Aritmetiska funktioner

Theo Backman NV3a

Vallentuna Gymnasium den 20 januari 2005

1 Notation och inledning

1.1 Definition

En aritmetisk funktion är en funktion definierad för de positiva heltalen och som ger värden i en delmängd av de komplexa talen.

I fortsättningen kommer de positiva heltalen betecknas Z^+. Att ett heltal d delar ett heltal k innebär att det det finns ett tredje heltal e så att $k = de$. Om d delar k skrivs det i fortsättningen som $d \mid k$ och utläses d delar k. Det största heltalet d som delar både a och b kommer i fortsättningen betecknas (a, b), vi har speciellt om $(a, b) = 1$ att a och b är relativa prima.

Jag ger några exempel på aritmetiska funktioner som kommer diskuteras i texten.

$$\tau(n) = \sum_{d|n} 1 \quad d, n \in \mathrm{Z}^+$$

τ-funktionen ger antalet delare till heltalet n.

$$\sigma(n) = \sum_{d|n} d \quad d, n \in \mathrm{Z}^+$$

σ-funktionen ger summan av delarna till heltalet n.

$$\sigma_s(n) = \sum_{d|n} d^s \quad d, n \in \mathrm{Z}^+$$

σ-funktionerna är en generalisering av τ- och σ-funktionen. Man kan lätt se att $\tau(n) = \sigma_0(n)$ och att $\sigma(n) = \sigma_1(n)$. τ-och σ-funktionen används relativt ofta och har då fått speciella namn.

$$\iota_s(n) = n^s \quad n \in \mathrm{Z}^+ s \in \mathrm{C}$$

ι-funktionerna. Dessa funktioner blir intressanta om man kombinerar dem med andra funktioner.

$$\varphi(n) = \sum_{(a,n)=1 \ 1 \le a \le n} 1$$

Euler totientfunktionen, räknar antalet heltal mindre än n och relativa prima till n.

2 Dirichletmultiplikation

Vi låter A beteckna mängden av alla aritmetiska funktioner. De olika aritmetiska funktionerna kan kombinaras och på så vis ge upphov till nya aritmetiska funktioner. Exempel på kombinationer vi skulle kunna definiera är

$$(f+g)(n) = f(n) + g(n)$$

och

$$(f \cdot g)(n) = f(n) \cdot g(n)$$

Vi skall dock rikta vår uppmärksamhet mot en mindre uppenbar kombination, som ges av $f \times g$, definierad så att

$$(f \times g)(n) = \sum_{d|n} f(d) g\Big(\frac{n}{d}\Big) = \sum_{ab=n} f(a)g(b)$$

Detta kallas för Dirichletmultiplikation.

2.1 Sats

Dirichletmultiplikation är associativ. Om $f,\ g,\ h \in A$ så är $(\,(f \times g) \times h\,)(n) = (f \times (g \times h))(n)$ för alla $n \in \mathrm{Z}^+$.

Bevis. För ett fixt $n \in \mathrm{Z}^+$,

$$\begin{aligned}
(\,(f \times g) \times h\,)(n) &= \sum_{dc=n} (f \times g)(d) h(c) \\
&= \sum_{dc=n} \left\{ \sum_{ab=d} f(a)g(b) \right\} h(c) \\
&= \sum_{abc=n} f(a)g(b)h(c) \\
&= \sum_{ae=n} f(a) \left\{ \sum_{bc=e} g(b)f(c) \right\} \\
&= \sum_{ae=n} f(a)(g \times h(e)) \\
&= (f \times (g \times h))\,(n).
\end{aligned}$$

Vi visar nu att Dirichletmultiplikation är kommutativ.

2.2 Sats

Om $f,\ g \in A$ så är $(f \times g)(n) = (g \times f)(n)$ för alla $n \in \mathrm{Z}^+$

Bevis.

$$(f \times g)(n) = \sum_{ab=n} f(a)g(b) = \sum_{ba=n} g(b)f(a) = (g \times f)(n)\,.$$

Vi utreder nu frågan om det kan finnas en funktion ε i A så att $f \times \varepsilon = \varepsilon \times f = f$ för alla $f \in A$? Eftersom Dirichletmultiplikationen är kommutativ behöver vi bara undersöka ifall det finns en funktion ε så att $f = \varepsilon \times f$ för alla $f \in A$, eller ekvivalent, så att för varje $f \in A$,

$$f(n) = (\varepsilon \times f)(n) \text{ för alla } n \in \mathrm{Z}^+. \tag{1}$$

2.3 Sats

Det aritmetiska funktionen $\varepsilon(n) = \lfloor 1/n \rfloor$ är den entydiga funktionen som uppfyller $\varepsilon \times f = f$ för alla $f \in A$.

