2.6 Calculul radacinilor primitive

Pana acum am caracterizat toate numerele n care admit radacini primitive si am dat si structura generala a grupului $U(\mathbb{Z}_n)$. Observam, insa, ca demonstratiile pentru existenta acestor radacini nu sunt constructive, ci pur existentiale - nu ni se indica nicio metoda de calcul pentru determinarea acestor radacini. Din pacate, nu este cunoscut un algoritm eficient pentru a determina radacinile primitive.
Mai jos, vom prezenta un algoritm destul de simplu pentru a gasi cea mai mica radacina primitiva modulo p unde $p \geq 3$ este numar prim. Vom da intai rezultatul care sta la baza algoritmului:

Propozitia 2.6.1. *Fie p un numar prim si $q_1, q_2, \ldots, q_k$ toti divizorii primi distincti ai lui $p-1$. Atunci r este radacina primitiva modulo p daca si numai daca*

$$r^{(p-1)/q_i} \not\equiv 1 \pmod{p},$$

oricare ar fi $1 \leq i \leq k$.

Demonstrație. " $\Longrightarrow$ ": Daca r este radacina primitiva, atunci $p-1$ este cel mai mic numar pentru care $r^t \equiv 1 \pmod{p}$ si rezultatul este evident.
" $\Longleftarrow$ ": Fie un astfel de r cu proprietatea ca

$$r^{(p-1)/q_i} \not\equiv 1 \pmod{p},$$

pentru orice i. Notam $t = \mathrm{ord}_p(r)$. Vom arata ca $t = p-1$. Este evident ca t divide $p-1$, asadar putem scrie $p-1 = tu$, cu u natural. Presupunem prin absurd ca $t \neq p-1$, si acest fapt implica $u > 1$. Cum u divide $p-1$, exista un indice i astfel incat q_i divide u. Putem deci scrie $u = q_i v$, si apoi $p-1 = tq_i v$. Asadar t divide $(p-1)/q_i$, si conform teoremei 2.1.1 avem ca

$$r^{(p-1)/q_i} \equiv 1 \pmod{p}$$

contradictie. Deci trebuie ca $t = p-1$, asadar r este radacina primitiva modulo p. $\square$

Folosind acest rezultat, putem determina cea mai mica radacina primitiva modulo p printr-o cautare directa. Incercam, pe rand, numerele $2, 3, 4, \ldots$ si vedem daca gasim unul care satisface conditia din propozitia anterioara. Primul numar astfel gasit este chiar radacina primitiva cautata. Iata algoritmul mai jos:

1. Daca $p = 2$, atunci afiseaza 1 si incheie. Altfel, seteaza $a \longleftarrow 2$.

2. (Descompunerea in factori) Calculeaza $q_1, q_2, \ldots, q_k$ divizorii primi ai lui $p - 1$.

3. (Ridicare la putere) Verifica daca $a^{(p-1)}/q_i \not\equiv 1 \pmod{p}$ pentru fiecare $1 \leq i \leq k$. In caz afirmativ, afiseaza a si incheie.

4. (Incrementeaza a) Seteaza $a \longleftarrow a + 1$.

Fara a intra in detalii, mentionam ca descompunerea in factori primi a unui numar intreg este o problema "dificila", in sensul ca nu este cunoscut niciun algoritm eficient care sa realizeze descompunerea numerelor foarte mari. De aceea, nici algoritmul de mai sus nu poate fi considerat eficient.