Opgaven Getaltheorie en Cryptografie (deel 3)

Inleverdatum: 11 april 2002

13.*a)* Zij p een priemgetal met $p \equiv 3 \pmod 4$ en zij a een kwadraatrest modulo p. Bekend is dat $x^2 \equiv a \pmod p$ precies twee oplossingen in restklassen modulo p heeft, zeg $\pm x_1 \pmod p$. Bewijs dat één van deze oplossingen een kwadraatrestklasse, en één een niet-kwadraatrestklasse modulo p is.

b) Zij $n = pq$ waarbij p, q twee verschillende priemgetallen zijn met $p \equiv q \equiv 3 \pmod 4$. Zij a een kwadraatrestklasse modulo n. Bewijs dat er precies één restklasse $x \pmod n$ bestaat zodat $x^2 \equiv a \pmod n$ en zodat x zelf een kwadraatrestklasse modulo n is. (Dit is het idee achter het cryptosysteem van Blum en Goldwasser).

c) Geef een voorbeeld waaruit blijkt dat b) niet juist is wanneer $p \equiv q \equiv 1 \pmod 4$.

14. Zij $n = p_1 p_2 \cdots p_t$ een Carmichael-getal, waarbij $p_1, \ldots, p_t$ verschillende priemgetallen zijn met $p_1 < p_2 < \cdots < p_t$.

a) Bewijs dat $(p_i - 1) \mid \Big(\prod_{\substack{j=1 \\ j \neq i}}^{t} p_j \Big) - 1$ voor $i = 1, \ldots, t$.

b) Bewijs dat er geen Carmichael-getallen zijn die uit twee priemgetallen zijn samengesteld.

c) Bepaal alle Carmichael-getallen ≤ 600.

15.*a)* Als n een priemgetal is dan geldt voor elke $a \in \mathbb{Z}$ met $\gcd(a, n) = 1$ dat $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod n$. Laat zien dat wanneer n samengesteld is, er een getal a is met $\gcd(a, n) = 1$ en $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod n$.
Aanwijzing. Maak onderscheid tussen de volgende twee gevallen:
1) n is geen Carmichael-getal;
2) n is wel een Carmichael-getal.
(Schrijf $n = p_1 p_2 \cdots p_t$ met $p_1, \ldots, p_t$ verschillende oneven priemgetallen. Zij b een niet-kwadraatrest modulo p_1 en neem a met $a \equiv b \pmod{p_1}$, $a \equiv 1 \pmod{p_i}$ $(i = 2, 3, \ldots, t)$.)

b) Zij n een samengesteld getal. Bewijs dat er hoogstens $\frac{1}{2}\varphi(n)$ getallen a zijn met $a \in \{1, \ldots, n-1\}$, $\gcd(a, n) = 1$ en $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod n$.

Opmerking. De *samengesteldheidstest van Solovay-Strassen* voor een gegeven getal n is om een aantal getallen $a \in \{1, \ldots, n-1\}$ te kiezen en voor deze getallen na te gaan of $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}$. Het getal n wordt samengesteld verklaard als er een a wordt gevonden die niet aan deze test voldoet, en priem als alle gekozen a aan de test voldoen. Wanneer N getallen zijn gekozen dan is de kans dat een samengesteld getal ten onrechte priem wordt verklaard is hoogstens 2^{-N}. De test van Solovay-Strassen is een voorloper van de test van Rabin-Miller.

16. Het n-de Fermat-getal F_n is gedefinieerd door $F_n = 2^n + 1$.

a) Bewijs dat $F_n | F_{mn}$ voor elk oneven getal m.

b) Bewijs: als F_n een priemgetal is dan is $n = 2^m$ voor zeker niet-negatief geheel getal m.

c) Zij $n \in \mathbb{N}$. Bewijs dat $\left(\frac{3}{F_n}\right) = -1$ als n even is en $3 | F_n$ als n oneven is.

d) Bewijs de *priemtest van Pépin* voor Fermat-getallen F_n met $n \geq 2$:
F_n is een priemgetal $\iff 3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.

