Udda Perfekta Tal

Kajsa Matti

Examensarbete för kandidatexamen
2014

Abstract

This bachelor's thesis is about odd perfect numbers and some of the conditions and characteristics they have if they exist. Both classical results and contemporary proofs from newer articles are included. Also history about the results and the mathematicians who managed to prove those and some of today's research and results are contained.

Innehåll

1 Bakgrund

Redan de gamla grekerna upptäckte och fascinerades av perfekta tal. Då kände man till fyra stycken, nämligen $6, 28, 496$ och 8128. Sedan dess har man upptäckt flera, dock bara jämna. Idag vet man mycket om jämna perfekta tal men väldigt lite om de udda. Man vet inte ens om de existerar. Hittills (våren 2014) har ingen lyckats hitta ett enda, men det finns heller inget bevis för att de inte skulle existera. Låt oss säga att det finns udda perfekta tal, vad har de då för egenskaper och vilka villkor gäller? Hur stora är de och hur många finns det?

Det första resultatet om perfekta tal kom från Euklides. Han var en grekisk matematiker som levde 300 f.Kr. och som bland annat studerade talteori. I hans arbete Elementa visar han att om $2^k - 1$ är ett primtal, där $k > 1$, så är $n = 2^{k-1}(2^k - 1)$ ett perfekt tal.

Cirka tvåtusen år senare, det vill säga på 1700-talet, kom nästa bevis. Det var från Leonhard Euler som föddes i Schweiz och levde mellan år 1707 och 1783. Han var en oerhört produktiv matematiker som skrev flera hundra artiklar. Han bevisade att den form Euklides kom fram till, $n = 2^{k-1}(2^k - 1)$ där $2^k - 1$ är ett primtal, är den generella formen för alla jämna perfekta tal. Han bevisade även senare att den generella formen för udda perfekta tal är $N = p_1^{k_1} p_2^{2j_2} \cdots p_r^{2j_r}$ där p_i är olika udda primtal och $p_1 \equiv k_1 \equiv 1 \pmod 4$. Dessa resultat har haft stor betydelse för forskningen om udda perfekta tal.

På 1800-talet använde den brittiska matematikern James Joseph Sylvester Eulers resultat och visade i en fransk tidsskrift [9], [10], att ett udda perfekt tal måste innehålla minst fem olika primtalsfaktorer.

En annan matematiker som också använde sig av Eulers resultat är Judy A. Holdener som år 2002 lyckades visa det som matematikern Jacques Touchard visade femtio år tidigare [4] nämligen att ett udda perfekt tal måste ha formen $12m + 1$ eller $36m + 9$. Touchard visade detta med hjälp av differentialekvationer och relationen

$$\frac{n^2(n-1)}{12}\sigma(n) = \sum_{k=1}^{n-1}(5k(n-k) - n^2)\sigma(k)\sigma(n-k)$$

som Balthasar van der Pol härledde år 1951 [12], men i detta arbete har jag återgivit Judy A. Holdeners bevis som endast använder sig av talteori [4].

Ett annat bevis som kom på 1900-talet, närmare bestämt år 1913, var Leonard Eugene Dicksons [3]. Han bevisade att för ett fixt k så finns det endast ett ändligt antal udda perfekta tal med högst k olika primtalsfaktorer. Paul Pollack lyckades nästan hundra år senare visa samma sak men med hjälp av topologi, vilket gör beviset mycket kortare och elegantare [8].

Det finns fortfarande mycket kvar att forska kring udda perfekta tal. Den vanligaste frågan och det många matematiker studerar är deras storlek. Sylvester visade på 1800-talet att ett udda perfekt tal måste bestå av minst fem olika primtalsfaktorer med hjälp av uppskattningar och talteori. Idag använder man sig främst av datorer för att forska kring udda perfekta tals storlek. År 2007 skrev Pace P. Nielsen i sin artikel [6] att de måste bestå av minst nio olika primtalsfaktorer och om 3 inte är en primtalsfaktor, måste ett udda perfekt tal bestå av minst tolv olika primtalsfaktorer. Det totala antalet primtalsfaktorer i ett udda perfekt tal måste vara minst etthundraen. Det var matematikerna Ochem och Rao som visade detta år 2012 [7]. I samma artikel visar de också att ett udda perfekt tal måste vara större än 10^{1500} och att det åtminstone måste innehålla en faktor p^j större än 10^{62}. Det mesta lutar åt att udda perfekta tal inte existerar. Men det finns som sagt heller inget bevis för att de inte skulle det. Tills ett sådant bevis publiceras kommer forskningen med all säkerhet att fortsätta.

