

## Opgaven Getaltheorie en Cryptografie (deel 4)

Inleverdatum: 13 mei 2002

19.a) Laat zien dat 5 een voortbrenger is van  $\mathbb{F}_{37}^*$ .

b) In het sleuteldistributiesysteem van Diffie en Hellman (met  $G = \mathbb{F}_{37}^*$ ,  $\alpha = 5$ ) gebruikt  $A$  de publieke sleutel  $k_A = 17$  en  $B$  de publieke sleutel  $k_B = 23$ . Bepaal de gemeenschappelijke sleutel  $k_{AB}$  van  $A$  en  $B$ .

c) Zij  $G = \mathbb{F}_{37}^*$ ,  $\alpha = 5$  en definieer de functie

$$f : G \rightarrow \mathbb{Z}/36\mathbb{Z} : f(x \bmod 37) = x \text{ als } 1 \leq x \leq 35, f(36 \bmod 37) = 0.$$

In het digitale handtekeningensysteem van El-Gamal gebruikt  $A$  de publieke sleutel  $k_A = 17$ . Bepaal een digitale handtekening van  $A$  bij de boodschap  $m = 19$ , dat wil zeggen bepaal  $a, b$  zodat  $(\alpha^m \cdot k_A^{f(a)})^b \equiv a \pmod{37}$ .

20. Gevraagd wordt (een speciaal geval van de) Pollard-rho methode voor het berekenen van discrete logaritmen uit te werken.

Zij  $G$  een efficiënt berekenbare groep,  $\alpha \in G$ ,  $\beta \in \langle \alpha \rangle$  en zij  $p$  een priemgetal met  $\alpha^p = 1$ . We willen  $x$  bepalen met  $\beta = \alpha^x$ .

Verdeel  $G$  in drie deelverzamelingen  $S_1, S_2, S_3$  met  $1 \notin S_2$ .

Definieer de rijen  $\{x_k\}_{k=0}^\infty, \{a_k\}_{k=0}^\infty, \{b_k\}_{k=0}^\infty$  door

$$x_0 = 1, \quad x_{k+1} = \begin{cases} \beta x_k & \text{als } x_k \in S_1, \\ x_k^2 & \text{als } x_k \in S_2, \\ \alpha x_k & \text{als } x_k \in S_3 \end{cases}$$

$$a_0 = 0, \quad a_{k+1} = \begin{cases} a_k & \text{als } x_k \in S_1, \\ 2a_k \pmod{p} & \text{als } x_k \in S_2, \\ a_k + 1 \pmod{p} & \text{als } x_k \in S_3 \end{cases}$$

$$b_0 = 0, \quad b_{k+1} = \begin{cases} b_k + 1 \pmod{p} & \text{als } x_k \in S_1, \\ 2b_k \pmod{p} & \text{als } x_k \in S_2, \\ b_k & \text{als } x_k \in S_3 \end{cases}$$

- a) Bewijs dat  $x_k = \alpha^{a_k} \beta^{b_k}$  voor  $k = 0, 1, 2, \dots$
- b) Maak aannemelijk dat er indices  $i, j$  zijn met  $0 \leq i < j \leq O(\sqrt{p})$  zodat  $x_i = x_j$  (vat de rij  $\{x_k\}_{k=0}^\infty$  op als elementen van  $\langle \alpha \rangle$  die aselekt worden gekozen en weer teruggelegd).
- c) Maak aannemelijk dat er een index  $l$  is met  $l \leq O(\sqrt{p})$  zodat  $x_{2l} = x_l$ . Leg uit hoe  $x$  kan worden gevonden als  $b_{2l} - b_l$  niet deelbaar is door  $p$ .