Vi antar att en sådan funktion existerar och utreder vilka egenskaper den i så fall måste ha. $f(1) = \varepsilon(1)f(1)$ eftersom vill att likheten skall gälla för f, en godtycklig funktion så måste det specifikt gälla då $f(1) \neq 0$ och då kan vi säkert säga att $\varepsilon(1) = 1$.

$$f(2) = f(1)\varepsilon(2) + f(2)\varepsilon(1).$$

$\varepsilon(1) = 1$ så då följer att $f(1)\varepsilon(2) = 0$, f är en godtycklig funktion så vi kan dra slutsatsen att $\varepsilon(2) = 0$. Vi forsätter med induktion över n för att visa att $\varepsilon(n) = 0$ för $n \geq 2$. Anta att $\varepsilon(n) = 0$ för $n = 2, \ldots, k-1$ $(k \geq 3)$. Nu betraktar vi (1) då $n = k$

$$f(k) = \sum_{d|k} \varepsilon(d) f\left(\frac{k}{d}\right) = \varepsilon(1)f(k) + \sum_{d|k\ \ 1<d<k} \varepsilon(d) f\left(\frac{k}{d}\right) + \varepsilon(k)f(1)$$

enligt induktionsantagandet är

$$\sum_{d|k\ \ 1<d<k} \varepsilon(d) f\left(\frac{k}{d}\right) = 0$$

alltså blir

$$f(k) = \varepsilon(1)f(k) + \varepsilon(k)f(1)$$

eftersom vi betraktar en godtycklig funktion f så måste $\varepsilon(k) = 0$ för $k \geq 2$. Det finns alltså en funktion som uppfyller (1) och den är

$$\varepsilon = \varepsilon(n) : 1, 0, 0 \ldots .$$

Ett annat sätt att uttrycka ε får man om man observerar funktion

$$\lfloor x \rfloor = max \ \{n : n \in \mathrm{Z}, \ n \leq x\}$$

heltalsdelen av x. Det framgår nu att $\varepsilon(n) = \lfloor 1/n \rfloor$. Och därmed är satsen bevisad.

Nu betraktar vi den aritmetiska funktionen $\theta(n) = 0$ för alla $n \in \mathrm{Z}^+$. Vi formulerar en sats angående funktionen och bevisar den.

2.4 Sats

$\theta \times f = \theta$ för alla $f \in A$ och om $g \times f = g$ för alla $f \in A$ så är $g = \theta$.

Bevis. Att

$$(\theta \times f)(n) = 0 = \theta(n)$$

följer genast av definitionen för θ.

$$(g \times f)(1) = g(1)f(1) = g(1)$$

för en godtycklig funktion f ger detta att $g(1) = 0$. Vi fortsätter med induktion över n. Anta att $g(n) = 0$ för $n = 1, \ldots, k-1$.

$$(g \times f)(k) = \sum_{d|k} g(d) f\left(\frac{k}{d}\right) = \sum_{d|k \ d<k} g(d) f\left(\frac{k}{d}\right) + g(k)f(1)$$

eftersom $g(d) = 0$ för $d < k$ så blir

$$(g \times f)(k) = g(k)f(1) = g(k)$$

återigen är likheten endast uppfylld för en godtycklig aritmetisk funktion om $g(k) = 0$, vilket bevisar satsen.

3 Inverser av aritmetiska funktioner

3.1 Definition

Låt $f \in A$, om det finns en funktion f' så att $f \times f' = e$, så kallar vi f' inversen av f.

