TENTAMEN - ELEMENTARY NUMBER THEORY 2019/03/21

JULIAN KÜLSHAMMER

1. (i) Determine all (integer) solutions to the linear Diophantine equation $111x+81y-45z = 15$.

(ii) Determine all continued fractions $\langle a_0, a_1, \ldots, a_n\rangle$ whose value $K(\langle a_0, a_1, \ldots, a_n\rangle)$ is equal to $\frac{239}{35}$.

Solution 1. (i) With the substitution $z' = -z + 2x + y$, the solutions to the equation

$$111x + 81y - 45z = 15$$

are the same as the solutions to the equation

$$21x + 36y + 45z' = 15.$$

Performing the substitution $x' = x + y + 2z'$, we obtain the equation

$$21x' + 15y + 3z' = 15.$$

Again substituting $z'' = z' + 7x' + 5y$ we obtain

$$3z'' = 15.$$

Therefore $z'' = 5$, and $x' = s, y = t$ are free parameters. Substituting back we obtain

$$\begin{aligned} z' &= z'' - 7x' - 5y = 5 - 7s - 5t \\ x &= x' - y - 2z' = -10 + 15s + 9t \end{aligned}$$

Again substituting back we obtain

$$z = 2x + y - z' = -25 + 37s + 24t.$$

Summarising one (of the many) possible parametrisations of the solution set is

$$\begin{aligned} x &= -10 + 15s + 9t \\ y &= t \\ z &= -25 + 37s + 24t \end{aligned}$$

with $s, t \in \mathbb{Z}$.

(ii) We use the Euclidean algorithm to obtain

$$\begin{aligned} 239 &= 6 \cdot 35 + 29 \\ 35 &= 1 \cdot 29 + 6 \\ 29 &= 4 \cdot 6 + 5 \\ 5 &= 1 \cdot 5 + 1 \\ 5 &= 5 \cdot 1 \end{aligned}$$

Therefore, $\frac{239}{35} = K(\langle 6, 1, 4, 1, 5\rangle) = K(\langle 6, 1, 4, 1, 4, 1\rangle)$. Since every rational number can be expressed as the value of a continued fraction in exactly two different ways, these are all continued fraction expansions of $\frac{239}{35}$.

2. Solve the following system of linear congruences:

$$\begin{aligned} x &\equiv 2 \mod 12 \\ x &\equiv 6 \mod 10 \\ x &\equiv 11 \mod 45 \end{aligned}$$

Solution 2. By the Chinese Remainder Theorem, the system of linear congruences is equivalent to the system

$$\begin{aligned} x &\equiv 2 \mod 4 \\ x &\equiv 2 \mod 3 \\ x &\equiv 6 \mod 2 \\ x &\equiv 6 \mod 5 \\ x &\equiv 11 \mod 9 \\ x &\equiv 11 \mod 5 \end{aligned}$$

Using that $2 \equiv 6 \mod 2$, $2 \equiv 11 \mod 3$ and $6 \equiv 11 \mod 5$, the system is equivalent to

$$\begin{aligned} x &\equiv 2 \mod 4 \\ x &\equiv 1 \mod 5 \\ x &\equiv 2 \mod 9 \end{aligned}$$

We solve the system inductively. It is easy to see that $1 = 1 \cdot 5 - 1 \cdot 4$. Therefore, $5 \equiv 1 \mod 4, 5 \equiv 0 \mod 5, -4 \equiv 1 \mod 5, -4 \equiv 0 \mod 4$. It follows that

$$x = 2 \cdot 5 + 1 \cdot (-4) = 6$$

is a number that satisfies $x \equiv 2 \mod 4$ and $x \equiv 1 \mod 50$. In a next step we try to find a number x such that $x \equiv 6 \mod 20$ and $x \equiv 2 \mod 9$. We have that $1 = (-4) \cdot 20 + 9 \cdot 9$. Therefore $6 \cdot 81 + 2 \cdot (-80) = 326 \equiv 146 \mod 180$ is a number that solves the whole system of congruences and all solutions are of the form $x = 146 + 180n$ for $n \in \mathbb{Z}$.

