ÖVNING 8 - DISKRET MATEMATIK

ERIC AHLQVIST

1. Eulerfunktionen

Om n är ett positivt heltal så definierar vi

$$\phi(n) = |\{k \in \mathbb{Z} : 1 \leq k \leq n,\ \operatorname{sgd}(k, n) = 1\}| .$$

Funktionen

$$\begin{aligned} \mathbb{Z}_+ &\to \mathbb{Z}_+ \\ n &\mapsto \phi(n) \end{aligned}$$

kallas för *Eulerfunktionen.*

Sats 1.1. *Om $n \geq 2$ är ett heltal vars primtalsfaktorisering är*

$$n = p_1^{e_1} \cdots p_s^{e_s}$$

så har vi att

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right) .$$

Exempel 1.2. Om p är ett primtal har vi att $\phi(p) = p - 1$. Detta stämmer med Sats 1.1 ovan eftersom

$$p \left(1 - \frac{1}{p}\right) = p - 1 .$$

Extra Övn. 8 (1). (a) Visa att

$$\phi(26^2) = 12 \cdot 26 .$$

(b) Finn alla $n \in \mathbb{Z}_+$ sådana att

$$\phi(n^2) = 12n .$$

Lösning. (a) Vi har att $26 = 2^2 \cdots 13^2$ och Sats 1.1 ger då

$$\begin{aligned} \phi(26) &= 26^2 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{13}\right) \\ &= 26^2 \cdot \frac{1}{2} \cdot \frac{12}{13} \\ &= 26 \cdot 12 . \end{aligned}$$

(b) Låt

$$n = p_1^{e_1} \cdots p_s^{e_s}$$

vara primtalsfaktoriseringen av ett heltal $n \geq 2$. Enligt Sats 1.1 har vi att

$$\begin{aligned} \phi(n^2) &= n^2 \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right) \\ &= p_1^{2e_1 - 1} \cdots p_s^{2e_s - 1} (p_1 - 1) \cdots (p_s - 1) \end{aligned}$$

och vi har att

$$12n = 12 p_1^{e_1} \cdots p_n^{e_s} ,$$

vilket ger ekvationen

$$p_1^{2e_1 - 1} \cdots p_s^{2e_s - 1} (p_1 - 1) \cdots (p_s - 1) = 12 p_1^{e_1} \cdots p_n^{e_s} .$$

Om vi delar med $p_1^{e_1}\cdots p_s^{e_s}$ på båda sidor får vi

$$12 = p_1^{e_1-1}\cdots p_s^{e_s-1}(p_1-1)\cdots(p_s-1)\,. \tag{1}$$

Eftersom $p_i - 1$ är en faktor i 12 för varje i så har vi att

$$p_i \in \{2,3,5,7,13\}$$

för varje i. Möjliga faktoriseringar på formen (1) är då

$$\begin{aligned}
12 &= 13^{1-1}(12)\\
12 &= 3^{1-1}7^{1-1}(2)(6)\\
12 &= 3^{2-1}2^{2-1}(2)(1)\\
12 &= 2^{1-1}3^{1-1}7^{1-1}(1)(2)(6)\\
12 &= 2^{1-1}13^{1-1}(1)(12)\\
12 &= 2^{2-1}7^{1-1}(1)(6)
\end{aligned}$$

vilket svarar mot

$$\begin{aligned}
n &= 13\\
n &= 3\cdot 7 = 21\\
n &= 3^2\cdot 2^2 = 36\\
n &= 2\cdot 3\cdot 7 = 42\\
n &= 2\cdot 13 = 26\\
n &= 2^2\cdot 7 = 28\,.
\end{aligned}$$

