Klausur — Elementare Zahlentheorie SoSe 2014

N-P. Skoruppa und Fabien Cléry

17. Juli 2014

Name:	
Matrikelnummer:	
Studiengang:	
Studiensemester:	
Geburtsdatum:	

Sie erhalten Papier für Ihre Notizen und Lösungen von uns. Auf Ihrem Arbeitsplatz sollten sich nichts anderes als das Aufgabenblatt, das von uns gestellte Papier und maximal drei Kugelschreiber befinden. Insbesondere sind Taschenrechner, Handys, Vorlesungsmitschriften und Etuis nicht erlaubt.

1 Grundbegriffe

Vervollständigen Sie die folgenden Aussagen.

1.1

Die Ordnung der primitiven Restklasse $3 + 40\mathbb{Z}$ in $(\mathbb{Z}/40\mathbb{Z})^*$ ist

4.

1.2

Die Ordnung einer Primitivwurzel modulo 3^5 ist

$3^4 \cdot 2 = 243 \cdot 2 = 486$.

1.3

Die Anzahl der Geraden in der projektiven Ebene über $\mathbb{Z}/5Z$ ist

gleich der Anzahl der Punkte, also $(5^3 - 1)/4 = 31$.

1.4

Die zur Gruppe der primitiven Restklassen modulo einer ganzen Zahl $m > 0$ duale Gruppe ist definiert als

die Menge der Gruppenhomomorphismen $(\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ versehen mit üblicher Multiplikation von Funktionen.

1.5

Das Legendresymbol modulo einer ungeraden Primzahl p ist folgendermaßen definiert:

$$\left(\tfrac{a}{p}\right) = \begin{cases} 1 & \text{falls } a \equiv x^2 \bmod p \text{ lösbar ist,} \\ 0 & \text{falls } p|a, \\ -1 & \text{sonst.} \end{cases}$$

1.6

Für ganze Zahlen $a_1, \ldots, a_n$ wird das Ideal $\mathbb{Z}a_1 \cap \mathbb{Z}a_2 \cap \cdots \cap \mathbb{Z}a_n$ erzeugt von

dem kleinsten gemeinsamen Vielfachen der $a_1, \ldots, a_n$.

1.7

Die Primzahlverteilungsfunktiom $\pi(x)$ ist definiert als

die Anzahl aller Primzahlen $\leq x$.

1.8

Eine elliptische Kurve über $\mathbb{Q}$ ist

eine ebene projektive algebraische Kurve, die in affinen Koordinaten durch eine Gleichung $y = f(x)$ gegeben ist, wobei f ein kubisches Polynom mit rationalen Koeffizienten ohne mehrfache Nullstellen ist.

1.9

Die Inverse der Möbiusfunktion (bzgl. des Dirichletprodukts) ist die arithmetische Funktion

die n auf n abbildet.

1.10

Ein Dirichletcharakter modulo m ist

ein Gruppenhomomorphismus $(\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$.

2 Methoden

2.1

Entscheiden Sie, welche der folgenden Gleichungen nicht-triviale Lösungen in ganzen Zahlen besitzen

1. $x^2 + 7y^2 - 11z^2 = 0$.
2. $23x^2 + 3y^2 - 7z^2 = 0$.

1. $(2, 1, 1)$ ist eine (offensichtliche) Lösung. 2. Es ist $\left(\frac{3\cdot 7}{23}\right) = \left(\frac{3}{23}\right)\left(\frac{7}{23}\right) = \left(\frac{23}{3}\right)\left(\frac{23}{7}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{7}\right) = -1$. Also gibt es nach dem Satz von Legendre keine Lösung über $\mathbb{Z}$.

2.2

Bestimmen Sie die Menge aller rationalen Lösungen (x, y) der Gleichung

$$2x^2 + 2xy - y^2 = 3.$$

Es ist $(1, 1)$ eine rationale Lösung. Das Geradenbüschel $\{y = t(x - 1) + 1 : t \in \mathbb{Q}\}$ parametrisiert die rationalen Punkte auf $2x^2 + 2xy - y^2 = 3$, indem man der Geraden $y = t(x - 1) + 1$ den zweiten Schnittpunkt $(\frac{t^2-2t+4}{t^2-2t-2}, \frac{t^2+4t-2}{t^2-2t-2})$ mit der Kurve $2x^2 + 2xy - y^2 = 3$ zuordnet.

2.3

1. Haben die folgenden Kongruenzen Lösungen?

   (a) $x^2 \equiv 14 \bmod 31$,

   (b) $x^2 \equiv 25 \bmod 1997$.

2. Zeigen Sie, dass $x \in \mathbb{Z}$ genau dann ein Quadrat modulo eine gegebenen Primzahl p ist, wenn x^5 ein Quadrat modulo p ist.

3. Sei p ungerade Primzahl. Zeigen Sie, dass mindestens eine der drei Zahlen -1, 2, -2 ein Quadrat modulo p ist.

1. (a) Ja, denn $\left(\frac{14}{31}\right) = \left(\frac{2}{31}\right)\left(\frac{7}{31}\right) = \left(\frac{31}{7}\right) \cdot (-1)^{\frac{31-1}{2} \cdot \frac{7-1}{2}} = \left(\frac{3}{7}\right) \cdot (-1) = \left(\frac{7}{3}\right) = 1$. (b) Ja, denn es ist ja sogar $5^2 = 25$. 2. Dies folgt wegen $\left(\frac{x}{p}\right) = \left(\frac{x^5}{p}\right)$. 3. Es ist -1 Quadrat modulo p, falls $p \equiv 1 \bmod 8$ or $p \equiv 5 \bmod 8$, es ist 2 ein Quadrat modulo p, falls $p \equiv \pm 1 \bmod 8$, und es ist -2 ein Quadrat modulo p, falls $p \equiv 1 \bmod 8$ or $p \equiv 3 \bmod 8$.