**21.** In het standaard Gauss-eliminatiealgoritme voor het oplossen van stelsels lineaire vergelijkingen over lichamen wordt gebruik gemaakt van een "veegprocedure" die als volgt werkt. Neem aan dat er onder het stelsel twee vergelijkingen zijn waarvan de coëfficiënt van  $x_j$  niet gelijk is aan 0, zeg

$$\begin{aligned} L &:= c_{11}x_1 + \dots + c_{1j}x_j + \dots + c_{1n}x_n + d_1 = 0 \\ M &:= c_{21}x_1 + \dots + c_{2j}x_j + \dots + c_{2n}x_n + d_2 = 0 \end{aligned}$$

met  $c_{1j} \neq 0, c_{2j} \neq 0$ . Zij  $M' := M - (c_{2j}/c_{1j})L$ . Als we nu in het oorspronkelijke stelsel  $M$  door  $M'$  vervangen verandert de oplossingsverzameling van het stelsel niet terwijl de coëfficiënt van  $x_j$  in  $M'$  gelijk is aan 0. Merk op dat we moeten delen door  $c_{1j}$ ; daarom is bovengenoemde veegprocedure niet te generaliseren naar stelsels lineaire vergelijkingen over willekeurige ringen in plaats van lichamen.

Door de veegprocedure herhaaldelijk toe te passen kunnen we een gegeven stelsel lineaire vergelijkingen omzetten in een stelsel in driehoeksvorm

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 + \dots &= 0 \\ & a_{22}x_2 + a_{23}x_3 + \dots = 0 \\ & & a_{33}x_3 + \dots = 0 \\ & & & \ddots \end{aligned}$$

waarvan eenvoudig de oplossingsverzameling kan worden bepaald.

In plaats van stelsels lineaire vergelijkingen over een lichaam bekijken we stelsels lineaire vergelijkingen van de vorm

$$(*) \begin{cases} L_1 := a_{11}x_1 + \dots + a_{1n}x_n + b_1 \equiv 0 \pmod{N} \\ L_2 := a_{21}x_1 + \dots + a_{2n}x_n + b_2 \equiv 0 \pmod{N} \\ \vdots \\ L_m := a_{m1}x_1 + \dots + a_{mn}x_n + b_m \equiv 0 \pmod{N} \end{cases}$$

die we willen oplossen in congruentieklassen  $x_1, \dots, x_n \pmod{N}$ . Hier is  $N$  een geheel getal  $> 1$  en zijn de coëfficiënten  $a_{ij}$  gehele getallen met  $0 \leq a_{ij} < N$ .

De bovengenoemde veegprocedure voor de lineaire vormen  $L, M$  werkt niet altijd omdat de optredende coëfficiënten niet inverteerbaar hoeven te zijn in de ring  $\mathbb{Z}/n\mathbb{Z}$ . Daarom geven we een alternatieve veegprocedure.

- a) Bewijs dat de oplossingsverzameling van (\*) onveranderd blijft als:
- (i) voor zekere  $i \in \{1, \dots, m\}$   $L_i$  wordt vervangen door  $L_i + \sum_{\substack{j=1 \\ j \neq i}}^r \lambda_j L_j$  met  $\lambda_j \in \mathbb{Z}$ ;
  - (ii) voor zekere  $i \in \{1, \dots, m\}$   $L_i$  wordt vervangen door  $\mu_i L_i$  met  $\text{ggd}(\mu_i, N) = 1$ .
- Laat aan de hand van een voorbeeld zien dat de oplossingsverzameling van (\*) kan veranderen wanneer we een lineaire vorm  $L_i$  vervangen door  $\mu_i L_i$  waarbij  $\mu_i \neq 0$  en  $\text{ggd}(\mu_i, N) > 1$ .
- b) Zijn

$$\begin{aligned} L &:= c_{11}x_1 + \dots + c_{1j}x_j + \dots + c_{1n}x_n + d_1 \equiv 0 \pmod{N} \\ M &:= c_{21}x_1 + \dots + c_{2j}x_j + \dots + c_{2n}x_n + d_2 \equiv 0 \pmod{N} \end{aligned}$$

twee congruentievergelijkingen uit (\*) waarvan de coëfficiënt van  $x_j$  ongelijk is aan 0. Door zonodig deze vergelijkingen te verwisselen of met  $-1$  te vermenigvuldigen (wat de oplossingsverzameling niet verandert) mogen we aannemen dat  $c_{1j} \geq c_{2j} > 0$ . Definieer:

$$r_{-2} := c_{1j}, \quad r_{-1} := c_{2j}, \quad M_{-2} := L, \quad M_{-1} := M.$$

