + (n + 1) = 3n,$$

   which evidently is an integer divisible by 3.

(b) (0.2p) Generalize this fact, i.e., find and prove a more general result from which the result above follows.

Solution. Assume $n = 2k+1$ for some integer k. Then the following sum of n consecutive integers

$$(m-k) + \cdots + (m-1) + m + (m+1) + \cdots + (m+k)$$

is equal to $(2k+1)m$. As any sum of an odd number of consecutive integers can be expressed in this way (m is the middle value of the integers), we have proved that for n odd, the sum of n consecutive integers is divisible by $n = 2k+1$. As $n = 3$ is an odd integer, this generalizes the statement in the previous subproblem.

3. (a) (0.1p) Give a definition of the greatest common divisor of a set of n non-zero integers $a_1, a_2, \ldots, a_n$, denoted by $\gcd(a_1, a_2, \ldots, a_n)$.

Solution. We define the greatest common divisor of the integers in the set $\{a_1, a_2, \ldots, a_n\}$ to be a positive integer D that satisfies
(i) D divides each of the integers a_1, a_2, ..., a_n.
(ii) If d divides each of the integers a_1, a_2, ..., a_n then d divides D.
We note that there is at most one integer D satisfying these two conditions. If there were another integer D' satisfying *(i)* and *(ii)* (with D substituted by D'), then D must divide D', and similarly we get that D' divides D. Hence $D = D'$.

(b) (0.2p) Use your definition above to prove that, for any three non-zero integers a_1, a_2 and a_3,

$$\gcd(a_1, a_2, a_3) = \gcd(\gcd(a_1, a_2), a_3).$$

Solution. Let D denote $\gcd(a_1, a_2, a_3)$ and let D' denote the integer $\gcd(\gcd(a_1, a_2), a_3)$. Then D divides a_1 and a_2 and hence, from the definition of the greatest common divisor of a_1 and a_2 we get that D divides $\gcd(a_1, a_2)$. Combining this with the fact that D divides a_3 we get, again by using the definition of the greatest common divisor of $\gcd(a_1, a_2)$ and a_3, that D divides D'.
Furthermore, if D' divides $\gcd(a_1, a_2)$ and a_3 (by definition of greatest common divisor), then D' also divides a_1 and a_2. This implies that D' divides the greatest common divisor of these three integers, i.e., that D' divides D.
If D' divides D and D divides D' then we must have that $D = D'$.

(c) (0.2p) Generalize the formula

$$\operatorname{lcm}(a_1, a_2) = \frac{a_1 a_2}{\gcd(a_1, a_2)},$$

to the case of finding $\text{lcm}(a_1, a_2, \ldots, a_n)$. You must also prove that your formula is correct.
The formula shall be such that a programmer who has a module for finding the greatest common divisor of any two integers, (but not for finding the least common divisor), can use your formula in some way, perhaps in a recursive way.

Solution. We use the notation

$$m_t = \text{lcm}(a_1, a_2, \ldots, a_t).$$

With arguments similar to those used above, it is evident that

$$m_t = \text{lcm}(m_{t-1}, a_t),$$

and thus that

$$m_t = \frac{m_{t-1} a_t}{\gcd(m_{t-1}, a_t)}$$

is true for $t = 3, 4, \ldots, n$. This gives a recursion for the sequence m_2, m_3, ..., m_n, where just multiplication of integers and taking the greatest common divisor of two integers are involved.