OPPKLARING OM CARMICHAEL-TALL

Side 91 i Burton er forvirrende fordi man her uten noen nærmere forklaring bruker to ulike definisjoner av Carmichael-tall:

(1) Et sammensatt heltall n er et Carmichael-tall hvis $a^{n-1} \equiv 1 \pmod{n}$ holder for alle a slik at $\gcd(a,n) = 1$.
(2) Et sammensatt heltall n er et Carmichael-tall hvis $a^n \equiv a \pmod{n}$ holder for alle heltall a.

Det er klart at hvis betingelsen i (2) holder, så holder automatisk betingelsen i (1). Men hva med den motsatte implikasjonen? Vi kan vise at den følger av *Korselts kriterium*: n er et Carmichael-tall i henhold til definisjon (1) hvis og bare hvis (i) n er kvadratfri og (ii) $p|n$ medfører at $(p-1)|(n-1)$.

La oss først vise at Korselts kriterium bringer oss fra (1) til (2). Siden n er kvadratfri, holder det å vise at $a^n \equiv a \pmod{p}$ holder for alle primtall p som deler n. Hvis $p|a$, holder dette trivielt. I motsatt fall har vi $a^{p-1} \equiv 1 \pmod{p}$ ved Fermats teorem og dermed $a^{n-1} \equiv 1 \pmod{p}$ ved del (ii) av Korselts kriterium. Ganger vi denne kongruensen med a, får vi den ønskede kongruensen $a^n \equiv a \pmod{p}$.

Det gjenstår å etablere Korselts kriterium. La oss først anta at n er et Carmichael-tall i henhold til (1). Vi viser først at n er kvadratfri. La oss anta at det finnes et primtall p slik at $n = p^k m$ med $k \geq 2$ og $p \nmid m$. Ved det kinesiske restteoremet finnes an a slik at $a \equiv 1 + p \pmod{p^k}$ og $a \equiv 1 \pmod{m}$. Det betyr spesielt at $\gcd(a,n) = 1$, så vi har $a^{n-1} \equiv 1 \pmod{n}$ og dermed $a^{n-1} \equiv 1 \pmod{p^2}$. Bruker vi binomialteoremet på kongruensen $a \equiv 1 + p \pmod{p^2}$, får vi $a^{n-1} \equiv 1 + (n-1)p \pmod{p^2}$. Dermed har vi $(n-1)p \equiv 0 \pmod{p^2}$ som er gir en motsigelse.

Vi vil så vise at $(p-1)|(n-1)$. Siden n er kvadratfri, er p og n/p relativt primiske. Nå bruker vi noe vi skal lære i avsnitt 8.2: Det finnes et heltall b slik at $b^k \not\equiv 1 \pmod{p}$ for $k = 1, \ldots, p-2$. Gitt dette bruker vi nok en gang kinesisk restteorem: Vi finner a slik at $a \equiv b \pmod{p}$ og $a \equiv 1 \pmod{n/p}$. Siden $\gcd(a,n) = 1$, gir definisjonen i (1) at $a^{n-1} \equiv 1$. Men det betyr at $(p-1)|(n-1)$ ved vårt valg av b.

Den motsatte implikasjonen i Korselts kriterium er enklere: Vi antar at n er et kvadratfritt sammensatt helttall og at vi har $(p-1)|(n-1)$ når $p|n$. Hvis $\gcd(a,n) = 1$, gir Fermats teorem at $a^{p-1} \equiv 1 \pmod{p}$. Vi har dermed $a^{p-1} \equiv 1 \pmod{p}$ siden $(p-1)|(n-1)$. Siden n er kvadratfri og dette holder for alle p som deler n, følger av dette at $a^{n-1} \equiv 1 \pmod{n}$.

Date: 26. september 2021.