Zahlentheorie und Kryptologie, Wintersemester 2012/13
M. Hortmann

Blatt 10

bitte heften Sie dieses Blatt vor Ihre Lösungen

Namen			**Gruppe**	**Tutor**
1a	b	c	**Summe**	**bearbeitet**
1	1	1	2 Pkte=100%	

Aufgabe 1

In der gitterbasierten Kryptographie benutzt man als diskrete Untergruppen von $\mathbb{R}^n$ meist solche, die bereits Untergruppen von $\mathbb{Z}^n$ sind. Ein volldimensionales Gitter im $\mathbb{R}^n$ läßt sich dann darstellen durch eine *n*x*n*-Matrix *A* mit ganzzahligen Einträgen, vom Rang *n*; die Spaltenvektoren von *A* sind eine $\mathbb{Z}$ -Basis des Gitters. Ist $U \in GL_n(\mathbb{Z})$, so beschreibt die Matrix $B=AU$ dasselbe Gitter. Erklärt man jetzt *A* und *B* für äquivalent, so erhält man eine Äquivalenzrelation, deren Äquivalenzklassen genau den volldimensionalen Gittern entsprechen. Wie üblich hätte man gern ein "ausgezeichnetes Element" in jeder Äquivalenzklasse. Hierzu kann die "Hermitesche Normalform" dienen: Eine ganzzahlige *nxn* Matrix vom Rang *n* besitzt hermitische Normalform, wenn unterhalb der Hauptdiagonalen alle Einträge Null sind, alle anderen Einträge nichtnegativ, und in jeder Zeile das Element in der Hauptdiagonale größer ist als die übrigen Elemente der betreffenden Zeile.

Man kann nun zeigen: Zu jeder ganzzahligen *n*x*n*-Matrix *A* vom Rang *n* gibt es eine äquivalente Matrix *H* in hermitischer Normalform.

a) Beweisen Sie: diese Matrix *H* ist eindeutig bestimmt.

In Pari läßt sich die Hermitische Normalform mit der Funktion `mathnf` berechnen.

(Es war für mich verblüffend, daß bei zufälligen Matrizen `A=matrix(10,10,i,j,random(1000))` die Hermitische Normalform `mathnf(%)` meist schon ab der zweiten Zeile trivial ist. Haben Sie eine Idee wieso?)

b) Versuchen Sie zunächst, zufällige ganzzahlige (vollrangige) 2x2, 3x3, 4x4 Matrizen durch Spaltenvertauschungen und Addition ganzzahliger Vielfacher von Spalten zu anderen Spalten, also durch Rechts-Multiplikationen mit Matrizen aus $GL_n(\mathbb{Z})$, auf hermitische Normalform zu bringen[1], um dann einen entsprechenden Algorithmus für *n*x*n*-Matrizen zu formulieren.

1 Sie können sich ja von Pari die Ergebnisse vorsagen lassen.

c) Gegeben sei die folgende 10x10-Matrix in Hermitischer Normalform, deren erste beiden Zeilen `[6140719 247239 1913082 5798183 1140149 4938746 2346277 1310748 2204069 1568617]` und `[0 3 1 1 2 1 1 2 1 2]` sind, während die weiteren Zeilen wie die entsprechenden Zeilen der Einheitsmatrix aussehen.

Finden Sie eine äquivalente Matrix, von deren Koeffizienten keiner den Betrag 10 überschreitet. Damit hätten Sie eine Gitterbasis aus sehr kurzen Vektoren.

Hinweis: Für die Lösung gibt es eine fertige Pari-Funktion[2], die auch in der Reference Card aufgeführt ist. Ihre Aufgabe besteht also im Wesentlichen darin, diese zu finden und anzuwenden. Natürlich sollten Sie dies auch als Anregung zu nehmen, sich mit dem dahinterliegenden Algorithmus zu beschäftigen.

Testen Sie vielleicht auch aus, bei wie großen Matrizen und wie großen Koeffizienten dieser Algorithmus "aufgibt".

2 Eine Lösung in Sage habe ich nicht hinbekommen: die Transformationsmatrizen, die sich in meinen Rechnungen ergaben, hatten immer auch gebrochene und nie, wie bei uns nötig, nur ganzzahlige Einträge.