Alla aritmetiska funktioner har tydligen inte en invers, ta θ som ett exempel. Det kan inte existera en funktion θ' så att $(\theta \times \theta')(n) = \varepsilon(n)$ för alla n, för att vid $n = 1$ skulle detta kräva att

$$0 = \theta(1)\theta'(1) = (\theta \times \theta')(1) = \varepsilon(1) = 1$$

vilket är orimligt. Egentligen visar detta exempel på det enda sättet en funktion kan kan undgå att ha en invers. Nästa sats ger en beskrivning av situationen.

3.2 Sats

Ett nödvändigt och tillräckligt villkor för att en aritmetisk funktion $f$skall ha en invers är att $f(1) \neq 0$ och denna invers är unik.

Bevis. Först, ponera att f' existerar och eftersom $(f \times f')(1) = \varepsilon(1)$ så måste $f(1) \neq 0$. Vi förutsätter att $f(1) \neq 0$ och betrakar den aritmetiska funktion g som definieras induktivt så att

$$\begin{aligned} g(1) &= \frac{1}{f(1)} \\ g(n) &= \frac{-1}{f(1)} \sum_{cd=n \ 1<c} f(c)g(d) \qquad n > 1. \end{aligned}$$

Våra ansträngnigar riktas mot ett bevis till att $f \times g = \varepsilon$ och sedan att $g = f'$.

$$(f \times g)(1) = f(1)g(1) = f(1)\frac{1}{f(1)} = 1 = \varepsilon(1)$$

och

$$(f \times g)(2) = f(1)g(2)+f(2)g(1) = f(1)\left\{ \frac{-1}{f(1)}f(2)g(1) \right\}+f(2)g(1) = 0 = \varepsilon(2)$$

anta att $(f \times g)(k) = 0$ för $k = 2, \ldots, n-1$ $(n \geq 3)$. Då är

$$
\begin{aligned}
(f \times g)(n) &= f(n)g(1) + \sum_{ab=n \ 1<b} f(a)g(b) \\
&= f(n)g(1) + \sum_{ab=n \ 1<b} f(a)\left\{ \frac{-1}{f(1)} \sum_{cd=b \ 1<c} f(c)g(d) \right\} \\
&= f(n)g(1) - \frac{1}{f(1)} \sum_{ab=n \ 1<b} f(a)\left\{ \sum_{cd=b} f(c)g(d) - f(1)g(b) \right\} \\
&= f(n)g(1) - \frac{1}{f(1)} \sum_{ab=n \ 1<b} f(a) \sum_{cd=b} f(c)g(d) + \sum_{ab=n \ 1<b} f(a)g(b) \\
&= f(n)g(1) - \frac{1}{f(1)} \sum_{ab=n \ 1<b} f(a)(f \times g)(b) + \sum_{ab=n \ 1<b} f(a)g(b)
\end{aligned}
$$

Enligt antagandet är den första summan i sista ledet bara möjligen skild från 0 vid $b = n$, så ovanstående förenklas till

$$
(f \times g)(n) = f(n)g(1) - \frac{1}{f(1)} f(1)(f \times g)(n) + \sum_{ab=n \ 1<b} f(a)g(b) = 0
$$

Det visar att för alla n så är $(f \times g)(n) = \varepsilon(n)$. Nu kvarstår bara att visa att $g = f'$. Genom att utgå från $\varepsilon = f \times g$ och $\varepsilon = f \times f'$ så ser man att

$$
f' = \varepsilon \times f' = (f \times g) \times f' = (f \times f') \times g = \varepsilon \times g = g
$$

vilket slutligen visar att inversen är unik och således är satsen bevisasd.

Vi bildar mängden av inverterbara aritmetiska funktioner och betecknar den A^*.

4 Multiplikativa funktioner

4.1 Definition

En funktion f kallas multiplikativ om för varje m och n så att $(m,n)=1$ så är $f(mn)=f(m)f(n)$ och om $f(1)\neq 0$. Mängden av de aritmetiska funktioner som är multiplikativa betecknas M.

Om $f\in M$ och $f(n_0)\neq 0$, men eftersom $(1,n_0)=1$ så blir $f(n_0)=f(1\cdot n_0)=f(1)f(n_0)$ alltså så är även $f(1)\neq 0$.

4.2 Sats

Om $f,g\in M$ så är $f\times g\in M$. Dirichletprodukten av två multiplikativa funktioner är multiplikativ.

