Proseminar Algebra und Geometrie in der Schule
Wintersemester 2016/17

24. bzw. 25. Oktober 2016, HS F bzw. HSB 7

Die erste Aufgabe wird gemeinsam gelöst, die anderen zwei Aufgaben werden von Studierenden vorgetragen. Dabei wird der mathematische Hintergrund, das nötige Vorwissen und die Strategie zur Lösung dieser Aufgabe erläutert. Im Vortrag soll möglichst einfach, in gutem Deutsch und präzise gesprochen werden, die Argumentation soll lückenlos sein und die Voraussetzungen sollen offengelegt werden.

7) Aus: Pauer, F., Scheirer-Weindorfer, M., Simon, A.: Mathematik 3. HAK. öbv Wien 2012. 1. Auflage
Aufgabe 811: Berechne mithilfe des erweiterten euklidischen Algorithmus natürliche Zahlen u so, dass $u \cdot a \bmod p = 1$ ist.
c. a=12, p=47
d. a=345, p=11

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

Aufgabe 4. 19: Alice verwendet als öffentlichen RSA-Schlüssel $(33, 13)$.
a) Zeigen Sie, dass $(33, 17)$ *der private Schlüssel von Alice ist.*
b) Alice bekommt von Bob die Nachricht

23 03 24 17 01 08 26 05 31 26 05 01 21 18 14 24 01 13.

Entschlüsseln Sie diese Nachricht.

9) Aus: Pauer, F., Scheirer-Weindorfer, M., Simon, A.: Mathematik 3. HAK. öbv Wien 2012. 2. Auflage 2013.
Aufgabe 942: Berechne die Reste der Potenz a^n nach Division mit Rest durch die Primzahl p.
c. $a = 10, n = 10000, p = 59$

Hinweis: Verwenden Sie den kleinen Satz von Fermat.