Einführung in die Zahlentheorie
Blatt 8

hhu Düsseldorf
WiSe 2021/22

Abgabe: bis Montag 6.12.2021

Vorlesungswebseite: `http://reh.math.uni-duesseldorf.de/~khalupczok/EZ/`
Die folgenden Aufgaben sind schriftlich zu bearbeiten und abzugeben. Wie üblich sind dabei alle Behauptungen zu beweisen. Resultate aus der Vorlesung dürfen verwendet werden, die zugehörigen Referenznummern können Sie zur Klarstellung dann mit angeben.

Aufgabe 1 (2 Punkte):

Zeigen Sie unter Verwendung der Eulerkongruenz mod $9n$: Jede ungerade natürliche Zahl n, die kein Vielfaches von 5 ist, teilt eine Repetier-Eins (vgl. Aufgabe 3 auf Blatt 1).

Aufgabe 2 (5 Punkte):

Wieviele Lösungen kann die Kongruenz $x^3 - 54x^2 - 5x + 3^{41} \equiv 0 \bmod 55$ maximal haben? Berechnen Sie alle Lösungen durch Zerlegung des Polynoms in Linearfaktoren mod 55, welche in diesem Beispiel (nach Reduktion der Koeffizienten) leicht zu machen ist.

Aufgabe 3 (5 Punkte):

Sei $f(X) = a_nX^n + \cdots + a_1X + a_0$ ein Polynom vom Grade $n \geq 1$ mit Koeffizienten in $\mathbb{Z}$. Es bezeichne P_f die Menge aller Primzahlen p, für welche die Kongruenz

$$f(X) \equiv 0 \bmod p$$

lösbar in $\mathbb{Z}$ ist. Zeigen Sie: Die Menge P_f ist unendlich.

(**Hinweis**: Es gibt ein $c \in \mathbb{N}$ mit $|f(x)| \geq 2$ für alle $x \geq c$. Übergang zu $g(X) = f(cX)$ zeigt, dass man Œ $c = 1$ annehmen darf. Ferner kann man von $a_0 \neq 0$ ausgehen. Ist nun $a_0 = 1$, so verfahre man ganz ähnlich wie in Euklids Beweis. Auf den Fall $a_0 = 1$ kann man sich aber per Übergang zu $g(X) = f(a_0X)$ leicht zurückziehen.)

Aufgabe 4 (5 Punkte):

(1) Bestimmen Sie eine Nullstelle der Funktion $f(x) = x^3 - 10 \bmod 3^n$ für $n = 1, 2, 3, 4, 5$.

(2) Berechnen Sie die beiden Lösungen von $x^2 \equiv -1 \bmod 13^n$ für $n = 1, 2, 3, 4$.

Aufgabe 5 (3 Punkte):

(1) Sei p prim. Zeigen Sie durch Reduktion der Faktoren $1, \ldots, p-1$ in $(p-1)!$ auf den absolut kleinsten Rest mod p, dass gilt:

$$(p-1)! \equiv (-1)^{\frac{p-1}{2}} \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 \bmod p.$$

(2) Geben Sie für $p \equiv 1 \bmod 4$ prim die Lösungen der Kongruenz $r^2 \equiv -1 \bmod p$ explizit an.

(3) Finden Sie auf diesem Wege die beiden Lösungen von $r^2 \equiv -1 \bmod 29$ (nach jeder Multiplikation kann mod 29 reduziert werden, um kleinere Zahlen zu erhalten).