Bevis. $f(1)=g(1)=1$ och $(f\times g)(1)=1$. Om $(m,n)=1$ så är

$$\begin{aligned}(f\times g)(mn)&=\sum_{d|mn}f(d)g\Big(\frac{mn}{d}\Big)\\&=\sum_{a|m\ b|n\ ab=d}f(ab)g\Big(\frac{m}{a}\frac{n}{b}\Big)\\&=\sum_{a|m\ b|n}f(a)f(b)g\Big(\frac{m}{a}\Big)g\Big(\frac{n}{b}\Big)\\&=\left\{\sum_{a|m}f(b)g\Big(\frac{m}{a}\Big)\right\}\left\{\sum_{b|n}f(b)g\Big(\frac{n}{b}\Big)\right\}\\&=(f\times g)(m)(f\times g)(n)\end{aligned}$$

vilket visar att $f\times g\in M$.

$\iota_s(n)=n^s$ då $n\in \mathrm{Z}^+$ och $s\in \mathrm{C}$. Det är känt att $(mn)^s=m^sn^s$ och då måste $\iota_s(mn)=\iota_s(m)\iota_s(n)$ och då följer att $\iota_s\in M$.

4.3 Sats

Om f är en multiplikativ funktion och om

$$g(n)=\sum_{d|n}f(d)=(\iota_0\times f)(n),$$

då är även g multiplikativ.

Bevis. Båda funktionerna i ovanstående Dirichletprodukt är multiplikativa och då följer att g är multiplikativ, vilket skulle bevisas.

Alla multiplikativa funktioner har en invers, nu undersöker vi om dessa inverser är multiplikativa och vi låter numera inversen till f betecknas f^{-1}.

4.4 Sats

Om $f \in M$ så finns f^{-1} och $f^{-1} \in M$.

Bevis. Definitionen för en multiplikativ funktion ger att f^{-1} existerar. Det är även så att $f^{-1}(1) = 1/f(1) = 1$. Anta att vi har bevisat att $f^{-1}(st) = f^{-1}(s)f^{-1}(t)$ vid alla tillfällen då $(s,t) = 1$ för alla s,t så att $1 \leq st \leq k-1$. Låt $k = mn$ vara en godtycklig faktorisering av k så att $(m,n) = 1$. Nu betrakatar vi

$$\begin{aligned}
0 = \varepsilon(k) &= \sum_{d|k} f(d) f^{-1}\left(\frac{k}{d}\right) \\
&= \sum_{a|m \;\; b|n} f(ab) f^{-1}\Big(\frac{m}{a}\frac{n}{b}\Big) \\
&= \sum_{a|m \;\; b|n \;\; ab>1} f(ab) f^{-1}\Big(\frac{m}{a}\frac{n}{b}\Big) + f(1) f^{-1}(mn) \\
&= \sum_{a|m \;\; b|n \;\; ab>1} f(a) f(b) f^{-1}\Big(\frac{m}{a}\Big) f^{-1}\Big(\frac{n}{b}\Big) + f^{-1}(mn) \\
&= \sum_{a|m \;\; b|n} f(a) f(b) f^{-1}\Big(\frac{m}{a}\Big) f^{-1}\Big(\frac{n}{b}\Big) - f^{-1}(m) f^{-1}(n) + f^{-1}(mn) \\
&= \left\{ \sum_{a|m} f(a) f^{-1}\Big(\frac{m}{a}\Big) \right\} \left\{ \sum_{b|n} f(b) f^{-1}\Big(\frac{n}{b}\Big) \right\} - f^{-1}(m)\, f^{-1}(n) + f^{-1}(mn) \\
0 &= \varepsilon(m)\varepsilon(n) - f^{-1}(m) f'(n) + f^{-1}(mn)
\end{aligned}$$

eftersom $1 < k$ så måste någon av m, n vara större än 1, vilket medför att $\varepsilon(m)\varepsilon(n)$ försvinner. Nu ser vi att $f^{-1}(m)f^{-1}(n) = f^{-1}(mn)$ vilket visar att $f^{-1} \in M$.

4.5 Sats

Den funktion ε som uppfyllde likheten $f \times \varepsilon = f$ är multiplikativ.