2. Möbiusfunktionen

Funktionen

$$\begin{aligned}
\mathbb{Z}_+ &\to \{-1,0,1\}\\
d &\mapsto \mu(d)
\end{aligned}$$

där

$$\mu(d) = \begin{cases} 1 & \text{om } d = 1\,,\\ (-1)^k & \text{om } d \text{ är en product av } k \text{ distinkta primtal}\,,\\ 0 & \text{om } d \text{ har en upprepad primfaktor}\,, \end{cases}$$

kallas för *Möbiusfunktionen.*

Sats 2.1 (Möbius inversformel)**.** *Låt $f, g\colon \mathbb{Z}_+ \to \mathbb{Z}_+$ vara två funktioner. Då har vi att*

$$f(n) = \sum_{d|n} g(d)$$

för alla $n \in \mathbb{Z}_+$ om och endast om

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$$

för alla $n \in \mathbb{Z}_+$.

Biggs 11.5.2. Visa att om n har primfaktorisering

$$n = p_1^{e_1} \cdots p_s^{e_s}$$

så är antalet delare av n

$$(e_1 + 1) \cdots (e_s + 1)\,.$$

Lösning. Varje delare till n har formen

$$p_1^{a_1} \cdots p_s^{a_s}$$

där $0 \leq a_i \leq e_i$ för alla $1 \leq i \leq s$. Antalet sätt att välja en sådan s-tuple $(a_1, \dots, a_s)$ är

$$(e_1 + 1) \cdots (e_s + 1)\,.$$

Extrauppgift. Visa mha Möbius inversformel att det för varje $n \in \mathbb{Z}_+$ gäller att

$$\sum_{d|n} \phi(d) = n\,.$$

Lösning. Antag att $n \in \mathbb{Z}_+$ har primtalsfaktorisering

$$n = p_1^{e_1} \cdots p_s^{e_s}\,.$$

Vi har enligt Sats 1.1 at

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right)\,.$$

Om vi multiplicerar ihop parenteserna får vi att

$$\begin{aligned}
\phi(n) &= n - \sum_{i=1}^{s} \frac{n}{p_i} + \sum_{i \neq j} \frac{n}{p_i p_j} - \cdots + (-1)^k \frac{n}{p_1 \dots p_s} \\
&= \sum_{d|n} \mu(d) \frac{n}{d}\,.
\end{aligned}$$

Möbius inversformel ger nu att

$$n = \sum_{d|n} \phi(d)\,.$$

3. Ringar och Kroppar

En ring där alla nollskiljda element har en multiplikativ invers kallas för en *divisionsring.* En *kropp* är en kommutativ divisionsring, dvs en kommutativ ring där varje nollskiljt element har en multiplikativ invers.

Extra Övn. 8 (2). Låt $(R, +, \cdot)$ vara en ring sådan att $(R, +)$ är en cyklisk grupp. Visa att $(R, +, \cdot)$ är kommutativ (dvs $a \cdot b = b \cdot a$ för alla $a, b \in R$).

Lösning. Låt r vara en generator för $(R, +)$ och låt a och b vara två godtyckliga element i R. Då finns det naturliga tal s, t så att $a = sr$ och $b = tr$ (där sr (eller tr) betyder $r + \cdots + r$ med s (eller t) stycken termer). Dvs

$$\begin{aligned}
a \cdot b &= (sr)(tr) \\
&= r^2 + \cdots + r^2 \\
&= (st)r^2 \\
&= (tr)(sr) \\
&= b \cdot a\,.
\end{aligned}$$

Extra Övn. 8 (3). Ett element a i en ring R kallas för *nilpotent* om det finns ett $n \in \mathbb{Z}$ så att $a^n = 0$. Visa att om $a \in R$ är nilpotent så är elementet $1 - a$ inverterbart i R.

Lösning. Inversen till $1 - a$ ges av

$$1 + a + a^2 + a^3 + \dots .$$

Mycket riktigt, det finns ett n så att $a^n = 0$ och därför har vi att

$$\begin{aligned}(1-a)(1+a+a^2+a^3+\cdots+a^{n-1}) &= 1 - a + a - a^2 + a^2 - \cdots - a^{n-1} + a^{n-1} - a^n \\ &= 1\,.\end{aligned}$$