2 Talteoretiska funktioner

Definition 2.1 Givet ett positivt heltal n, låt $\sigma(n)$ beteckna summan av alla positiva delare till n.

$$\sigma(n) = \sum_{\substack{d|n \\ 0<d\leq n}} d.$$

Sats 2.2 Om n är ett positivt heltal med primtalsfaktoriseringen $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ så är

$$\sigma(n) = \frac{p_1^{k_1+1}-1}{p_1-1} \cdot \frac{p_2^{k_2+1}-1}{p_2-1} \cdots \frac{p_r^{k_r+1}-1}{p_r-1}.$$

Bevis Betrakta produkten

$$(1+p_1+p_1^2+\cdots+p_1^{k_1})(1+p_2+p_2^2+\cdots+p_2^{k_2})\cdots(1+p_r+p_r^2+\cdots+p_r^{k_r}). \qquad (1)$$

Varje positiv delare till n uppkommer en gång och endast en gång som en term i utvecklingen av (1). Så

$$\begin{aligned}\sigma(n) &= (1+p_1+p_1^2+\cdots+p_1^{k_1})(1+p_2+p_2^2+\cdots+p_2^{k_2})\cdots(1+p_r+p_r^2+\cdots+p_r^{k_r}) \\ &= \frac{p_1^{k_1+1}-1}{p_1-1} \cdot \frac{p_2^{k_2+1}-1}{p_2-1} \cdots \frac{p_r^{k_r+1}-1}{p_r-1}.\end{aligned}$$

Högerledet fås genom att använda formeln för summor av ändliga geometriska serier. ■

Definition 2.3 En talteoretisk funktion f kallas för *multiplikativ* om

$$f(m \cdot n) = f(m)f(n) \quad \text{då} \quad gcd(m,n) = 1.$$

Sats 2.4 Funktionen $\sigma(n)$ är en multiplikativ funktion.

Bevis Fallet då något av talen m och n är lika med 1 är trivialt. Låt därför m och n vara heltal större än 1 och låt $gcd(m,n) = 1$. Antag att primtalsfaktoriseringarna av m och n ser ut som följer:

$$m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}, \quad n = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}.$$

Detta medför att

$$mn = p_1^{k_1} \cdots p_r^{k_r} \cdot q_1^{j_1} \cdots q_s^{j_s}.$$

Enligt sats 2.2 får vi då

$$\sigma(mn) = \left(\frac{p_1^{k_1+1}-1}{p_1-1} \cdots \frac{p_r^{k_r+1}-1}{p_r-1}\right)\left(\frac{q_1^{j_1+1}-1}{q_1-1} \cdots \frac{q_s^{j_s+1}-1}{q_s-1}\right) = \sigma(m)\sigma(n). \blacksquare$$

3 Perfekta tal

Definition 3.1 Ett positivt heltal n kallas *perfekt* om summan av alla positiva delare till n, inklusive n självt, är lika med $2n$. Alltså, n är ett perfekt tal om

$$\sigma(n) = 2n.$$

Exempel 3.2 6 är ett perfekt tal ty

$$\sigma(6) = 1+2+3+6 = 2 \cdot 6.$$

28 är ett perfekt tal ty

$$\sigma(28) = 1+2+4+7+14+28 = 2 \cdot 28.$$

4 Eulers resultat

Sats 4.1 Om N är ett udda perfekt tal är

$$N = p_1^{k_1} p_2^{2j_2} \cdots p_r^{2j_r}$$

där p_i, $i = 1, 2, \ldots, r$, är olika udda primtal och $p_1 \equiv k_1 \equiv 1 \pmod 4$.

