Blatt 4

Prof. Dr. N-P. Skoruppa und C. Math. L. Fischer Abgabe: Mo, 14-05-2007

Für jede richtig gelöste Aufgabe werden 4 Punkte vergeben.

Aufgabe 1. Entscheiden Sie, welche der folgenden Gruppen zyklisch sind, und beweisen Sie Ihre Behauptungen:

$$\text{(a) } \mathbb{Q}^*, \qquad \text{(b) } (\mathbb{Z}/35\mathbb{Z})^*, \qquad \text{(c) } \left\{ \begin{pmatrix} \cos\frac{\pi l}{6} & -\sin\frac{\pi l}{6} \\ \sin\frac{\pi l}{6} & \cos\frac{\pi l}{6} \end{pmatrix} : l \in \mathbb{Z} \right\}.$$

Aufgabe 2. Eine der vier kleinsten natürlichen Zahlen x mit

$$x^2 \equiv -1 \bmod 3414711517913$$

ist die ISBN-Nummer eines Buches. Von welchem Buch reden wir?

Aufgabe 3. Es sei $n = 295927$, $e = 1003$. Mit diesen Daten werden Texte folgendermassen verschlüsselt: Jedes Zeichen wird durch seinen (dezimalen) ASCII-Zeichencode ersetzt[1], dann wird jeder solcher Zeichencode c durch den Rest von c^e modulo n ersetzt. So ergibt zum Beispiel *Bingo* zunächst die Folge von ASCII-Zeichencodes $\langle 66\ 105\ 110\ 103\ 111\rangle$ und dann nach Potenzieren und Reduzieren modulo n ($66^e \equiv 293465 \bmod n$, $\dots$) den verschlüsselten Text $\langle 293465\ 39846\ 272858\ 41356\ 76026\rangle$. Entschlüsseln Sie den so chiffrierten Text auf der nächsten Seite[2].

Aufgabe 4. Sei p eine Primzahl. Gegeben sei ein Polynom $f(x)$ mit ganzzahligen Koeffizienten und a eine ganze Zahl, sodass gilt: $f(a) \equiv 0 \bmod p$ und $f'(a) \not\equiv 0 \bmod p$. Zeigen Sie: Für jede Potenz p^n gibt es eine ganze Zahl a_n, sodass $f(a_n) \equiv 0 \bmod p^n$ und $a_n \equiv a \bmod p$. Die Zahl a_n ist durch diese Eigenschaften modulo p^n eindeutig bestimmt. (Hinweis: Betrachten Sie die Taylorentwicklung von $f(x)$ um $x = a$.)

Aufgabe 5. Zeigen Sie: Eine natürliche Zahl mit der Dezimaldarstellung $z_n z_{n-1} \dots z_1 z_0$ ($z_j \in \{0, 1, \dots, 9\}$) ist durch 7 teilbar genau dann wenn die Summe $(z_0 + 3z_1 + 2z_2) - (z_3 + 3z_4 + 2z_5) + - \dots$ durch 7 teilbar ist.

---

[1] In PARI/GP kann kann man hierzu bequem `Vecsmall(), StrChr()` benutzen.

[2] Sie können den chiffrierten Text auch von der Webseite zur Vorlesung herunterladen.

Verschlüsselte Nachricht zur Aufgabe 3

98405 82634 101934 226323 231505 293607 76026 136445 167528 101934 128836 226323
76026 178226 226323 99708 39846 54751 87200 39846 272858 41356 200762 39846 54751
82634 39846 272858 41356 226323 231505 293607 39846 128836 101934 226323 272858
200762 128836 136445 101934 293607 54751 226323 178226 293607 76026 128836 226323
103224 76026 128836 231505 76026 54751 39846 87200 101934 226323 272858 200762
128836 136445 101934 293607 54751 226323 113642 272858 99708 226323 76026 178226
226323 293607 101934 54751 76026 167528 46132 39846 272858 41356 226323 87200 82634
101934 226323 167528 113642 87200 87200 101934 293607 226323 39846 272858 87200
76026 226323 87200 82634 101934 39846 293607 226323 231505 293607 39846 128836
101934 226323 178226 113642 103224 87200 76026 293607 54751 226323 39846 54751
226323 212821 272858 76026 240446 272858 226323 87200 76026 226323 136445 101934
226323 76026 272858 101934 226323 76026 178226 226323 87200 82634 101934 226323
128836 76026 54751 87200 226323 39846 128836 231505 76026 293607 87200 113642 272858
87200 226323 113642 272858 99708 226323 200762 54751 101934 178226 200762 167528
226323 39846 272858 226323 113642 293607 39846 87200 82634 128836 101934 87200
39846 103224 101123 226323 226323 231758 87200 226323 82634 113642 54751 226323
101934 272858 41356 113642 41356 101934 99708 226323 87200 82634 101934 226323 39846
272858 99708 200762 54751 87200 293607 111913 226323 113642 272858 99708 226323
240446 39846 54751 99708 76026 128836 226323 76026 178226 226323 113642 272858
103224 39846 101934 272858 87200 226323 113642 272858 99708 226323 128836 76026
99708 101934 293607 272858 226323 41356 101934 76026 128836 101934 87200 101934
293607 54751 226323 87200 76026 226323 54751 200762 103224 82634 226323 113642
272858 226323 101934 276422 87200 101934 272858 87200 226323 87200 82634 113642
87200 226323 39846 87200 226323 240446 76026 200762 167528 99708 226323 136445
101934 226323 54751 200762 231505 101934 293607 178226 167528 200762 76026 200762
54751 226323 87200 76026 226323 99708 39846 54751 103224 200762 54751 54751 226323
87200 82634 101934 226323 231505 293607 76026 136445 167528 101934 128836 226323
113642 87200 226323 167528 101934 272858 41356 87200 82634 101123 101123 101123
226323 226323 96098 200762 293607 87200 82634 101934 293607 291846 226323 87200
82634 101934 226323 99708 39846 41356 272858 39846 87200 111913 226323 76026 178226
226323 87200 82634 101934 226323 54751 103224 39846 101934 272858 103224 101934
226323 39846 87200 54751 101934 167528 178226 226323 54751 101934 101934 128836
54751 226323 87200 76026 226323 293607 101934 24565 200762 39846 293607 101934
226323 87200 82634 113642 87200 226323 101934 46132 101934 293607 111913 226323
231505 76026 54751 54751 39846 136445 167528 101934 226323 128836 101934 113642
272858 54751 226323 136445 101934 226323 101934 276422 231505 167528 76026 293607
101934 99708 226323 178226 76026 293607 226323 87200 82634 101934 226323 54751 76026
167528 200762 87200 39846 76026 272858 226323 76026 178226 226323 113642 226323
231505 293607 76026 136445 167528 101934 128836 226323 54751 76026 226323 101934
167528 101934 41356 113642 272858 87200 226323 113642 272858 99708 226323 54751
76026 226323 103224 101934 167528 101934 136445 293607 113642 87200 101934 99708
101123 226323 167969 291695 113642 293607 167528 226323 96098 293607 39846 101934
99708 293607 39846 103224 82634 226323 76783 113642 200762 54751 54751 291846 226323
230039 39846 54751 24565 200762 39846 54751 39846 87200 39846 76026 272858 101934
54751 226323 68526 293607 39846 87200 82634 128836 101934 87200 39846 103224 113642
101934 291846 226323 144427 189439 44590 144427 56382