Opgaven Getaltheorie en Cryptografie (deel 2)

Inleverdatum: 21 maart 2002

6. Zij $n \in \mathbb{Z}$, $n > 1$. Zij $M_{p,q}(\mathbb{Z})$ de verzameling van $p \times q$-matrices met elementen in $\mathbb{Z}$. Voor $A = (a_{ij})$, $B = (b_{ij}) \in M_{p,q}(\mathbb{Z})$ schrijven we $A \equiv B \pmod{n}$ als $a_{ij} \equiv b_{ij} \pmod{n}$ voor $i = 1, \ldots, p$, $j = 1, \ldots, q$.

a) Zij $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2,2}(\mathbb{Z})$ een matrix met $\gcd(ad - bc, n) = 1$. Definieer

$$A^* := \alpha \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}, \quad \text{met } \alpha(ad - bc) \equiv 1 \pmod{n}.$$

Bewijs dat

$$A \cdot A^* \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{n}, \quad A^* \cdot A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{n}.$$

b) Zij $A \in M_{2,2}(\mathbb{Z})$ als in a) en zij $B \in M_{2,2}(\mathbb{Z})$. Neem aan dat de elementen van A, B behoren tot $\{0, 1, \ldots, n-1\}$. Bewijs dat er een unieke 2×2-matrix X met elementen in $\{0, 1, \ldots, n-1\}$ is zodat

$$AX \equiv B \pmod{n}$$

en dat deze matrix in $O\big((\log n)^2\big)$ bitoperaties kan worden gevonden.

7. Gegeven zijn oneven getallen a, b met $a > b \geq 3$. Definieer de paren (r_i, s_i) $(i = 0, 1, 2, \ldots)$ recursief als volgt:

$$r_0 := b, \quad s_0 := \text{rest van } a \text{ bij deling door } b;$$

$$\big(r_{i+1}, s_{i+1}\big) := \begin{cases} \big(\max(\frac{r_i}{2}, s_i), \min(\frac{r_i}{2}, s_i)\big) & (r_i \text{ even, } s_i \text{ oneven}); \\ \big(r_i, \frac{s_i}{2}\big) & (r_i \text{ oneven, } s_i \text{ even}); \\ \big(\max(\frac{r_i - s_i}{2}, s_i), \min(\frac{r_i - s_i}{2}, s_i)\big) & (r_i, s_i \text{ beide oneven}). \end{cases}$$

Zij i_0 de eerste index i met $s_i = 0$.

a) Bewijs dat voor $i = 0, 1, 2, \ldots, i_0$ het volgende geldt:
$\gcd(r_i, s_i) = \gcd(a, b)$; $0 \leq s_i \leq r_i \leq b$; r_i, s_i zijn niet beide even; $r_{i+1}s_{i+1} \leq \frac{1}{2}r_i s_i$.
Laat verder zien dat $r_{i_0} = \gcd(a, b)$.

b) We berekenen $\gcd(a, b)$ door achtereenvolgens de paren (r_i, s_i) $(i = 0, 1, 2, \ldots, i_0)$ te berekenen. Laat zien dat dit $O(\log a \cdot \log b)$ bitoperaties kost.

8. Bepaal de oplossingen van de volgende congruenties met de op het college behandelde methoden:

a) $x^2 \equiv 18 \pmod{73}$;

b) $x^2 \equiv 3 \pmod{13^4}$.

9. Zij $a \equiv 1 \pmod 8$.

a) Definieer de rijen $\{x_t\}_{t=0}^{\infty}$, $\{z_t\}_{t=0}^{\infty}$ door:

$$x_0 := 1;$$
$$x_t z_t \equiv -\frac{x_t^2 - a}{2^{2^t+2}} \pmod{2^{2^t}}, \quad x_{t+1} = x_t + 2^{2^t+1} z_t \quad \text{voor } t = 0, 1, 2, \ldots.$$

Bewijs dat $x_s^2 \equiv a \pmod{2^{2^s+2}}$ voor alle $s \geq 0$.

b) Zij $k \geq 3$ en $c^2 \equiv a \pmod{2^k}$. Bewijs dat de oplossingen van $x^2 \equiv a \pmod{2^k}$ worden gegeven door $x \equiv \pm c \pmod{2^k}$, $x \equiv 2^{k-1} \pm c \pmod{2^k}$.