Bevis. $\varepsilon(mn) = \varepsilon(m)\varepsilon(n)$ för $mn = 1$ blir det $\varepsilon(1) = \varepsilon(1)\varepsilon(1) = 1$, men då $1 < mn$ så måste någon av m eller n vara större än 1, vilket ger att båda leden blir noll och därmed är satsen visad.

5 Möbiusfunktionen

Nästa sats kommer vara till stor hjälp när vi ska studera multiplikativa funktioner.

5.1 Sats

$f \in M$ och $n > 1$ kan skrivas

$$n = \prod_{i=1}^{k} {p_i}^{\beta_i}, \qquad \beta_i > 0 \tag{2}$$

då är

$$f(n) = \prod_{i=1}^{k} f\left({p_i}^{\beta_i}\right). \tag{3}$$

Bevis. För $n = 1$ finns det inget att bevisa. Vi antar att satsen är sann för $1 \leq k < K$. Då är

$$\begin{aligned} f\left(\prod_{i=1}^{K} {p_i}^{\beta_i}\right) &= f\left(\left\{\prod_{i=1}^{K-1} {p_i}^{\beta_i}\right\} {p_K}^{\beta_K}\right) \\ &= f\left(\prod_{i=1}^{K-1} {p_i}^{\beta_i}\right) f\left({p_K}^{\beta_K}\right) \\ &= \left\{\prod_{i=1}^{K-1} f\left({p_i}^{\beta_i}\right)\right\} f\left({p_K}^{\beta_K}\right) \\ &= \prod_{i=1}^{K} f\left({p_i}^{\beta_i}\right). \end{aligned}$$

Den här satsen säger oss att en multiplikativ funktion är helt och hållet bestämd av dess värden vid p^β for varje primtal p och för varje $\beta \in \mathrm{Z}^+$. Vi ska demonstrera en användning för **5.2** genom att leta efter inversen till ι_0, vi vet att ι_0^{-1} existerar och att den är multiplikativ. Så vi behöver endast finna $\iota_0^{-1}\left(p^\beta\right)$ för primtal p och för $\beta = 1, 2, \ldots$ därför låter vi p vara ett primtal och fortsätter med induktion över β. För $\beta = 1$ gäller att

$$\begin{aligned} 0 = \varepsilon(p) &= (\iota_0^{-1} \times \iota_0(p) \\ &= \iota_0^{-1}(1)\iota_0(p) + \iota_0^{-1}(p)\iota_0(1) \\ &= 1 + \iota_0^{-1}(p) \end{aligned}$$

och nu framgår att $\iota_0^{-1}(p) = -1$. För $\beta = 2$, $\varepsilon(p^2) = \left(\iota_0^{-1} \times \iota_0\right)(p^2)$ blir det

$$0 = \sum_{j=0}^{2} \iota_0^{-1}\big(p^j\big)\iota_0\big(p^{2-j}\big) = 1 - 1 + \iota_0^{-1}\big(p^2\big),$$

så $\iota_0^{-1}(p^2) = 0$. Anta nu att $\iota_0^{-1}\big(p^\beta\big) = 0$ för $2 \leq \beta < B$; då är

$$\begin{aligned} 0 = \varepsilon\big(p^B\big) &= \sum_{j=0}^{B} \iota_0^{-1}\big(p^j\big) \\ &= \iota_0^{-1}(1) + \iota_0^{-1}(p) + \sum_{j=2}^{B-1} \iota_0^{-1}\big(p^j\big) + \iota_0^{-1}\big(p^B\big) \\ &= \iota_0^{-1}\big(p^B\big) \end{aligned}$$

Vi har visat att $\iota_0^{-1}(p) = -1$ och att $\iota_0^{-1}\big(p^\beta\big) = 0$ då $\beta > 2$ för alla primtal p.

Vanligtvis brukar man kalla denna funktion Möbiusfunktionen och den skrivs μ. Vi adopterar detta skrivsätt och använder **5.2** för att slutföra; om $n > 1$ och faktoriserad som i (2) så är

$$\mu(n) = \prod_{i=1}^{k} \mu\big({p_i}^{\beta_i}\big),$$

Vi sammanfattar ovanstående diskusioner i en sats.

