Et notat om modular exponentation-algoritmen
— siden jeg to ganger har mislyktes i å forklare det i forelesningene
Åsmund Eldhuset
30.01.2010

La oss si at vi blir bedt om å finne $9^{78} \bmod 25$. Siden 25 ikke er et primtall, kan vi ikke bruke Fermats lille teorem. Hvis man føler seg avansert, kan man bruke Eulers teorem (`http://en.wikipedia.org/wiki/Euler's_theorem`), men det er ikke pensum. Da må man ty til algoritmen som er gitt på side 226 i boken i stedet. Den illustreres best ved et eksempel. Tanken er å først skrive eksponenten som en sum av toerpotenser (merk at vi skal bruke toerpotenser uansett hva grunntallet og eksponenten i potensen er): $78 = 64 + 8 + 4 + 2$. Da kan vi splitte opp uttrykket vårt slik: $9^{78} \bmod 25 = 9^{64+8+4+2} \bmod 25 = 9^{64} \cdot 9^8 \cdot 9^4 \cdot 9^2 \bmod 25 = (9^{64} \bmod 25)(9^8 \bmod 25)(9^4 \bmod 25)(9^2 \bmod 25) \bmod 25$ (på grunn av regelen om at $ab \bmod m = (a \bmod m)(b \bmod m) \bmod m$). Nå har vi altså skaffet oss en haug av potenser hvor grunntallene er 9 (det opprinnelige grunntallet vårt) og eksponentene er forskjellige toerpotenser. Det flotte med dette er at de større potensene kan regnes ut fra de mindre. Den generelle regelen ser slik ut (fortsatt er det ingen magi involvert; vi bruker bare vanlige potensregler og modulo-regler):

$$\begin{aligned} a^{2n} \bmod m &= (a^n)^2 \bmod m = (a^n)(a^n) \bmod m = (a^n \bmod m)(a^n \bmod m) \bmod m \\ &= (a^n \bmod m)^2 \bmod m \end{aligned}$$

Så hvis vi vet $a^n \bmod m$, kan vi finne $a^{2n} \bmod m$. Hvis vi begynner med $a^1 \bmod m$, kan vi da finne a opphøyd i en hvilken som helst toerpotens (modulo m). I eksempelet vårt fungerer det slik:

$$\begin{aligned} 9^1 \bmod 25 &= 9 \\ 9^2 \bmod 25 &= 9^{2 \cdot 1} \bmod 25 = (9^1 \bmod 25)^2 \bmod 25 = 9^2 \bmod 25 = 6 \\ 9^4 \bmod 25 &= 9^{2 \cdot 2} \bmod 25 = (9^2 \bmod 25)^2 \bmod 25 = 6^2 \bmod 25 = 11 \\ 9^8 \bmod 25 &= 9^{2 \cdot 4} \bmod 25 = (9^4 \bmod 25)^2 \bmod 25 = 11^2 \bmod 25 = 21 \\ 9^{16} \bmod 25 &= 9^{2 \cdot 8} \bmod 25 = (9^8 \bmod 25)^2 \bmod 25 = 21^2 \bmod 25 = 16 \\ 9^{32} \bmod 25 &= 9^{2 \cdot 16} \bmod 25 = (9^{16} \bmod 25)^2 \bmod 25 = 16^2 \bmod 25 = 6 \\ 9^{64} \bmod 25 &= 9^{2 \cdot 32} \bmod 25 = (9^{32} \bmod 25)^2 \bmod 25 = 6^2 \bmod 25 = 11 \end{aligned}$$

Merk at med en gang man får et svar som man allerede har fått, vil svarene begynne å repetere seg ($9^{128} \bmod 25 = 21$, $9^{256} \bmod 25 = 16$ osv.), så der kan man spare litt tid hvis man er heldig.

Nå er vi klare til å sette sammen det endelige svaret, for helt i starten fant vi jo ut at $9^{78} \bmod 25 = (9^{64} \bmod 25)(9^8 \bmod 25)(9^4 \bmod 25)(9^2 \bmod 25) \bmod 25$, og vi har nå funnet verdiene av alle delene av dette uttrykket — så svaret er $11 \cdot 21 \cdot 11 \cdot 6 \bmod 25 = 15246 \bmod 25 = 21$.