Voor  $i = 0, 1, 2, \dots$  bereken  $q_i, r_i, M_i$  door:

$$\begin{aligned} r_{i-2} &= q_i r_{i-1} + r_i \quad \text{met } q_i, r_i \in \mathbb{Z}, 0 \leq r_i < r_{i-1}, \\ M_i &\equiv M_{i-2} - q_i M_{i-1} \pmod{N} \end{aligned}$$

(dat wil zeggen van de coëfficiënten van  $M_{i-2} - q_i M_{i-1}$  wordt de rest bij deling door  $N$  genomen).

Bewijs het volgende:

- (i) voor  $i = 0, 1, 2, \dots$  geldt dat de coëfficiënt van  $x_j$  in  $M_i$  gelijk aan  $r_i \pmod{N}$ ;
  - (ii) voor  $i = 0, 1, 2, \dots$  geldt dat de oplossingsverzameling van stelsel (\*) niet verandert wanneer  $L, M$  worden vervangen door  $M_{i-1}, M_i$ ;
  - (iii) er is een index  $i$  zodat de coëfficiënt van  $x_j$  in  $M_i$  gelijk is aan 0.
- Dus door deze procedure kunnen we  $L, M$  vervangen door een paar vergelijkingen zodat van minstens één ervan de coëfficiënt van  $x_j$  gelijk is aan 0.

c) Bepaal alle oplossingen van het onderstaande stelsel lineaire congruentievergelijkingen:

$$2x_1 + 3x_2 + 5x_3 + 6 \equiv 0 \pmod{30}$$

$$5x_1 - 4x_2 - 2x_3 - 1 \equiv 0 \pmod{30}$$

$$3x_1 - 15x_2 + 8x_3 + 2 \equiv 0 \pmod{30}$$

**22.** Zij  $n = pq$  waarbij  $p, q$  twee verschillende priemgetallen zijn van orde van grootte  $10^{150}$  en zij  $e \in \mathbb{Z}$ ,  $e \geq 3$ . Zij  $v \in (\mathbb{Z}/n\mathbb{Z})^* = \{a \in \mathbb{Z} : 1 \leq a \leq n-1, \text{ggd}(a, n) = 1\}$ . Geef een protocol waarmee  $A$   $B$  ervan kan overtuigen dat hij een oplossing kent van  $x^e \equiv v \pmod{n}$  zonder iets over die oplossing prijs te geven aan  $B$ . Maak aannemelijk dat  $A$  slechts met heel kleine kans de controles van  $B$  kan passeren als hij geen oplossing kent van  $x^e \equiv v \pmod{n}$ . Maak verder aannemelijk dat  $B$  uit het protocol geen enkele informatie over  $x$  af kan leiden.

**23.**  $A$  en  $B$  willen op een eerlijke manier met een dobbelsteen gooien over de telefoon. Daartoe kiezen  $A$  en  $B$  aselect  $b_1, b_2 \in \{0, 1, 2, 3, 4, 5\}$  die ze naar elkaar sturen. De uitkomst van het protocol is  $b \equiv b_1 + b_2 \pmod{6}$ . In het onderstaande protocol stuurt  $A$  een codering  $s$  van  $b_1$  naar  $B$  waarmee hij  $b_1$  vastlegt maar waarmee hij zijn keuze voor  $b_1$  geheimhoudt voor  $B$ . Daarna stuurt  $B$  zijn keuze  $b_2$  naar  $A$ .

