Zwischenklausur — Elementare Zahlentheorie SoSe 2014

N-P. Skoruppa und Fabien Cléry

15. Mai 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

Seien a und b ganze Zahlen. Dann gilt $\mathbb{Z}a \subseteq \mathbb{Z}b$ genau dann wenn ...

1.2

Eine Teilmenge I eines Ringes R ist ein Ideal, falls ...

1.3

Zu gegebenen ganzen Zahlen a und $m > 0$ gibt es eine ganze Zahl b, sodass $ab \equiv 1 \bmod m$ genau dann, wenn ...

1.4

Es gibt keine ganze Zahl x, sodass $x \equiv 2 \bmod 52$ und $x \equiv -2 \bmod 39$, denn ...

1.5

Sei p eine Primzahl und a eine nicht durch p teilbare ganze Zahl. Die Ordnung von a modulo p ist $< p$, denn ...

2 Methoden

2.1

Zeigen Sie: Ist $2^n + 1$ eine Primzahl, so ist n eine Zweierpotenz.

2.2

Zeigen Sie: Sind a und b teilerfremde ganze Zahlen, so sind auch $a + b$ und ab teilerfremd.

2.3

Berechnen Sie jeweils den Rest von 3^{10} modulo 23, von 3^{100} modulo 23 und von 100^{1000} modulo 13.

2.4

Sei p eine Primzahl. Für die Aufgabe erinnern wir uns, dass für $0 < k < p$ stets p den Binomialkoeffizienten $\binom{p}{k}$ teilt.

1. Zeigen Sie, dass $(a + b)^p \equiv a^p + b^p \bmod p$.
2. Zeigen Sie durch Induktion über a, dass $a^p \equiv a \bmod p$.

2.5

Sei X die Menge aller Primzahlen in der Restklasse $3 + 4\mathbb{Z}$.

(i) Zeigen Sie, dass X nicht leer ist.

(ii) Zeigen Sie, dass das Produkt zweier Zahlen in $1 + 4\mathbb{Z}$ wieder in $1 + 4\mathbb{Z}$ liegt.

Wir wollen zeigen, dass X unendlich ist. Dazu nehmen wir, das Gegenteil an und leiten einen Widerspruch ab. Wir nehmen also an, dass $X = \{p_1, \ldots, p_n\}$.

(iii) Folgern Sie aus (ii), dass $a := 4p_1 \cdots p_n - 1$ durch mindestens ein p_j teilbar ist.

(iv) Andererseits ist es aber unmöglich ist, dass ein p_j die Zahl a teilt. Warum?