Übungen elementare Zahlentheorie

Abt. Reine Mathematik SS 2005 – Blatt 1

Abgabetermin: Mittwoch, 5.05.05 in der Vorlesung

Abgabe ist nur in Zweiergruppen möglich!

---

1. Beweisen Sie ausgehend von den Peanoaxiomen das Assoziativgesetz für die Addition in den natürlichen Zahlen.

2. Zeigen Sie, dass das Peano-Axiom II aus dem Axiom II$'$,
$$0 \notin \nu(\mathbb{N}),$$
und dem Peano-Axiom III folgt.

3. Zeigen Sie: Für $n \in \mathbb{N}, n \geq 2$ gilt
$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} \notin \mathbb{Z}.$$

4. (a) Es sei $H = \{4k+1; k \in \mathbb{N}\}$. Zeigen Sie:
   $(H, \times)$ ist eine kommutative Halbgruppe mit Eins.
   (b) Eine Zahl $p \in H$, $p \neq 1$ heiße H-Primzahl, wenn 1 und p ihre einzigen Teiler aus H sind. Zeigen Sie:
   Jede Zahl aus H ist Produkt von H-Primzahlen.
   (c) Die Produktdarstellung ist nicht eindeutig.
   Hinweis: Betrachten Sie die ersten sieben H-Primzahlen.

Übungen elementare Zahlentheorie

Abt. Reine Mathematik SS 2005 – Blatt 2

Abgabetermin: Mittwoch, 12.05.05 in der Vorlesung

Abgabe ist nur in Zweiergruppen möglich!

---

1. Es seien a, m, s, t natürliche Zahlen.

   (a) Die Zahl $a^{st} - 1$ hat die Faktoren $a^t - 1$ und $\sum_{j=0}^{s-1} a^{jt}$.

   (b) Ist $a^m - 1$, mit $m > 1$, eine Primzahl, so ist m eine Primzahl und $a = 2$.

   Die $M_p = 2^p - 1$, mit p einer Primzahl, heißen Mersennesche Zahlen.

2. Es seien a, b, m, n natürliche Zahlen.

   (a) Ist n ungerade, so teilt $a + b$ die Zahl $a^n + b^n$.

   (b) Ist $a \geq 2$ und $a^m + 1$ prim, so ist a gerade und m eine Potenz von 2 .

   Die $F_n = 2^{2^n} + 1$ heißen Fermatsche Zahlen.

   Die F_k haben wegen des folgenden Satzes von Gauß eine Bedeutung:
   Das regelmäßige m -Eck kann man genau dann mit Zirkel und Lineal konstruieren, wenn

   $$m = 2^t \text{ oder } m = 2^t \cdot p_1 \ldots p_k$$

   ist, wobei die p_i paarweise verschiedene Fermatsche Primzahlen sind.

3. Es sei $p_1 < p_2 < \ldots$ eine Aufzählung aller Primzahlen. Zeigen Sie, dass für die k -te Primzahl gilt

   $$p_k < 2^{2^{k-1}}.$$

4. Zeigen Sie, dass es unendlich viele Primzahlen p gibt mit

   $$p \equiv 5 \mod 6.$$

5. Bestimmen Sie das kleinste $r \in \mathbb{N}$, dass die folgenden Kongruenzen gleichzeitig löst

   $$\begin{aligned} r &\equiv 1 \mod 2 \\ r &\equiv 2 \mod 9 \\ r &\equiv 3 \mod 5 \\ r &\equiv 5 \mod 11 \end{aligned}$$

Übungen elementare Zahlentheorie

Abt. Reine Mathematik SS 2005 – Blatt 3

Abgabetermin: Mittwoch, 19.05.05 in der Vorlesung

Abgabe ist nur in Zweiergruppen möglich!

---

1. Bestimmen Sie den größten gemeinsamen Teiler der Zahlen

$$1581,\ 651,\ 186,\ 78.$$

und stellen Sie ihn als ganzzahlige Linearkombination dieser Zahlen dar.

2. Man zeige, dass für alle natürlichen Zahlen n gilt

$$4501770 \mid n^{97} - n.$$

3. Bestimmen Sie effektiv die letzten 4 Dezimalstellen von 3^{1000} .

4. Bestimmen Sie alle natürlichen Zahlen n mit

   (a) $\varphi(n) = n/2$,

   (b) $\varphi(n) = 2n$,

   (c) $\varphi(n) = 12$.

5. Berechnen Sie mit Maple die kleinste Primitivwurzel modulo $p = 1234567891$.
   Informationen über Maple finden Sie im Internet unter

   `http : //www.mathematik.uni − ulm.de/ReineMath/mitarbeiter/marhenke/ws04/maple.html`

Übungen elementare Zahlentheorie

Abt. Reine Mathematik SS 2005 – Blatt 4

Abgabetermin: Mittwoch, 25.05.05 in der Vorlesung

Abgabe ist nur in Zweiergruppen möglich!

---

1. Die Teilerzahlfunktion $A : \mathbb{N} \to \mathbb{C}$ ordnet einer natürlichen Zahl die Anzahl ihrer verschiedenen Teiler zu. Beweisen Sie die Formel

$$\sum_{d|n} A(d)\mu(d) = (-1)^r$$

mit μ der Möbiusfunktion und r der Anzahl verschiedener Primteiler von n .

2. Berechenen Sie die folgenden Jacobisymbole:

$$\text{(a)} \quad \left(\frac{221}{383}\right), \quad \text{(b)} \quad \left(\frac{14993}{65537}\right), \quad \text{(c)} \quad \left(\frac{3}{p}\right) \quad \text{mit } p \neq 3 \text{ einer Primzahl.}$$

3. Es seien a , b ungerade natürliche Zahlen. Beweisen Sie die folgenden Aussagen:

   (a) Gilt $\left(\frac{x}{b}\right) = 1$ für alle zu b teilerfremden $x \in \mathbb{N}$, so ist b ein Quadrat.

   (b) Gilt $\left(\frac{a}{x}\right) = 1$ für alle zu a teilerfremden $x \in \mathbb{N}$, so ist a ein Quadrat.

   (c) Ist a kein Quadrat, so gibt es unendlich viele Primzahlen p für die a kein quadratischer Rest modulo p ist.
   Hinweis: Hat man $p_1, \ldots, p_n$ bereits gefunden, so existiert ein $y \in \mathbb{N}$ mit

$$y \equiv p_1 \mod 4a\,, \quad y \equiv 1 \mod p_1 \cdots p_n.$$

   Bemerkung: Für unendlich viele Primzahlen p ist a ein quadratischer Rest modulo p .

4. Es sei $f(X)$ das Polynom $(X^2 - 5)(X^2 - 29)(X^2 - 5 \cdot 29) \in \mathbb{Z}[X]$. Zeigen Sie, dass

$$f(X) \equiv 0 \mod m$$

für alle $m \geq 1$ lösbar ist, obwohl $f(X) = 0$ keine ganzzahlige Lösung besitzt.