5.2 Sats

Möbiusfunktionen μ, definierad som $\iota_0 \times \mu = \mu \times \iota_0 = \varepsilon$, är en multiplikativ funktion med värden givna av

$$\mu(n) = \begin{cases} 1 \text{ om } n = 1; \\ (-1)^k \text{ om } n \text{ är en produkt av } k \text{ olika primtal;} \\ 0 \text{ om } n \text{ är delbar med kvadraten på något heltal.} \end{cases}$$

Och ekvivalent, Möbiusfunktionen uppfyller ekvationen $\mu(1) = 1$, och för $1 < n$ så är

$$\sum_{d|n} \mu(d) = 0.$$

5.3 Sats

Möbius inversionsformel. Om

$$g(n) = \sum_{d|n} f(d) \tag{4}$$

då är

$$f(n) = \sum_{d|n} g(d)\mu\Big(\frac{n}{d}\Big). \tag{5}$$

Det omvända gäller också, så att (5) implicerar (4).

Bevis. Ekvationen (4) är i all enkelhet $g = \iota_o \times f$, och (5) är $f = g \times \mu$. Tydligen är $g = \iota_0 \times f$ endast om $g \times \mu = f \times \iota_0 \times \mu = f \times \varepsilon = f$.

5.4 Sats

Om $g \in M$ och

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

så är även $f \in M$.

Bevis. Det här är omvändningen av **4.3**, om $g = \iota_0 \times f$ då är $f = g \times \mu$. Det är känt att g och $\mu \in M$, så deras Dirichletprodukt $f \in M$.

Det är värt att notera att Möbius inversionsformel är ett specialfall av denna bakomliggande sats. Satsen är trivial och presenteras utan bevis.

5.5 Sats

Om $h \in A^*$ och om $f, g \in A$. Då är $f \times h = g$ om och endast om $f = g \times h^{-1}$.

6 σ-funktionerna

6.1 Definition

Om s är något komplext tal så är funktionen $\sigma_s \in A$ definierad av $\sigma_s = \iota_s \times \iota_0$. Funktionerna σ_s kallas för σ-funktionerna.

Att denna definition är densamma som vi gav i inledning ser man om man observerar att

$$\begin{aligned}\sigma_s(n) &= (\iota_s \times \iota_0)(n) \\ &= \sum_{d|n} \iota_s(d)\iota_0\left(\frac{n}{d}\right) \\ &= \sum_{d|n} d^s,\end{aligned}$$

och då framgår det att $\sigma_s(n)$ är summan av den s:te potensen av de positiva delarna av n. Vidare har vi, om p är ett primtal,

$$\begin{aligned}\sigma_s(p^\beta) &= \sum_{j=0}^{\beta} (p^j)^s \\ &= \beta + 1 \quad \text{om } s = 0\end{aligned}$$

eller

$$\begin{aligned}\sigma_s(p^\beta) &= \sum_{j=0}^{\beta} (p^j)^s \\ &= \frac{p^{s(\beta+1)} - 1}{p^s - 1} \quad \text{om } s \neq 0.\end{aligned}$$

Eftersom σ-funktionerna är Dirichletprodukter av multiplikativa funktioner följer att σ-funktionerna är multiplikativa. Denna multiplikativiet medför att **5.2** är applicerbar och om

$$1 < n = \prod_{j=1}^{k} {p_j}^{\beta_j},$$

så får vi att

$$\tau(n) = \sigma_0(n) = \prod_{j=1}^{k}(\beta_j + 1),$$

$$\sigma(n) = \sigma_1(n) = \prod_{j=1}^{k}\frac{{p_j}^{\beta_j+1} - 1}{p_j - 1},$$

$$\sigma_s(n) = \prod_{j=1}^{k}\frac{{p_j}^{s(\beta_j+1)} - 1}{{p_j}^s - 1}, \qquad s \neq 0.$$

