SS 2003 Prof. Dr. Wolfram Koepf Elemente der Arithmetik und Algebra II
Blatt 6 Ausgabe: 02. Juni 2003
Abgabe: Di 10. Juni 2003, 11 Uhr

1. **RSA-Verschlüsselung**: Wir verwenden das RSA-System. Der Empfänger gibt als öffentlichen Schlüssel $e = 43$, $n = 77$ bekannt. Eine Nachricht N wird als $C = 5$ zum Empfänger gesandt und abgefangen. Was ist N? (4 Punkte)

2. **(Diffie-Hellman Vereinbarung)** Anabell und Brigitte vereinbaren öffentlich die Zahl $g = 3$ und die Primzahl $p = 59$.

   (a) Insgeheim denkt sich Anabell die Zahl 2, Brigitte nimmt 5 als ihre Geheimzahl. Beschreiben Sie an diesem Beispiel, wie nach Diffie-Hellman der gemeinsame Schlüssel zustandekommt. Bestimmen Sie diesen Schlüssel im Verlauf ihrer Beschreibung. (3 Punkte)

   (b) Nun denken sich Anabell und Brigitte insgeheim neue Zahlen aus. Annabell schickt 12 an Brigitte, und Brigitte schickt Anabell eine 22.
   Hans Hacker hört die beiden ab. Übernehmen Sie Hackers Rolle und finden Sie den vereinbarten Schlüssel heraus. (3 Punkte)

   (c) Das geht ja fast im Kopf – und natürlich ganz schnell, wenn Hans obendrein einen leistungsstarken Rechner hätte. Warum gilt dieses Verfahren dennoch nicht als untauglich? (1 Punkt)

3. **(Natürliche Zahlen)** Die natürlichen Zahlen kann man sich wie Hausnummern an einer unendlich langen Straße vorstellen, hat Hans in der Schule gelernt. Hans wohnt in Hausnummer $1a$. Folgerichtig möchte er die natürlichen Zahlen $1, 2, 3 \ldots$ durch eine zweite Reihe $1a, 2a, \ldots$ ergänzen. Der Nachfolger von na aus der zweiten Reihe ist dann $(na)' := (n')a = (n+1)a$, die Nachfolger der "alten" $n \in \mathbb{N}$ sind weiterhin $n' = n + 1$.

   (a) Diese neue Zahlenmenge erfüllt leider nicht mehr die Peano-Axiome für $\mathbb{N}$. Welche der fünf Axiome gelten noch, welche sind verletzt? (3 Punkte)

   (b) Wie kann man die Idee von Hans retten und die zweite Reihe so integrieren, dass die Vereinigung $\{1, 2, \ldots\} \cup \{1a, 2a, \ldots\}$ allen Axiomen genügt? (2 Punkte)