Matematiska Institutionen
KTH

Solutions to homework number 1 to SF2736, fall 2014.

Please, deliver this homework at latest on Monday, November 17, 2014. Provide both your name and your e-mail address with your solutions.

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

1. (0.1p) Find $700^{1734} \pmod{347}$.

   Solution We first prove that 347 is a prime number: As $\sqrt{347} < 19$ it is sufficient to check if any of the prime numbers less than 19 divides 347. Neither of 2, 3, 7, 11, 13 or 17 divides 347, so 347 is a prime number and we can apply the theorem of Fermat, as 347 does not divide 700. We get

   $$700^{1734} \equiv_{347} (700^{346})^5 700^4 \equiv_{347} 1^5 \cdot 6^4 \equiv_{347} 6^4 \equiv_{347} 1296 \equiv_{347} 255.$$

   As $0 \leq 255 < 347$ we get

   ANSWER: 255.

2. (0.2p) Find all solutions to the Diophantine equation

   $$346y + 512z = 10.$$

   Solution We get an equivalent system of equations by dividing by 2: $173y + 256z = 5$. The Euclidian algorithm gives

   $$256 = 1 \cdot 173 + 83, \quad 173 = 2 \cdot 83 + 7, \quad 83 = 12 \cdot 7 - 1,$$

   from which follows that

   $$1 = 12 \cdot 7 - 83 = 12(173 - 2 \cdot 83) - 83 = 12 \cdot 173 - 25 \cdot 83 = 12 \cdot 173 - 25(256 - 173)$$

   Thus

   $$173 \cdot 37 - 256 \cdot 25 = 1,$$

   and

   $$173 \cdot 185 + 256(-125) = 5$$

   Let y and z be any integer solution to the given equation. Then

   $$173y + 256z = 173 \cdot 185 + 256(-125) \quad \Longleftrightarrow \quad 173(185 - y) = 256(z + 125)$$

As 173 and 256 are coprime we may conclude that

$$z + 125 = 173k, \qquad 185 - y = 256k$$

for some integer k. It is easy to verify that each integer k gives a solution. Thus

ANSWER $y = 185 - 256k$ and $z = -125 + 173k$, where $k \in \mathbb{Z}$.

3. (0.3p) Let p be a prime number less than or equal to 13, and let a and b be elements in the ring $\mathbb{Z}_p$. Find the number of solutions in $\mathbb{Z}_p$ to the system of equations

$$\begin{cases} x + y + z = 1 \\ x + 2y + (a+1)z = b+1 \\ x + 3y + (a^2+2a+2)z = 3b+1 \end{cases}$$

Solution We solve the system by Gauss eliminations:

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 1 & 2 & a+1 & b+1 \\ 1 & 3 & a^2+2a+2 & 3b+1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 1 & a & b \\ 0 & 2 & a^2+2a+1 & 3b \end{array}\right) \sim$$

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & 1 & a & b \\ 0 & 0 & a^2+1 & b \end{array}\right)$$

If $a^2+1 \neq 0$ then the system has exactly one solution. If $a^2+1=0$ and $b \neq 0$ there are no solutions, while if $b=0$ the number of solutions is equal to p.

Now, in $\mathbb{Z}_3$, $\mathbb{Z}_7$ and $\mathbb{Z}_{11}$ as easily check the equation $a^2+1=0$ has no solutions. In $\mathbb{Z}_2$ we have $1^2+1=0$, $\mathbb{Z}_5$ we get that $(\pm 2)^2+1=0$, and in $\mathbb{Z}_{13}$, we get $(\pm 5)^2=-1$.

ANSWER. For $p=5$ one solution if and only if $a \neq \pm 2$. If $a = \pm 2$ no solution if $b \neq 0$ and five solutions if $b \neq 0$.

For $p=13$ one solution if and only if $a \neq \pm 5$. If $a = \pm 5$ no solution if $b \neq 0$ and 13 solutions if $b \neq 0$.

For $p=2$ one solution if and only if $a=0$. If $a=1$ no solution if $b \neq 0$ and two solutions if $b \neq 0$.

If $p = 2, 3, 7, 11$ exactly one solution for each a and b.

4. (0.4) For which integer sequences a_1, a_2, ..., a_t is it true that

$$\gcd(a_1, a_2, \ldots, a_t)\,\mathrm{lcm}(a_1, a_2, \ldots, a_t) = a_1 a_2 \cdots a_t\,.$$

Solution Let p_1, ..., p_s be prime numbers such that, for $i = 1, 2, \dots, t$,

$$a_i = p_1^{e_{i,1}} \cdots p_s^{e_{i,s}}$$

where $e_{i,j}$ are non-negative integers for $1 \le i \le t$ and $1 \le j \le s$.

Let, for $j = 1, 2, \dots, s$, f_j be the least of the integers $e_{i,j}$ and g_j be the largest of theses integers for $i = 1, 2, \dots, t$. Then

$$\gcd(a_1, a_2, \dots, a_t) = p_1^{f_1} \cdots p_s^{f_s},$$

$$\mathrm{lcm}(a_1, a_2, \dots, a_t) = p_1^{g_1} \cdots p_s^{g_s}$$

and

$$a_1 a_2 \cdots a_t = p_1^{e_{1,1}+\cdots+e_{t,1}} \cdots p_s^{e_{1,s}+\cdots+e_{t,s}}.$$

Consequently, the given equality is true if and only if

$$f_i + g_i = e_{1,i} + \cdots + e_{t,i}$$

is true for every $i = 1, 2, \dots, s$

If $t = 2$ this is always true. For $t > 2$, the equality above is true if and only if

$$e_{1,i} + \cdots + e_{t,i} = g_i,$$

that is, when all but one of the integers $e_{i,j}$ are equal to zero, or equivalently, the prime number p_i divides at most one of the integers a_1, ..., a_t. Hence

ANSWER. Either $t = 2$ or the integers a_1, ..., a_t are pairwise coprime.