17.*a)* Zij $p > 2$ een priemgetal en zijn a, b, c gehele getallen met $a, b, c \in \{0, 1, \ldots, p-1\}$, $\text{ggd}(a, p) = 1$. Definieer de rij $\{x_k\}_{k=0}^{\infty}$ door

$$x_0 = c, \quad x_{k+1} \equiv a x_k + b \pmod{p}, \;\; 0 \leq x_{k+1} < p \;\; (k = 0, 1, 2, \ldots).$$

Bewijs dat $x_k \equiv a^k \cdot c + \frac{a^k - 1}{a-1} \cdot b \pmod{p}$.

b) Bewijs dat de rij $\{x_k\}_{k=0}^{\infty}$ periodiek is als $\text{ggd}((a-1)c + b, p) = 1$. Voor welke drietallen (a, b, c) is de periode maximaal en wat is de maximale periode?

c) Beschouw de volgende variant van de Pollard-rho factorisatiemethode.
Zij n het te factoriseren getal;
kies $a, b, c \in \{0, 1, \ldots, n-1\}$;
bereken $x_0 := c, \quad x_{k+1} \equiv a x_k + b \pmod{n}$, $(k = 0, 1, 2, \ldots)$;
voor elke even index $k = 2l$, bereken $\text{ggd}(x_{2l} - x_l, n)$;
als de ggd 1 is, ga verder; als de ggd n is begin opnieuw met andere a, b, c; als de ggd ongelijk is aan 1 of n hebben we een factor gevonden.

Leg uit waarom deze variant van de Pollard-rho-methode waarschijnlijk minder goed werkt dan de oorspronkelijke Pollard-rho-methode.

18. Gegeven is een getal n dat deelbaar is door een priemgetal p zodat $p+1$ is samengesteld uit priemgetallen $\leq K$. In deze opgave geven we een methode om n te factoriseren (de zogenaamde $(p+1)$-methode). Voor deze methode moeten we werken in de restklassenring $\mathbb{Z}[X]/(n, X^2 - A)$ waarbij $\text{ggd}(A, n) = 1$.

a) Bewijs het volgende:
(i) elke restklasse in deze ring kan worden gerepresenteerd door $a+bX$ met $a, b \in \mathbb{Z}$, $0 \leq a, b < n$;
(ii) $(a + bX)(c + dX) \equiv (ac + bdA) + (ad + bc)X \pmod{(n, X^2 - A)}$;
(iii) als A een niet-kwadraatrest modulo p is, dan is er een surjectief ringhomomorfisme

$$\varphi : \ \mathbb{Z}[X]/(n, X^2 - A) \to \mathbb{F}_{p^2} : \ \ a + bX \mapsto \overline{a} + \overline{b}\alpha \,,$$

waarbij $\overline{x}$ het beeld is van x onder $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ en waarbij α een nulpunt is van $X^2 - \overline{A}$.

b) Definieer

$$K_0 := \Big(\prod_{q:\, q \leq K} q \Big)^{[\log n / \log 2]},$$

waarbij het product wordt genomen over alle priemgetallen $q \leq K$.
Zij $\beta \in \mathbb{F}_{p^2}^*$. Bewijs dat $\beta^{p+1} \in \mathbb{F}_p^*$ en dat $\beta^{K_0} \in \mathbb{F}_p^*$.

c) Zij A een niet-kwadraatrest modulo p en zijn $a, b \in \mathbb{Z}$ getallen met $\text{ggd}(a, n) = \text{ggd}(b, n) = 1$. Bewijs dat

$$(a + bX)^{K_0} \equiv a^* + b^* X \pmod{(n, X^2 - A)} \quad \text{met } p | b^*.$$

Opmerking. De $(p+1)$-methode werkt nu als volgt:
1) Kies aselect $A \in \{1, 2, \ldots, n-1\}$. Bereken $\text{ggd}(A, n)$. Als deze ggd ongelijk is aan 1 dan hebben we een factor gevonden. Neem verder aan dat $\text{ggd}(A, n) = 1$.
2) Kies aselect $a, b \in \{1, 2, \ldots, n-1\}$. Bereken $\text{ggd}(a, n)$, $\text{ggd}(b, n)$. Als één van deze ggd's ongelijk is aan 1 dan hebben we een factor gevonden. Neem verder aan dat beide ggd's gelijk zijn aan 1.
3) Bepaal $a^*, b^* \in \{0, 1 \ldots, n-1\}$ zodat

$$(a + bX)^{K_0} \equiv a^* + b^* X \pmod{(n, X^2 - A)}.$$

4) Bereken $\text{ggd}(n, b^*)$. Als deze ggd gelijk is aan 1 ga terug naar 1) en probeer een andere A; als deze ggd gelijk is aan n ga terug naar 2) en probeer andere b, c; als deze ggd ongelijk is aan 1 of n dan hebben we een factor gevonden.

In onderdeel c) is aangetoond dat $\text{ggd}(n, b^*)$ deelbaar is door p als A een niet-kwadraatrest modulo p is; dus als de uitkomst van de ggd gelijk is aan 1 dan was A kennelijk een kwadraatrest modulo p en moet er een andere A worden gekozen. Als de uitkomst van de ggd gelijk is aan n dan was A kennelijk goed gekozen maar a, b niet; dus dan moeten andere a, b worden gekozen.