getaltheorie hw1

Rocco van Vreumingen

6 oktober 2016

2.6)
Er geldt

$$\phi(mn) = mn \prod_{p_i|mn} \frac{p_i - 1}{p_i}$$

$$= mn\left(\prod_{p_i|n} \frac{p_i - 1}{p_i} \cdot \prod_{p_i|m} \frac{p_i - 1}{p_i}\right) / \prod_{p_i|m \ en \ p_i|n} \frac{p_i - 1}{p_i}$$

Dit, (*), gaan we zometeen verder herschrijven. Als we nu ggd(m, n) schrijven als product van priemen, zeg $q_1^{e_1}...q_k^{e_k}$, dan is

$$\phi(ggd(m, n)) = q_1^{e_1}...q_k^{e_k} \prod_{i=1}^{k} \frac{q_i - 1}{q_i}$$

Dus bij (*) is $1/\prod_{p_i|m \ en \ p_i|n} \frac{p_i-1}{p_i}$ gelijk aan ggd$(m, n)/\phi($ggd$(n, m))$. We krijgen nu

$$\phi(mn) = mn\left(\prod_{p_i|n} \frac{p_i - 1}{p_i} \cdot \prod_{p_i|m} \frac{p_i - 1}{p_i}\right) / \prod_{p_i|m \ en \ p_i|n} \frac{p_i - 1}{p_i}$$

$$= m \prod_{p_i|m} \frac{p_i - 1}{p_i} * n \prod_{p_i|n} \frac{p_i - 1}{p_i} \big(ggd(m, n)/\phi(ggd(n, m))\big)$$

$$= \phi(m)\phi(n)\big(ggd(m, n)/\phi(ggd(n, m))\big)$$

2.13) Er geldt $(p-1)! = 1 * 2 * 3 * ... * ((p-1)/2) * ((p+1)/2) * ... * (p-1)$. In modulo p is dat $1*2*3*...*((p-1)/2)*-((p-1)/2))*...*-1 = ((p-1)/2)!^2$ (hier zit geen minteken voor omdat $p-1$ een veelvoud van 4 is).
Omdat $(p-1)!$ in modulo p gelijk is aan -1 (Wilson), moet ook $((p-1)/2)!^2 \equiv -1(mod\ p)$.

1.9) Zo'n perfect getal kun je niet zo ontbinden in priemfactoren dat een daarvan een 2 is, anders was het perfecte getal even.
Stel eerst dat de priemontbinding gelijk is aan p^k, $k \in \mathbb{N}$ en p een oneven priem.

Per definitie van perfectie moet gelden $p^k = \sum_{i=0}^{k-1} p^i = \frac{p^k-1}{p-1} < p^k$, tegenspraak.

Stel nu dat de priemontbinding gelijk is aan $p^k q^\ell$, $k, \ell \in \mathbb{N}$ en p, q oneven priem.
Dan krijgen we

$$
\begin{aligned}
p^k q^\ell &= \sum_{i=0}^{k-1} p^i \sum_{j=0}^{\ell-1} q^j + p^k \sum_{j=0}^{\ell-1} q^j + q^\ell \sum_{i=0}^{k-1} p^i \\
&= (\frac{p^k-1}{p-1})(\frac{q^\ell-1}{q-1}) + p^k(\frac{q^\ell-1}{q-1}) + q^\ell(\frac{p^k-1}{p-1}) \\
&= \big(\frac{p^k-1}{p-1} + p^k\big)\big(\frac{q^\ell-1}{q-1} + q^\ell\big) - p^k q^\ell \\
&\leq \big(\frac{p^k}{p-1} + p^k\big)\big(\frac{q^\ell}{q-1} + q^\ell\big) - p^k q^\ell \\
&= \frac{p}{p-1}\frac{q}{q-1} p^k q^\ell - p^k q^\ell < \frac{3}{2} * \frac{5}{4} p^k q^\ell - p^k q^\ell \\
&= (7/8) p^k q^\ell
\end{aligned}
$$

die laatste ongelijkheid is omdat $3, 5$ de laagste twee oneven priemen zijn.
Nu hebben we een tegenspraak. Dus de priemontbinding moet minstens 3 verschillende priemen bevatten.