1)  $B$  kiest twee verschillende priemgetallen  $p, q$  van orde van grootte  $10^{150}$  en berekent  $n = pq$ . Verder kiest  $B$   $x_0, x_1, x_2, x_3, x_4, x_5 \in (\mathbb{Z}/n\mathbb{Z})^*$  en berekent  $y_i \equiv x_i^2 \pmod{n}$  voor  $i = 0, \dots, 5$ . Neem aan dat  $y_0, \dots, y_5$  verschillend zijn.

$B$  stuurt  $n, y_0, \dots, y_5$  naar  $A$  en houdt  $p, q, x_0, \dots, x_5$  geheim.

2)  $A$  kiest aselect  $b_1 \in \{0, 1, 2, 3, 4, 5\}$ .  $A$  kiest aselect en onafhankelijk van  $b_1$   $r \in (\mathbb{Z}/n\mathbb{Z})^*$ .  $A$  berekent  $s \equiv y_{b_1} r^2 \pmod{n}$ .  $A$  stuurt  $s$  naar  $B$ .

3)  $B$  kiest aselect  $b_2 \in \{0, 1, 2, 3, 4, 5\}$  en stuurt  $b_2$  naar  $A$ .

4)  $A$  stuurt  $(b_1, r)$  naar  $B$ .

5)  $B$  controleert dat  $s \equiv y_{b_1} r^2 \pmod{n}$ .

6)  $B$  stuurt  $x_0, \dots, x_5, p, q$  naar  $A$ .

7)  $A$  controleert dat  $n = pq$  en dat  $x_i^2 \equiv y_i \pmod{n}$  voor  $i = 0, 1, 2, 3, 4, 5$ .

8)  $A$  en  $B$  berekenen  $b \equiv b_1 + b_2 \pmod{6}$ .

a) Neem aan dat  $A$  niet in staat is getallen van orde van grootte  $10^{300}$  te factoriseren. Vat  $y_0, \dots, y_5$  op als aselekt gekozen kwadraatrestklassen modulo  $n$ . Laat zien dat  $A$  zich met zijn codering  $s$  vastlegt op  $b_1$ , d.w.z.  $A$  is niet in staat bij gegeven  $s$  twee paren  $(b'_1, r')$ ,  $(b''_1, r'')$  te vinden met  $b'_1, b''_1 \in \{0, 1, 2, 3, 4, 5\}$ ,  $b'_1 \neq b''_1$  en  $s \equiv y_{b'_1} (r'_1)^2 \equiv y_{b''_1} (r''_1)^2 \pmod{n}$ .

b) Laat zien dat  $s$  geen informatie over  $b_1$  bevat.

Preciezer geformuleerd, vat  $y_{b_1}, r, s$  op als waarden van stochastische grootheden respectievelijk  $U, R, S$  op een kansruimte met kansmaat  $P$ . Veronderstel dat  $U$  uniform verdeeld is op  $\{y_0, \dots, y_5\}$ , dat  $R$  uniform verdeeld is op  $(\mathbb{Z}/n\mathbb{Z})^*$ , en dat  $U$  en  $R$  onderling onafhankelijk zijn, dat wil zeggen

$$P(U = y_i) = 1/6 \text{ voor } i = 0, 1, 2, 3, 4, 5,$$

$$P(R = r) = 1/\varphi(n) \text{ voor } r \in (\mathbb{Z}/n\mathbb{Z})^*,$$

$$P(U = u, R = r) = P(U = u)P(R = r) \text{ voor } u \in \{y_0, \dots, y_5\}, r \in (\mathbb{Z}/n\mathbb{Z})^*.$$

Bewijs dan dat  $U$  en  $S$  onderling onafhankelijk zijn, d.w.z.  $P(U = u, S = s) = P(U = u)P(S = s)$  voor  $u \in \{y_0, \dots, y_5\}$  en voor elke kwadraatrestklasse  $s \pmod{n}$ .