Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

WS 2015/16
25. Nov. 2015

Algorithmische Zahlentheorie und Kryptographie

Übungsblatt 6

Aufgabe 21

a) Sei p eine ungerade Primzahl. Man zeige: Die Gleichung

$$ax^2 + bx + c = 0, \qquad p \nmid a,$$

hat im Körper $\mathbb{F}_p$ genau $1 + (\frac{b^2-4ac}{p})$ Lösungen.

b) Man löse in $\mathbb{F}_{97}$ die Gleichung

$$7x^2 + 13x + 71 = 0.$$

Aufgabe 22

Sei p eine ungerade Primzahl. Man zeige:

a) Falls $3 \nmid p-1$, hat für jede zu p teilerfremde ganze Zahl a die Kongruenz $x^3 \equiv a \bmod p$ genau eine Lösung modulo p.

b) Falls $3 \mid p-1$, ist die Kongruenz $x^3 \equiv a \bmod p$ für eine zu p teilerfremde ganze Zahl a genau dann lösbar, wenn $a^{(p-1)/3} \equiv 1 \bmod p$. In diesem Fall gibt es genau 3 Lösungen modulo p.

Aufgabe 23

a) Sei $k \geqslant 3$ und $a \in \mathbb{Z}$ ungerade. Man zeige: Die Kongruenz

$$x^2 \equiv a \bmod 2^k$$

ist genau dann lösbar, wenn $a \equiv 1 \bmod 8$. Wieviele Lösungen gibt es in diesem Fall?

b) Man gebe eine Methode an, wie man aus einer Lösung von $x^2 \equiv a \bmod 2^k$ eine Lösung von $x^2 \equiv a \bmod 2^{k+1}$ konstruieren kann.

c) Man bestimme alle Lösungen der Kongruenz

$$x^2 \equiv 33 \bmod 1024.$$

Aufgabe 24

a) Man beweise: Für jede ganze Zahl $r \geqslant 1$ und jedes ungerade K ist die Abbildung

$$F_K : \mathbb{Z}/2^r \to \mathbb{Z}/2^r, \quad x \mapsto x(2x + K) \bmod 2^r$$

bijektiv.

---

b.w.

b) Sei jetzt $r = 16$. Wir verwenden F_K als Block-Chiffre für Blöcke der Länge 16 Bits = 2 Bytes. Dabei werde ein Paar (b_1, b_2) von Bytes ($b_i \in \{0, 1, \ldots, 255\}$) mit dem Element

$$x := b_1 + b_2 \cdot 2^8 \in \mathbb{Z}/2^{16}$$

identifiziert.

Der folgende Geheimtext der Länge von 152 Bytes entstand aus einem englischen Ascii-Klartext der Länge 150 Bytes durch Verschlüsselung im CBC-Modus. Die ersten zwei Bytes $iv =$ `AFFE` stellen den Initialisierungs-Vektor dar, der Schlüssel ist eine geheime ungerade Zahl mit $1 \leqslant K < 2^{16}$.

```
AFFE 9350 1105 CD29 6BDC BAE2 DC81 26BC A10C 88C4 DE3C 06E6 13FC 6E67 D757
23C7 ED11 83C9 6716 FEBF 3277 AAAC 191B 4F91 AC1F 1838 91B7 3B09 A232 2286
F54A 9E6A F729 BE84 16DD F0F6 7417 B19D DCE3 23D4 ED4B 0B18 D261 8265 2615
AF7C 627D 15C0 7C9C 588F AC5E F321 AE02 6C88 CCA9 0682 C291 CB20 B300 6AB0
86E7 F308 3BCE 4E1D C207 3BC1 140A F40C C4EA AE4B 7279 D7FC 119E F66D CE75
9501
```

Man finde den Klartext und gebe den Schlüssel K an.