2.4

Sei $n \in \mathbb{Z}_{\geq 0}$ und $F_n = 2^{2^n} + 1$.

1. Zeigen Sie, dass $F_{n+1} = (F_n - 1)^2 + 1$.

2. Zeigen Sie, dass $F_n \equiv 2 \bmod 5$ für $n \geq 2$.

3. Berechnen Sie die Jacobi-Symbole $\left(\frac{F_n}{5}\right)$ und $\left(\frac{5}{F_n}\right)$.

4. Zeigen Sie, dass $F_n - 2 = \prod_{k=0}^{n-1} F_k$ für $n \geq 1$.

5. Zeigen Sie, dass für $n \neq m$, F_n und F_m teilerfremd sind.

1. $F_{n+1} = 2^{2^{n+1}} + 1 = (2^{2^n})^2 + 1 = (F_n - 1)^2 + 1$. 2. folgt mittels Induktion: für $n = 2$, $F_2 = 2^{2^2} + 1 = 17 = 17 \equiv 2 \bmod 5$; von n nach $n+1$: $F_{n+1} = 2^{2^{n+1}} + 1 = (2^{2^n})^2 + 1$ aber $(2^{2^n}) \equiv 1 \bmod 5$. 3. Es ist nach quadratischer Reziprozität: $\left(\frac{F_n}{5}\right) = \left(\frac{5}{F_n}\right)$. Ferner $F_0 = 3$, $F_1 = 5$, $F_n \equiv 2 \bmod 5$ für $n \geq 2$, und $\left(\frac{3}{5}\right) = -1$, $\left(\frac{5}{5}\right) = 0$, $\left(\frac{2}{5}\right) = -1$. 4. $F_{n+1} = 2^{2^{n+1}} + 1 = (2^{2^n})^2 + 1 = (F_n - 1)^2 + 1$. 5. folgt mittels Induktion: für $n = 1$, $F_1 - 2 = 3 = F_0 = 17$; von n nach $n + 1$: $F_{n+1} - 2 = ((F_n - 1)^2 + 1) - 2 = (F_n - 1)^2 - 1 = F_n(F_n - 2)$. 5) Falls für eine Primzahl p gälte, dass $p \,|F_m$ und $p \,|F_n$, so würde nach Teil 4. folgen, dass $p \,|2$. Das ist aber nicht möglich, denn die F_n sind per Definition ungerade.

3 Bonusaufgabe

Eine (teilweise) korrekte Lösung der folgenden Aufgabe erhöht nicht die Gesamtpunktzahl für Ihre Klausur, aber Sie können damit Ihre Bonuspunktzahl erhöhen.

3.1

In dieser Übung berechnen wir die Summe $S := \sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{p}\right)$, wobei p eine ungerade Primzahl und $f(x) = ax^2 + \cdots$ ein quadratisches Polynom mit Koeffizienten in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ und Diskriminante $\neq 0$ ist.

1. Sei $C = \{(x, y) \in \mathbb{F}_p^2 : y^2 = f(x)\}$. Zeigen Sie, dass

$$\#C = \sum_{\substack{x \in F_p \\ f(x) \neq 0}} \left(1 + \left(\tfrac{f(x)}{p}\right)\right) + \#\{x \in \mathbb{F}_p : f(x) = 0\}.$$

   Folgern Sie $S = \#C - p$.

2. Sei $\widetilde{C} = \{[x : y : z] \in \mathbb{P}^2(\mathbb{F}_p) : y^2 = z^2 f(x/z)\}$. Zeigen Sie, dass $\widetilde{C}$ genau $1 + \left(\frac{a}{p}\right)$ Punkte auf der Ferngeraden $z = 0$ hat.

3. Zeigen Sie, dass $\#C \geq 1$. (Hinweis: Die Abbildung $x \mapsto f(x)$ hat für jedes x in $\mathbb{F}_p$ höchstens zwei Urbilder.) Folgern Sie, dass $\#\widetilde{C} = p + 1$.

4. Folgern Sie aus den beiden vorangehenden Teilen, dass $S = -\left(\frac{a}{p}\right)$.

1. Die erste Identität folgt aus $\#C = \sum_{x \in \mathbb{F}_p} \#\{y \in \mathbb{F}_p : y^2 = f(x)\}$ und $\#\{y \in \mathbb{F}_p : y^2 = f(x)\} = 1 + \left(\frac{f(x)}{p}\right)$ für $x \neq 0$. Die zweite ist eine offensichtliche Umstellung der ersten. 2. Schreibt man $f(x) = ax^2 + bx + c$, so sind die Punkte von $\widetilde{C}$ auf '$z = 0$' die Punkte $[x : y : 0]$, sodass $y^2 = ax^2$. 3. Da $x \mapsto f(x)$ für jedes x höchstens zwei Urbilder hat, muss f strikt mehr als $\frac{p-1}{2}$ Werte annehmen, also mehr Werte als es Nichtquadrate in $\mathbb{F}_p$ gibt. Damit kann $\#C$ durch das Geradenbüschel durch einen Punkt auf C parametrisiert werden, und ein Geradenbüschel hat $p+1$ Punkte (nach einem Satz der Vorlesung). 4. Nach 2. ist $\#C = \#\widetilde{C} - (1 + \left(\frac{a}{p}\right))$, nach 3. daher $\#C = p - \left(\frac{a}{p}\right)$, und somit nach 1. $S = -\left(\frac{a}{p}\right)$.