**ET: Solutions 2015-03-11**

1. (a) Solve the diophantine equation $35x - 55y + 77z = 23$.
   **Answer**: $(x, y, z) = (11s+138-44t, 23-7t, -5s-46+15t)$, $s, t \in \mathbb{Z}$. We do the following column transformations

$$\begin{pmatrix} 35 & -55 & 77 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 35 & 15 & 7 \\ 1 & 2 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 1 & 7 \\ 11 & 6 & -2 \\ 0 & 1 & 0 \\ -5 & -2 & 1 \end{pmatrix}$$

$$\mapsto \begin{pmatrix} 0 & 1 & 0 \\ 11 & 6 & -44 \\ 0 & 1 & -7 \\ -5 & -2 & 15 \end{pmatrix}$$

   and multiply the last matrix with the vector $\begin{pmatrix} s \\ 23 \\ t \end{pmatrix}$.

   (b) Determine all continued fractions $K(a_0, ..., a_n) = \frac{89}{19}$.
   **Answer**: We have $89 = 4 \cdot 19 + 13, 19 = 1 \cdot 13 + 6, 13 = 2 \cdot 6 + 1, 6 = 6 \cdot 1$. Hence $\frac{89}{19} = K(4, 1, 2, 6) = K(4, 1, 2, 5, 1)$.

2. Solve the congruence $251x \equiv 125 \mod (521)$.

   **Solution**:

   (a) $251x = 125 + 521y$
   (b) $521y \equiv -125 \mod (251)$
   (c) $19y \equiv -125 \mod (251)$
   (d) $19y = -125 + 251z$
   (e) $251z \equiv 125 \mod (19)$
   (f) $4z \equiv -8 \mod (19)$

   If we take $z = -2$, we obtain $y = -33$ and $x = -68$. So $x \equiv -68 \mod (521)$ is the solution.

3. Determine the zeros of the following polynomials

(a) $X^2 - X$ in $\mathbb{Z}_{91}$,

**Answer**: The solutions are the idempotents in $\mathbb{Z}_{91}$. We consider the following chinese remainder table:

$$\begin{array}{c|c} \mathbb{Z}_{91} & \mathbb{Z}_7 \times \mathbb{Z}_{13} \\ \hline -\overline{13} & (\overline{1}, \overline{0}) \\ \overline{14} & (\overline{0}, \overline{1}) \end{array} \quad ,$$

and obtain the idempotents $\overline{1}, \overline{0}, -\overline{13}, \overline{14}$.

(b) $X^{11} - 2$ in $\mathbb{Z}_{125}$,

**Answer**: Let $f = X^{11} - 2$. For $\xi \in \mathbb{Z}_5^*$ we have $f(\xi) = \xi^{-1} - 2$, thus there is the unique zero $\xi = -\overline{2}$. Since $f'(-\overline{2}) = 11 \cdot \overline{2}^{10} \neq 0$, there is a unique lift to any residue class ring $\mathbb{Z}_{5^k}$. Indeed $-\overline{2} \in \mathbb{Z}_{25}$ is a zero of $f$ as well. In $\mathbb{Z}_{125}$ it is of the form $-\overline{2} + t \cdot \overline{25}$, with a solution $t$ of the congruence

$$f'(-2)t \equiv -\frac{f(-2)}{25} \mod (5),$$

i.e.

$$-t \equiv -3 \mod (5).$$

So we find $t = 3$ and $\xi = \overline{73}$ is the unique zero of $f$ in $\mathbb{Z}_{125}$..

(c) $X^2 + 25$ in $\mathbb{Z}_{125}$.

**Answer**: We find $\xi = \overline{5k}$, where $k^2 \equiv -1 \mod (5)$, i.e. $k \equiv \pm 2 \mod (5)$ resp. $k \equiv \pm 2, \pm 7, \pm 12, \pm 17, \pm 22 \mod (25)$. So the solutions are

$$\pm\overline{10}, \pm\overline{35}, \pm\overline{60}, \pm\overline{85}, \pm\overline{110} \in \mathbb{Z}_{125}.$$

4. Determine whether the following residue classes are squares!

(a) $\overline{328} \in \mathbb{Z}_{823}$

**Answer**: No: We compute, the number 823 being prime, Legendre symbols:

$$\left(\frac{328}{823}\right) = \left(\frac{2}{823}\right)^3 \cdot \left(\frac{41}{823}\right) = \left(\frac{823}{41}\right) = \left(\frac{3}{41}\right) = \left(\frac{41}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

since $823 \equiv -1 \mod (8)$ and $41 \equiv 1 \mod (4)$.

(b) $\overline{823} \in \mathbb{Z}_{328}$.

**Answer**: No: The Chinese remainder isomorphism

$$\mathbb{Z}_{328} \xrightarrow{\cong} \mathbb{Z}_8 \times \mathbb{Z}_{41}$$

maps $\overline{823}$ to $(-\overline{1}, \overline{3})$. Since $-\overline{1} \in \mathbb{Z}_8$ is not a square, $\overline{823} \in \mathbb{Z}_{328}$ is not a square either.

5. (a) Find a primitive root in $\mathbb{Z}_{14641}^*$!