3. Solve the congruence $x^3 + x + 4 \equiv 0 \mod 343$.

Solution 3. Note that $343 = 7^3$. Therefore, we use Hensel's lemma to compute the solutions to the congruence $x^3 + x + 4 \equiv 0 \mod 343$. As a first step, we check by trial and error that $x \equiv 2 \mod 7$ is the unique solution to $x^3 + x + 4 \equiv 0 \mod 7$. We set

$$f(x) = x^3 + x + 4.$$

Then $f'(x) = 3x^2 + 1$. We compute that $f'(2) = 13 \not\equiv 0 \mod 7$. Therefore, there is a unique lift of the solution $x \equiv 2 \mod 7$ to a solution to $f(x) \equiv 0 \mod 49$. This unique solution is of the form $2 + 7t$ where t is the unique solution fo

$$f'(2)t \equiv -\frac{f(2)}{7} \mod 7.$$

As $f'(2) \equiv -1 \mod 7$ and $f(2) = 14$, we obtain that $t = 2$. Therefore $x = 2 + 7 \cdot 2 = 16$ is the unique solution to the congruence $f(x) \equiv 0 \mod 49$. It is clear that $f'(16) \equiv f'(2) \not\equiv 0 \mod 7$, therefore there is a unique solution to $f(x) \equiv 0 \mod 343$. This unique solution is of the form $16 + 49t$ where t is the unique solution to the congruence

$$f'(16)t \equiv -\frac{f(16)}{49} \mod 7.$$

Since $f'(16) \equiv -1 \mod 7$ and $\frac{f(16)}{49} = \frac{4116}{49} = 84 \equiv 0 \mod 7$, it follows that $t = 0$ and therefore $16 + 49 \cdot 0 = 16$ is the unique solution to $f(x) \equiv 0 \mod 343$.

4. (i) Show that $\overline{6}$ is a primitive root in $(\mathbb{Z}/11\mathbb{Z})^\times$.
(ii) How many primitive roots are there in $(\mathbb{Z}/11\mathbb{Z})^\times$? Determine all of them.

Solution 4. (i) A primitive root in $(\mathbb{Z}/11\mathbb{Z})^\times$ is an element of order $\phi(11) = 11 - 1 = 10$ in $(\mathbb{Z}/11\mathbb{Z})^\times$. Since $10 = 2 \cdot 5$, and (by Fermat's little theorem) the order of every element of $(\mathbb{Z}/11\mathbb{Z})^\times$ divides $\phi(11)$, it suffices to show that $6^2 \not\equiv 1 \mod 11$ and $6^5 \not\equiv 1 \mod 11$. We compute that $6^2 = 36 \equiv 3 \not\equiv 1 \mod 11$ and $6^5 = (6^2)^2 \cdot 6 \equiv 9 \cdot 6 \equiv 10 \mod 11$, it follows that the order of $\overline{6}$ is 10 and therefore $\overline{6}$ is a primitive root in $(\mathbb{Z}/11\mathbb{Z})^\times$.

(ii) There are $\phi(\phi(11)) = \phi(10) = \phi(2)\phi(5) = 1 \cdot 4 = 4$ primitive roots in $(\mathbb{Z}/11\mathbb{Z})^\times$. Every element of $(\mathbb{Z}/11\mathbb{Z})^\times$ is of the form $\overline{6}^j$ for some $j \in \{0, \dots, 9\}$. The primitive roots are precisely those of the form $\overline{6}^j$ with $\gcd(j, 10) = 1$. The possible j are therefore $j = 1, 3, 7, 9$. We compute hat $\overline{6}^1 = \overline{6}, \overline{6}^3 = \overline{3 \cdot 6} = \overline{7}$, $\overline{6}^7 = \overline{5 \cdot 6} = \overline{8}$, and $\overline{6}^9 = \overline{8 \cdot 3} = \overline{2}$. Therefore $\overline{2}, \overline{6}, \overline{7}, \overline{8}$ are the primitive roots in $(\mathbb{Z}/11\mathbb{Z})^\times$.

5. Let

$$s \colon \mathbb{N}_1 \to \mathbb{C}, \quad s(n) = \begin{cases} 0 & \text{if there exists a prime number } p \text{ such that } p^2 \mid n, \\ 1 & \text{else,} \end{cases}$$

be the characteristic function of the square free numbers.

(i) Show that s is multiplicative.
(ii) Compute the Möbius transform $s * \mu$ of s where μ is the Möbius function and $*$ denotes the convolution product.

Solution 5. (i) Let m and n be coprime integers. We have that

$$s(m)s(n) = \begin{cases} 0 & \text{if } p^2|m \text{ or } p^2|n, \\ 1 & \text{else,} \end{cases}$$

and

$$s(mn) = \begin{cases} 0 & \text{if } p^2|mn \\ 1 & \text{else.} \end{cases}$$

Since $p^2|mn$ if and only if $p^2|m$ or $p^2|n$ since m and n are coprime, it follows that $s(m)s(n) = s(mn)$ and therefore s is multiplicative.

(ii) Since s and μ are both multiplicative, it follows that $s * \mu$ is multiplicative and therefore it suffices to compute $s * \mu$ on prime powers. We obtain that

$$(s*\mu)(p^k) = \sum_{p^m|p^k} s(p^m)\mu(p^{m-k}) = \begin{cases} 0 & \text{if } k \geq 3, \\ -1 & \text{if } k = 2, \\ s(p)\mu(1) + s(1)\mu(p) = 1 + (-1) = 0 & \text{if } k = 1, \\ 1 & \text{if } k = 0. \end{cases}$$

where we used that $s(p^m) = \mu(p^m) = 0$ for $m \geq 2$ and $\mu(p) = -1$.