Bevis Låt N vara ett udda perfekt tal och låt $N = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ vara primtalsfaktoriseringen av N. Eftersom σ är en multiplikativ funktion och alla p_i är relativt prima så är

$$2N = \sigma(N) = \sigma(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}) = \sigma(p_1^{k_1})\sigma(p_2^{k_2}) \cdots \sigma(p_r^{k_r})$$

och eftersom N är ett udda tal gäller det att

$$N \equiv 1 \pmod 4 \quad \text{eller} \quad N \equiv 3 \pmod 4.$$

Om vi multiplicerar med 2 på båda sidorna får vi

$$2N \equiv 2 \pmod 4 \quad \text{eller} \quad 2N \equiv 6 \equiv 2 \pmod 4. \tag{2}$$

Enligt kongruenserna (2) så är alltså $2N = \sigma(N) \equiv 2 \pmod 4$ vilket innebär att ett (och endast ett) av talen $\sigma(p_i^{k_i})$ måste vara ett jämnt heltal och resten udda. Låt oss säga att $\sigma(p_1^{k_1})$ är det jämna heltalet.

För ett givet p_i finns två alternativ, antingen är $p_i \equiv 1 \pmod 4$ eller $p_i \equiv 3 \pmod 4$. Om $p_i \equiv 3 \equiv -1 \pmod 4$ gäller det att

$$\begin{aligned}\sigma(p_i^{k_i}) &= 1 + p_i + p_i^2 + \cdots + p_i^{k_i} \equiv 1 + (-1) + (-1)^2 + \cdots + (-1)^{k_i} \\ &\equiv \begin{cases} 0 & \text{om } k_i \text{ är udda,} \\ 1 & \text{om } k_i \text{ är jämt,} \end{cases} \pmod 4.\end{aligned}$$

Eftersom vi antog att $\sigma(p_1^{k_1}) \equiv 2 \pmod 4$ medför det att $p_1 \not\equiv 3 \pmod 4$ vilket innebär att $p_1 \equiv 1 \pmod 4$. Kongruensen $\sigma(p_i^{k_i}) \equiv 0 \pmod 4$ innebär att 4 delar $\sigma(p_i^{k_i})$ vilket är en motsägelse. Alltså om $p_i \equiv 3 \pmod 4$, där $i = 2, 3, \ldots, r$, så är dess exponent k_i ett jämt heltal.

Om $p_i \equiv 1 \pmod 4$ gäller det att

$$\sigma(p_i^{k_i}) = 1 + p_i + p_i^2 + \cdots + p_i^{k_i} \equiv 1 + 1 + 1^2 + \cdots + 1^{k_i} \equiv k_i + 1 \pmod 4.$$

Vi vet att $\sigma(p_1^{k_1}) \equiv 2 \pmod 4$ vilket medför att $k_1 \equiv 1 \pmod 4$. För $i = 2, 3, \ldots, r$ är $\sigma(p_i^{k_i}) \equiv 1 \pmod 4$ eller $\sigma(p_i^{k_i}) \equiv 3 \pmod 4$ vilket medför att $k_i \equiv 0 \pmod 4$ eller $k_i \equiv 2 \pmod 4$, i vilket fall som helst är k_i ett jämnt heltal.

Alltså $k_1 \equiv 1 \pmod 4$ och oavsett om $p_i \equiv 1 \pmod 4$ eller $p_i \equiv 3 \pmod 4$ är k_i ett jämnt heltal för $i = 2, 3, \ldots, r$, vilket gör vårt bevis fullständigt. ■

5 Touchards resultat

Lemma 5.1 Om N är ett udda perfekt tal kan det inte ha formen $6m - 1$.

Bevis Antag att $N = 6m - 1$ vilket medför att $N \equiv -1 \pmod 3$. För vilken delare d som helst gäller det att

$$d \cdot \frac{N}{d} = N \equiv -1 \pmod 3.$$

Det innebär antingen att $d \equiv 1 \pmod 3$ och $\frac{N}{d} \equiv -1 \pmod 3$ eller att $d \equiv -1 \pmod 3$ och $\frac{N}{d} \equiv 1 \pmod 3$. Då N enligt sats 4.1 inte kan vara en kvadrat medför detta att

$$\sigma(N) = \sum_{\substack{d|N \\ 0<d<\sqrt{N}}} \left(d + \frac{N}{d}\right) \equiv 0 \pmod 3.$$

Men

$$\sigma(N) = 2N = 2(6m-1) = 12m - 2 \equiv -2 \equiv 1 \pmod 3$$

vilket är en motsägelse och därför kan inte N ha formen $6m - 1$. ■

Lemma 5.2 Om N är ett udda perfekt tal så är $N \equiv 1 \pmod 4$.