Det finns några klassiska problem som kan formuleras i termer av σ-funktionen (σ_1). Problemen gäller de perfekta talen. Men innan vi ger oss in på dessa till viss del ännu olösta problem så ska vi definiera och undersöka Mersenneprimtalen. Ett Mersenneprimtal är något primtal på formen $q = a^b - 1$ då $a, b \in \mathrm{Z}^+$ och så att $b > 1$. Men om vi erindrar oss följande identitet,

$$x^{n+1} - 1 = (x - 1)(1 + x + x^2 + \cdots + x^n),$$

så ser vi att $q = a^b - 1$ endast kan vara ett primtal då $a = 2$, ty $a - 1 | a^b - 1$ och om $a - 1 \neq 1$ så får $a^b - 1$ en icke-trivial delare och medför då att heltalet i fråga inte kan vara ett primtal. Ytterligare har vi att om $b = mn, m \geq 1, n \geq 1$ så medför det att

$$2^b - 1 = 2^{mn} - 1 = (2^m)^n - 1 = c^n - 1, \text{ för något } c \geq 2$$

ett $c \geq 2$ ger att q är sammansatt. Följaktligen, ett Mersenneprimtal är på formen $2^p - 1$ då p är ett primtal.

Ett postivt heltal n kallas perfekt om $\sigma(n) = 2n$. Det är fortfarande en öppen utsaga hurvida det existerar några udda perfekta tal, alltså; det är varken bevisat att de kan existera eller att de inte kan existera. Men i följande sats visar vi på det enda sättet ett jämnt heltal kan vara perfekt. Euklides bevisade att det var tillräckligt för heltal på denna form att vara perfekta; Euler visade att alla jämna heltal nödvändigtvis är på denna form om de är perfekta.

6.2 Sats

Ett tillräckligt och nödvändigt villkor för att n ska vara ett jämnt perfekt tal är om $n = 2^{p-1}(2^p - 1)$, då $2^p - 1$ är ett primtal.

Bevis. Låt $n = 2^{p-1}(2^p - 1)$ och låt $2^p - 1$ vara ett primtal. Då har vi att

$$\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1) = (2^p - 1)(2^p) = 2n.$$

Nu till omvändningen; om n är jämn och perfekt, vi skriver det $n = 2^k m, k > 0$ och m är udda. Vi får att

$$\sigma(n) = (2^{k+1} - 1)\sigma(m) = 2n = 2^{k+1}m.$$

Vi får att $(2^{k+1}-1) \mid m$ låt oss säga att $m = (2^{k+1}-1)M$. Om vi substituerar i de tidigarer räkningarna så framgår att $\sigma(m) = 2^{k+1}M$. Detta ger att både m och M är skilda delare till m, så $\sigma(m) \geq m + M$. Detta ger dock att

$$2^{k+1}M = \sigma(m) \geq m + M = 2^{k+1}M,$$

vi får att n och M är de enda delarna till m. Följaktligen är $M = 1$ och $m = 2^{k+1} - 1$ är ett primtal; tidigare såg vi dock att $2^{k+1} - 1$ endast kan vara ett primtal då $k + 1 = p$ är ett primtal. Och vi har visat att n är på den sökta formen.

7 ϕ-funktionen

7.1 Definition

Vi kan definiera ϕ-funktionen som dirichletprodukten av ι_1 och μ.

7.2 Sats

Den aritmetiska funktionen ϕ är multiplikativ och uppfyller följande identiteter

$$\phi(n) = \sum_{d|n} d\mu\left(\frac{n}{d}\right) = n\sum_{d|n}\frac{\mu(d)}{d}.$$

Bevis. Eftersom både ι_1 och $\mu \in M$ så får vi att även $\phi \in M$. Vi har att

$$\begin{aligned}\phi(n) &= (\iota_1 \times \mu)(n)\\ &= \sum_{d|n} \iota_1(d)\mu\left(\frac{n}{d}\right)\\ &= \sum_{d|n} d\mu\left(\frac{n}{d}\right)\end{aligned}$$

och vi har även att

$$\begin{aligned}\phi(n) &= (\iota_1 \times \mu)(n)\\ &= \sum_{d|n} \iota_1\left(\frac{n}{d}\right)\mu(d)\\ &= n\sum_{d|n}\frac{\mu(d)}{d}\end{aligned}$$

Vilket bevisar satsen.