6. (i) Determine the value $z = K(\langle 4; \overline{4, 8}\rangle)$ of the periodic continued fraction $\langle 4; \overline{4, 8}\rangle$. Find an integer d such that $z^2 = d$.

(ii) Compute the first three convergents of z.

(iii) Give two positive integer solutions to the equation $x^2 - dy^2 = 1$ where d is as in (i).

Solution 6. (i) Since $z = K(\langle 4; \overline{4, 8}\rangle) = 4 + \frac{1}{K(\langle \overline{4,8}\rangle)}$ we first compute $y = K(\langle \overline{4, 8}\rangle)$. We have that

$$y = 4 + \frac{1}{8 + \frac{1}{y}} = 4 + \frac{y}{8y + 1}.$$

Multiplying both sides by $8y + 1$ we obtain that $8y^2 - 32y - 4 = 0$, or equivalently $y^2 - 4y - \frac{1}{2} = 0$. Using the p-q-formula, we obtain that the solutions to this quadratic equation are

$$y_{1/2} = 2 \pm \sqrt{4 + \frac{1}{2}}$$

Since $y > 0$, it follows that $y = 2 + \frac{3}{\sqrt{2}}$. It follows that

$$z = 4 + \frac{1}{2 + \frac{3}{\sqrt{2}}} = 4 + \frac{\sqrt{2}}{2\sqrt{2} + 3} = \frac{9\sqrt{2} + 12}{2\sqrt{2} + 3} = \frac{(9\sqrt{2} + 12)(2\sqrt{2} - 3)}{-1} = 3\sqrt{2} = \sqrt{18}.$$

Therefore, $d = 18$ is an integer such that $z^2 = d$.

(ii) The first three convergents of z are

$$c_1 = 4 + \frac{1}{4} = \frac{17}{4},\ c_2 = 4 + \frac{1}{4 + \frac{1}{8}} = \frac{140}{33},\ \text{and } c_3 = 4 + \frac{1}{4 + \frac{1}{8 + \frac{1}{4}}} = \frac{577}{136}.$$

(iii) The given equation is an instance of Pell's equation. The period of the continued fraction expansion of $\sqrt{18}$ is 2 and therefore even. It follows that the solutions to Pells equation are given by $(x, y) = (p_{2k-1}, q_{2k-1})$ where $k \in \mathbb{N}$. Therefore, two possible solutions are $(x, y) = (17, 4)$ and $(x, y) = (577, 136)$.

7. Let $p > 2$ be a prime number. Show that the smallest positive integer a, such that the Legendre symbol $\left(\frac{a}{p}\right) = -1$, is a prime number.

Solution 7. We know that $\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right) \cdot \left(\frac{n}{p}\right)$. Furthermore $\left(\frac{b}{p}\right) \in \{-1, 0, 1\}$ for all $b \in \mathbb{Z}$. Therefore, if a were composite, then $a = mn$ for some m,n with $0 < m, n < a$. If all $0 < b < a$ would satisfy $\left(\frac{b}{p}\right) \in \{0, 1\}$ we would obtain that

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right) \cdot \left(\frac{n}{p}\right) \in \{0, 1\},$$

a contradiction. Therefore, a has to be a prime number.

8. Prove that the Diophantine equation $x^4 - 4y^4 = z^2$ has no positive integer solution.

Solution 8. Let x, y, z be positive integers such that $x^4 - 4y^4 = z^2$. Assume without loss of generality that x, y, z are pairwise coprime (otherwise, one obtains a smaller solution by dividing the equation by a common divisor). Rewriting the equation, we obtain that

$$(x^2)^2 = z^2 + (2y^2)^2.$$

Therefore, $(2y^2, z, x^2)$ is a primitive pythagorean triple. It follows that there exist coprime $a, b \in \mathbb{Z}$ such that $x^2 = b^2 + a^2$, $z = b^2 - a^2$, and $2y^2 = 2ab$. In particular, $y^2 = ab$. Since a, b are coprime, it follows that there exist positive integers r, s such that $a = r^2$ and $b = s^2$. Substituting in $x^2 = b^2 + a^2$ we obtain that

$$x^2 = r^4 + s^4.$$

By the stronger version of the special case of Fermat's last theorem for $n = 4$ proved in the lecture, this Diophantine equation doesn't have any positive integer solutions, and therefore the original Diophantine equation $x^4 - 4y^4 = z^2$ doesn't have any positive integer solutions.