Goethe-Universität Frankfurt
Institut für Mathematik
Summer term 2020
30. Juni 2020

Elementare Zahlentheorie
Prof. Dr. Martin Möller
Dr. Jonathan Zachhuber
M.Sc. Riccardo Zuffetti

Übungsblatt 11

Aufgabe 1 (6 Punkte)

Let d be a positive integer that is not a square. Prove that if (x, y) is a positive solution of Pell's equation $X^2 - dY^2 = m$ for some $m \in \mathbb{Z}$ satisfying $|m| < \sqrt{d}$, then x/y is a convergent of the continued fraction expansion of $\sqrt{d}$. Is the vice-versa true?
Hint. Case $m > 0$: use Satz 8.25.(3) with $|\sqrt{d} - x/y|$. Case $m < 0$: look at y/x as an approximation of $1/\sqrt{d}$, following the idea of the previous case.

Aufgabe 2 (2 Punkte)

Let p be a prime greater than 5. Prove that:

(i) $X^2 \equiv 2 \bmod p$ admits a solution if and only if $p \equiv 1, 7 \bmod 8$.

(ii) $X^2 \equiv 3 \bmod p$ admits a solution if and only if $p \equiv 1, 11 \bmod 12$.

(iii) $X^2 \equiv 5 \bmod p$ admits a solution if and only if $p \equiv 1, 4 \bmod 5$.

(iv) $X^2 \equiv 6 \bmod p$ admits a solution if and only if $p \equiv 1, 5, 19, 23 \bmod 24$.

Aufgabe 3 (4 Punkte)

Let $m, n \in \mathbb{Z}_{>0}$ be odd and let $a \in \mathbb{Z}$ be such that $\gcd(a, mn) = 1$.

(i) Prove that if $m \equiv n \bmod 4|a|$ then $\left(\frac{a}{m}\right) = \left(\frac{a}{n}\right)$.

(ii) Give an example of $a > 0$ odd which shows that the condition $m \equiv n \bmod 2a$ is not sufficient for the previous point.

Aufgabe 4 (4 Punkte)

(i) Compute $\left(\frac{2017}{5843}\right)$ and $\left(\frac{13259}{35671}\right)$.

(ii) Deduce if the following quadratic congruence equations admit a solution.

$$\begin{aligned} &X^2 + 3826 \equiv 0 \mod 5843, \\ &X^2 + 9X + 6 \equiv 0 \mod 11, \\ &16X^2 + 40X + 17 \equiv 0 \mod 89, \\ &X^2 + 2X + 1002 \equiv 0 \mod 483. \end{aligned}$$

Please, upload your solutions on the Olat page of this course, by **14:00** on **Wednesday, 08.07.2020**.