7.3 Sats

Låt

$$1 < n = \prod_{j=1}^{r} {p_j}^{\beta_j}$$

då blir

$$\phi(n) = n\prod_{j=1}^{r}\left(1 - \frac{1}{p_j}\right).$$

Bevis. Låt p vara ett primtal, då kan vi bestämma värdet av $\phi(p^\beta)$ i termer av p och β

$$\begin{aligned}\phi(p^\beta) &= (\iota_1 \times \mu)(p^\beta) \\ &= \sum_{j=0}^{\beta} \iota_1(p^{\beta-j})\mu(p^j) \\ &= \iota_1(p^\beta)\mu(1) + \iota_1(p^{\beta-1})\mu(p) \\ &= p^\beta - p^{\beta-1} = p^\beta\left(1 - \frac{1}{p}\right)\end{aligned}$$

Och eftersom vi har att

$$1 < n = \prod_{j=1}^{r} {p_j}^{\beta_j}$$

så följer det att

$$\phi(n) = \prod_{j=1}^{r} {p_j}^{\beta_j}\left(1 - \frac{1}{p_j}\right) = n\prod_{j=1}^{r}\left(1 - \frac{1}{p_j}\right)$$

vilket skulle bevisas.

Om Y är en godtycklig ändlig mängd så låter vi $\mathbf{v}Y$ ange antalet element i Y. Betrakta funktionen γ definierad vid varje $n \in \mathrm{Z}^+$ så att

$$\gamma(n) = \mathbf{v}\{t : 1 \leq t \leq n, (t, n) = 1\}.$$

Låt n vara ett godtyckligt positivt heltal. Vi definierar $Y = \{1, 2, \ldots, n\}$. För varje $d, 1 \leq d \leq n$, bildar vi $Y_d = \{t : 1 \leq t \leq n, (t, n) = d\}$.

7.4 Sats

Den aritmetiska funktionen ϕ uppfyller följande identiteter

$$\sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d) = n$$

och $\phi(n)$ anger antalet heltal mindre än n och relativa prima till n

Bevis. Uppsättningen $\{Y_d : 1 \leq d \leq n\}$ bildar en partition av Y. Om $d \neq e, 1 \leq d \leq n$ och $1 \leq e \leq n$ och låt $Y_d \cap Y_e \neq \emptyset$. Då måste det finnas ett heltal $t, 1 \leq t \leq n$ så att $t \in Y_d \cap Y_e$. Men det ger att $e = (t, n) = d$ och då foljer att om $d \neq e$ så är $Y_d \cap Y_e = \emptyset$. Ytterliggare om $t \in Y$ låt $d = (t, n)$. Eftersom $d|n$ och $1 \leq d \leq n$, så får vi att $t \in Y_d$ och vi har att varje $t \in Y$ är

i någon av delmängderna. Detta visar att $\{Y_d : 1 \leq d \leq n\}$ är en partition av Y.

Vidare borde vi även ha att antalet element i Y är det samma som antalet element i alla $Y_d, d = 1, \ldots, n$ tillsammans. Märk dock att om d inta delar n så blir $Y_d = \emptyset$ och vi får att

$$n = \mathbf{v}Y = \sum_{d=1}^{n} \mathbf{v}Y_d = \sum_{d|n} \mathbf{v}Y_d.$$

Vidare har vi att för alla d då $d \mid n$ så har vi att.

$$\begin{aligned} \mathbf{v}Y_d &= \mathbf{v}\{t : 1, 1 \leq t \leq n, (t, n) = d\} \\ &= \mathbf{v}\left\{\frac{t}{d} : 1 \leq \frac{t}{d} \leq \frac{n}{d}, \left(\frac{t}{d}, \frac{n}{d}\right) = 1\right\} = \gamma\left(\frac{n}{d}\right). \end{aligned}$$

Det bevisar att $\iota_0 \times \gamma = \iota_1$. Möbius inversionsformel ger sedan att $\gamma = \mu \times \iota_1$, vilket bevisar satsen och nu ser vi även att definitionen för ϕ överensstämmer med den som gavs i inledningen.

8 Källhänvisningar

[1] **Anthony A. Gioia.** *The Theory of Numbers: An Introduction* (Dover, 2001).

[2] **G. H. Hardy E. M. Wright** *An Introduction to the Theory of Numbers* (Oxford University Press, 5:de utgåvan 1979).