Goethe-Universität Frankfurt
Institut für Mathematik

Prof. Dr. Jakob Stix
Theresa Kumpitsch

Elementare Zahlentheorie

Wintersemester 2021/22

Übungsblatt 12 21.01.22

Aufgabe 1 (Und noch eine Primzahlaufgabe, 5 Punkte)**.**
Sei p eine ungerade Primzahl. Ziel der Aufgabe ist es zu zeigen, dass es unendlich viele Primzahlen der Form $p = x^2 - 2y^2$ gibt. Dazu finden wir zunächst eine alternative Beschreibung solcher Primzahlen.

(a) Sei p eine Primzahl mit $p = x^2 - 2y^2$ für $x, y \in \mathbb{Z}$. Dann gilt $p \equiv \pm 1 \bmod 8$.
(b) Zeigen Sie die Rückrichtung von (a).
Tipp: Schauen Sie sich dazu nochmal den Satz von Thue (Satz 5.33) und den Beweis des Zwei-Quadrate-Satz (Theorem 5.39) an.
(c) Folgern Sie, dass es unendlich viele Primzahlen der Form $p = x^2 - 2y^2$ gibt.
Hinweis: Hier darf man bereits gezeigte Aussagen über Primzahlen der Form $\pm 1 + 8k$ benutzen, kann aber auch ein neues Argument à la Euklid finden (Tipp: Betrachte N^2-2).

Aufgabe 2 (Chevalley-Warning, 5 Punkte)**.** Sei p eine Primzahl und sei

$$E(\mathbb{F}_p) \coloneqq \left\{(x, y) \in \mathbb{F}_p^2 \mid y^2 = x^3 - 1\right\}.$$

Ziel ist zu zeigen, dass für $p = 3$ und $p \equiv 2 \bmod 3$ gilt $\#E(\mathbb{F}_p) = p$. Gehen Sie dazu wie folgt vor:

(a) Zeigen Sie die Behauptung für $p = 2, 3$.
Sei nun $p \geq 5$.
(b) Zeigen Sie, dass $0 < \#E(\mathbb{F}_p) < 2p$.
(c) Sei $p \equiv 2 \bmod 3$. Zeigen Sie, dass $\#E(\mathbb{F}_p) \equiv 0 \bmod p$.
Tipp: Nutzen Sie Chevalley-Warning (Abschnitt 14.2). Nutzen Sie speziell, dass

$$\#E(\mathbb{F}_p) \equiv S\left(1 - (y^2 + 1 - x^3)^{p-1}\right) \bmod p.$$

(d) Folgern Sie die Behaupung.

Aufgabe 3 (Diophantische Gleichungen mod n – Teil 2, 5 Punkte)**.**

(a) Sei $a \in \mathbb{Z}$. Untersuchen Sie die Lösbarkeit von $x^2 \equiv a \bmod 2^n$ für $n \geq 1$.
(b) Zeigen Sie, dass die Gleichung

$$(X^2 - 2)(X^2 - 17)(X^2 - 34) = 0$$

keine ganzzahlige Lösung $x \in \mathbb{Z}$ besitzt, allerdings Lösungen mod n für alle n.

Hinweis: Schauen Sie sich nochmal Blatt 10, Aufgabe 4 an.

Aufgabe 4 (Variantionen der Reichardt–Lind-Kurve (oder Freizeit), 5 Punkte)**.**
Freuen Sie sich darüber, dass es diese Woche eine Vorlesung und eine Aufgabe weniger gibt und gönnen sich eine Auszeit…

… oder denken Sie über folgende Frage nach: Gibt es eine Primzahl $p \neq 17$, so dass

$$X^4 - p = 2Y^2$$

keine rationalen Lösungen hat, aber mod m für jedes m eine Lösung hat?

Abgabe: Am kommenden Freitag, den **28.01.22**, bis um 12:00 digital auf OLAT.