Proseminar Algebra und Geometrie in der Schule
Wintersemester 2011

25. Oktober 2011

7) Aus: Reichel, H., Litschauer, D., Groß, H.: Das ist Mathematik 4. öbv hpt Verlagsgesellschaft, Wien 2002, 2. Auflage 2005.

Aufgabe 301: $\frac{p}{q} + \frac{q}{p} + 2$ *ist stets das Quadrat einer rationalen Zahl, wenn* $p \cdot q$ *eine Quadratzahl ist. Nimm an, dass die Variablen* p *und* q *für natürliche Zahlen* $(p, q \neq 0)$ *stehen!*
Beispiel: $p = 2, q = 8$ ...
1) Überprüfe die Gesetzmäßigkeit an zwei weiteren, selbst gewählten Beispielen!
2) Beweise, dass die Gesetzmäßigkeit allgemein gültig ist!

Diese Aufgabe gehört zum Abschnitt „Verbindung der vier Grundrechnungsarten mit Bruchtermen“. Ist hier mit $\frac{p}{q}$ eine Bruchzahl oder eine rationale Funktion gemeint?

8) Aus: Schneider, G. et al.: Mathematik III HAK/LW. Trauner Verlag, Linz 2008. 2. Auflage 2007, Nachdruck 2008.

Aufgabe 4. 20: Der Börsen-Hai Mackie Messer übermittelt seinem Freund Brown den Geheimtext

11 21 02 39 39 25 15 14 13 25 .

Der öffentliche RSA Schlüssel ist $(55, 23)$*. Knacken Sie den Kode, indem Sie den privaten Schlüssel* $(55, d)$ *ermitteln. Was will Mackie seinem Freund mitteilen?*

9) Aus: Schneider, G. et al.: Mathematik III HAK/LW. Trauner Verlag, Linz 2008. 2. Auflage 2007, Nachdruck 2008.

Aufgabe 4. 21: Rivest, Shamir und Adleman wählten in ihrem bahnbrechenden Aufsatz „A Method for Obtaining Digital Signatures and Public Key Cryptosystems“(1978) als Klartext das Zitat, das Shakespeare Julius Cäsar in den Mund legt: it is all greek to me.

Diesen Text kodierten sie nach der Stellung im Alphabet in eine Klartextzahl, für Zwischenräume setzten sie jeweils Nullen. In Viererblöcken geschrieben lautet die Nachricht:

0920 1900 0112 1200 0718 0505 1100 2015 0013 0500

Für die RSA Verschlüsselung wählten sie die Primzahlen $p = 47$ *und* $q = 59$*, als öffentliche Verschlüsselungszahl wählten sie* $e = 17$ *und berechneten* $d = 157$*.*
a) Zeigen Sie, dass $d = 157$ *die private Entschlüsselungszahl ist.*
b) Verschüsseln und Entschlüsseln Sie den Text nach dem RSA-Verfahren. Verwenden Sie ein CAS (...) oder die Datei RSA.xls von www.trauner.at .

Die Aufgaben sollen nicht nur wie von Schüler/inne/n gelöst werden. Es soll vor allem der mathematische Hintergrund, das nötige Vorwissen und die Strategie zur Lösung dieser Aufgaben erläutert werden. Dabei ist auf einen guten Vortrag zu achten. Im Vortrag soll einfach, aber präzise gesprochen werden, die Argumentation soll lückenlos sein und die Voraussetzungen sollen offengelegt werden. Für jede Aufgabe stehen 15 Minuten zur Verfügung.