10. Zij $n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$ met $p_1, \ldots, p_t$ verschillende priemgetallen en $k_1 > 0, \ldots, k_t > 0$. Zij $f \in \mathbb{Z}[X]$. Uit elementaire eigenschappen van congruenties volgt dat
$x \equiv y \pmod n \Longrightarrow f(x) \equiv f(y) \pmod n$.

a) Zij $S_f(n)$ de verzameling van alle restklassen $x \pmod n$ met $f(x) \equiv 0 \pmod n$. Zij $R_f(n)$ het aantal restklassen $x \pmod n$ met $f(x) \equiv 0 \pmod n$. Bewijs dat er een bijectieve afbeelding is van $S_f(p_1^{k_1}) \times \cdots \times S_f(p_t^{k_t})$ naar $S_f(n)$ en leid daaruit af dat

$$R_f(n) = R_f(p_1^{k_1}) \cdots R_f(p_t^{k_t}).$$

(**Aanwijzing.** Volgens de Chinese reststelling hoort er bij elk stel restklassen $x_1 \pmod{p_1^{k_1}}, \ldots, x_t \pmod{p_t^{k_t}}$ precies één restklasse $x \pmod n$ zodat $x \equiv x_i \pmod{p_i^{k_i}}$ voor $i = 1, \ldots, t$. Laat zien dat de afbeelding $(x_1, \ldots, x_t) \mapsto x$ de gevraagde bijectieve afbeelding geeft.)

b) Zij a een kwadraatrest modulo n, d.w.z. $\text{ggd}(a,n) = 1$ en $x^2 \equiv a \pmod{n}$ is oplosbaar. Bepaal het aantal oplossingen in restklassen modulo n van $x^2 \equiv a \pmod{n}$.

11. In het RSA-systeem kiest elke gebruiker A twee grote priemgetallen p_A, q_A en berekent $n_A = p_A q_A$. Verder kiest A een getal e_A met $e_A > 0$ en $\text{ggd}(e_A, \lambda(n_A)) = 1$, waarbij $\lambda(n_A) = \text{kgv}(p_A - 1, q_A - 1)$, en berekent d_A met $e_A d_A \equiv 1 (\text{mod } \lambda(n_A))$. De vercijferoperatie en ontcijferoperatie van A zijn gegeven door respectievelijk

$$E_A(m) \equiv m^{e_A} \pmod{n_A}, \quad 0 \leq E_A(m) < n_A\,,$$
$$D_A(c) \equiv c^{d_A} \pmod{n_A}, \quad 0 \leq D_A(m) < n_A\,,$$

Wanneer A een vercijferde boodschap voorzien van zijn digitale handtekening naar B wil sturen kiest hij een klare tekst m met $0 < m < \min(n_A, n_B)$ en berekent

$$c' := \begin{cases} D_A E_B(m) & \text{als } n_B < n_A, \\ E_B D_A(m) & \text{als } n_A < n_B. \end{cases}$$

A stuurt c' naar B en B berekent m. Laat zien dat

$$m = \begin{cases} D_B E_A(c') & \text{als } n_B < n_A, \\ E_A D_B(c') & \text{als } n_A < n_B. \end{cases}$$

12.*a)* Zijn a, n positieve gehele getallen met $n > 1$. Bewijs dat het aantal getallen $x \in \mathbb{Z}$ met $ax \equiv 0 \pmod{n}$ en $0 \leq x < n$ gelijk is aan $\text{ggd}(a, n)$.

b) Zij p een priemgetal en zij e een positief geheel getal.
Bewijs dat $\#\{a \in \mathbb{F}_p : a^e = a\} = 1 + \text{ggd}(e-1, p-1)$.

c) Zij E_A de RSA-vercijferoperatie van A zoals gedefinieerd in opgave 11. Een klare tekst m heet een *fixpunt* van E_A als $E_A(m) = m$. Een fixpunt kan worden opgevat als een klare tekst die bij het vercijferen gelijk blijft. Dus het is uiterst onwenselijk dat E_A veel fixpunten heeft.
Laat zien dat het aantal fixpunten van E_A gelijk is aan

$$\Big(1 + \text{ggd}(e_A - 1, p_A - 1)\Big) \cdot \Big(1 + \text{ggd}(e_A - 1, q_A - 1)\Big).$$

Voor welke e_A is het aantal fixpunten minimaal?