**Solution**: First of all $14641 = 11^4$. Now $\overline{2} \in \mathbb{Z}_{11}$ is a primitive root, since $\overline{2}^2 = \overline{4} \neq \overline{1}$ as well as $\overline{2}^5 = -\overline{1} \neq \overline{1}$. So $\overline{2} \in \mathbb{Z}_{121}$ has either order 10 as well or 110. But $\overline{2}^{10} = \overline{56} \neq \overline{1}$ holds in $\mathbb{Z}_{121}$, so $\overline{2}$ is a primitive root for $\mathbb{Z}_{121}^*$ and then automatically for $\mathbb{Z}_{14641}^*$ as well.

(b) Does $\mathbb{Z}_{1001}^*$ admit a primitive root?

**Answer**: No: The Chinese remainder isomorphism

$$\mathbb{Z}_{1001} \xrightarrow{\cong} \mathbb{Z}_7 \times \mathbb{Z}_{11} \times \mathbb{Z}_{13}$$

induces a bijection

$$\mathbb{Z}_{1001}^* \xrightarrow{\cong} \mathbb{Z}_7^* \times \mathbb{Z}_{11}^* \times \mathbb{Z}_{13}^*.$$

It follows that $\xi^{60} = 1$ holds for all $\xi \in \mathbb{Z}_{1001}^*$, while $|\mathbb{Z}_{1001}^*| = 720$.

6. (a) Find all $(x, y) \in \mathbb{N}, x < y$, s.th. $x^2 + y^2 = 845$.

**Answer**: We onsider the equation

$$z\overline{z} = 845 = 5 \cdot 13^2 = (2 + i)(2 - i)(3 + 2i)^2(3 - 2i)^2.$$

Up to sign and interchange of components the real and imaginary parts of the following complex numbers

i. $z = (2 + i)(3 + 2i)^2 = -2 + 29i$

ii. $z = (2 + i)(3 + 2i)(3 - 2i) = 26 + 13i$,

iii. $z = (2 + i)(3 - 2i)^2 = 22 - 19i$.

provide all $(x, y), x^2 + y^2 = 845$. We obtain

$(x,y) = (2,29), (13,26), (19,22)$.

(b) Which numbers $c \in \mathbb{N}_{>0}$ do occur in a pythagorean triple $(a,b,c) \in (\mathbb{N}_{>0})^3$?

**Answer**: All numbers having a prime divisor $p \equiv 1 \mod (4)$. For such a divisor ($c = c_0 p$) we have $p = z\overline{z}$ for some $z = x + iy, 0 < y < x$, and $z^2 = a + ib$ with $a, b > 0$. So $(c_0 a, c_0 b, c)$ is a pythagorean triple. If $c$ is not divisible with a prime $p \equiv 1 \mod (4)$, we have $c = 2^m q$ with a product $q$ of primes $\equiv 3 \mod (4)$, and $c^2 = z\overline{z}$ implies

$$z \in (1+i)^{2m}\mathbb{Z}q \cup (1+i)^{2m}\mathbb{Z}qi,$$

i.e. $x = 0$ or $y = 0$, whenever $c^2 = x^2 + y^2$.

7. (a) Find the continued fraction $K(a_0, ...) = \sqrt{15}$. Compute $K(a_0, a_1, a_2)^2$.

**Solution**:

i. $x_0 = \sqrt{15}$ gives $a_0 = [x_0] = 3$,
ii. $x_1 = \frac{1}{\sqrt{15}-3} = \frac{1}{6}(\sqrt{15}+3)$ gives $a_1 = [x_1] = 1$,
iii. $x_2 = \sqrt{15}+3$ gives $a_2 = [x_2] = 6$,
iv. $x_3 = \frac{1}{6}(\sqrt{15}+3)$ gives $a_2 = [x_2] = 1$.

Since $x_3 = x_1$ we obtain $\sqrt{15} = K(3, \overline{1,6})$. Furthermore $K(3,1,6)^2 = 14\frac{43}{49}$.

(b) Find three solutions $(x,y) \in \mathbb{N}^2$ of $x^2 - 15y^2 = 1$.

**Answer**: $(1,0), (4,1)$ and $(x,y)$, where $x + y\sqrt{15} = (4+\sqrt{15})^2$, i.e. $(x,y) = (31,8)$.

(c) Are there solutions $(x,y) \in \mathbb{N}^2$ of $x^2 - 15y^2 = -1$?

**Answer**: No. $4 + \sqrt{15}$ is the basic unit, since the coefficient of $\sqrt{15}$ equals 1, and $N(4+\sqrt{15}) = 1$. The fact, that the period of the preperiodic continued fraction $\sqrt{15} = K(...)$ is even, gives the result as well.

8. Let $\tau : \mathbb{N}_{>0} \longrightarrow \mathbb{C}$ be the arithmetic function with $\tau(n) :=$ the number of positive divisors of $n$. Find $\psi : \mathbb{N}_{>0} \longrightarrow \mathbb{C}$ with

$$\tau * \psi = \delta.$$

Here $\delta(n) = \delta_{n1}$.

**Solution**: We have $\tau = 1 * 1$ and $1 * \mu = \delta$. Hence $\psi = \mu * \mu$, a multiplicative function. For primes $p$ we find $\psi(p) = -2, \psi(p^2) = 1$ and $\psi(p^k) = 0$ for $k > 2$.