Goethe-Universität Frankfurt
Institut für Mathematik

Prof. Dr. Jakob Stix
Theresa Kumpitsch

Elementare Zahlentheorie

Wintersemester 2021/22

Übungsblatt 7 03.12.21

Aufgabe 1 (Unendlich viele Primzahlen (in arithmetischer Progression), 5 Punkte)**.**

(a) Seien $n, m \in \mathbb{N}$. Zeigen Sie: Wenn $n \not\equiv 1 \pmod m$, so existiert ein Primteiler p von n mit $p \not\equiv 1 \pmod m$.

(b) Modifizieren Sie den bekannten Trick von Euklid, um zu zeigen, dass es jeweils unendlich viele Primzahlen p gibt der Form

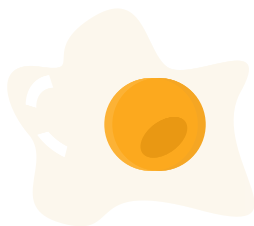
(i) $p \equiv 2 \pmod 3$,

(ii) $p \equiv 3 \pmod 4$,

(iii) $p \equiv 5 \pmod 6$.

(c) Betrachten Sie nun allgemeiner Primzahlen p mit $p \equiv k \pmod n$. Welche Bedingung muss man an k und n stellen damit der modifizierte Trick von Euklid, der in (b) verwendet wurde, funktioniert? Gibt es weitere Beispiele?

Aufgabe 2 (Sehr realitätsnahe Textaufgabe, 3 Punkte)**.**
Der kleine Carl Friedrich geht auf den Markt und kauft Eier, die er lose in einem Korb platziert. Als er auf dem Heimweg eine brilliante Idee zu einem mathematischen Problem hatte, lies er vor Schreck den Korb fallen und alle Eier zerbrachen. Er möchte zum Markt zurück, um die Eier zu ersetzen, hat aber vergessen, wie viele Eier in seinem Korb waren. Er weiß nur noch: Wenn die Eier auf 3er-Kartons aufgeteilt wurden, blieben 2 Eier übrig, als er die Eier in 4er, 5er oder 6er-Kartons aufteilte, blieben 3,4 bzw. 5 Eier übrig. Nur bei der Aufteilung in 7er-Kartons blieben keine Eier übrig.



Was ist die kleinste mögliche Menge an Eiern, die Carl Friedrich in seinem Korb hatte?

Aufgabe 3 (Noch eine "Anwendung" des Chinesischen Restsatzes, 3 Punkte)**.** Es gibt beliebig viele aufeinanderfolgende ganze Zahlen, die alle nicht als Summe zweier Quadrate darstellbar sind.
Tipp: Sie dürfen den "vollständigen" Zwei-Quadrate-Satz (Satz 5.41) benutzen.

Aufgabe 4 (Fermat-Pseudoprimzahlen, 3 Punkte)**.**

(a) Zeigen Sie, dass 341 eine Fermat-Pseudoprimzahl zur Basis 2 ist.

(b) Zeigen Sie, dass es unendlich viele Fermat-Pseudoprimzahlen zur Basis 2 gibt.
Tipp: Zeigen Sie: mit n ist auch $2^n - 1$ eine Fermat-Pseudoprimzahl zur Basis 2.

Aufgabe 5 (Carmichaelzahlen, 6 Punkte)**.**
Zeigen Sie die folgenden Aussagen:

(a) Wenn $p \mid n$, dann existiert in $(\mathbb{Z}/n\mathbb{Z})^\times$ein Element der Ordnung $p-1$.

(b) Wenn $p^2 \mid n$, dann existiert in $(\mathbb{Z}/n\mathbb{Z})^\times$ ein Element der Ordnung p.

(c) Die Zahl n ist genau dann eine Carmichaelzahl, wenn n quadratfrei ist und für jeden Primteiler $p \mid n$ gilt: $p-1 \mid n-1$

(d) Die 2 ist die einzige gerade Carmichaelzahl.

(e) Die 561 ist Carmichaelzahl.
Tipp: Verwenden Sie, dass für jede Primzahl p und $k \geq 2$ die Gruppe $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$ ein Element der Ordnung p enthält, beispielsweise als Konsequenz des Satzes von Cauchy.

Abgabe: Am kommenden Freitag, den **10.12.21**, bis um 12:00 digital auf OLAT.