Bevis Enligt sats 4.1 är $N = p_1^{k_1} p_2^{2j_2} \cdots p_r^{2j_r}$ där talen p_i är olika udda primtal och $p_1 \equiv k_1 \equiv 1 \pmod 4$. Vi förenklar och skriver om N till $N = p_1^{k_1} m^2$. Eftersom $p_1 \equiv 1 \pmod 4$ medför det att $p_1^{k_1} \equiv 1 \pmod 4$. m är ett udda tal vilket innebär att $m \equiv 1 \pmod 4$ eller $m \equiv 3 \pmod 4$. Om vi nu kvadrerar m får vi $m^2 \equiv 1 \pmod 4$ i båda fallen. Detta medför att

$$N = p_1^{k_1} m^2 \equiv 1 \cdot 1 \equiv 1 \pmod 4. \blacksquare$$

Sats 5.3 Om N är ett udda perfekt tal måste N ha formen $12m + 1$ eller $36m + 9$.

Bevis Enligt lemma 5.1 kan inte N ha formen $6m - 1$. Detta medför att $N = 6m + 1$ eller $N = 6m + 3$ vilket är ekvivalent med $N \equiv 1 \pmod 6$ eller $N \equiv 3 \pmod 6$. Enligt lemma 5.2 måste även $N \equiv 1 \pmod 4$. Därför är antingen $N \equiv 1 \pmod 4$ och $N \equiv 1 \pmod 6$ eller så är $N \equiv 1 \pmod 4$ och $N \equiv 3 \pmod 6$. Om vi löser dessa två kongruensekvationer samtidigt får vi att N måste ha formen $12m+1$ eller $12m+9$. Om vi tittar närmare på formen $12m+9$ och antar att $3 \nmid m$ följer det att

$$\sigma(N) = \sigma(3(4m+3)) = \sigma(3)\sigma(4m+3) = 4 \cdot \sigma(4m+3) \equiv 0 \pmod 4.$$

Detta är en motsägelse då $\sigma(N) \equiv 2 \pmod 4$. Alltså måste $3 \mid m$ och N ha formen $36m+9$. ■

6 Sylvesters resultat

Lemma 6.1 Ett udda perfekt tal N kan inte bestå av en eller två faktorer.

Bevis Antag att $N = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ där p_i är olika primtal. Vi vet att

$$\sigma(N) = \sigma(p_1^{k_1}) \cdots \sigma(p_r^{k_r}) = \left(\sum_{i=0}^{k_1} p_1^i\right) \cdots \left(\sum_{i=0}^{k_r} p_r^i\right) = 2p_1^{k_1} \cdots p_r^{k_r}$$

vilket är ekvivalent med

$$\frac{\sigma(N)}{N} = \left(\sum_{i=0}^{k_1} p_1^{-i}\right) \cdots \left(\sum_{i=0}^{k_r} p_r^{-i}\right) = 2.$$

Vi noterar att

$$\sum_{i=0}^{k} p^{-i} < \sum_{i=0}^{\infty} p^{-i} = \frac{1}{1-\frac{1}{p}} = \frac{p}{p-1}$$

och att $p/(p-1)$ är en avtagande funktion av p.

Om N består av två faktorer skall alltså följande gälla:

$$\frac{p_1}{p_1-1} \cdot \frac{p_2}{p_2-1} > \left(\sum_{i=0}^{k_1} p_1^{-i}\right)\left(\sum_{i=0}^{k_2} p_2^{-i}\right) = 2.$$

Men

$$\frac{p_1}{p_1-1} \cdot \frac{p_2}{p_2-1} \leq \frac{3}{2} \cdot \frac{5}{4} < 2$$

vilket är en motsägelse och därför kan inte udda perfekta tal bestå av två faktorer. De kan heller inte bestå av bara en faktor ty

$$\frac{p_1}{p_1-1} \leq \frac{3}{2} < 2. \blacksquare$$

Lemma 6.2 Ett udda perfekt tal N kan inte vara delbart med 105.

Bevis Antag att N är delbart med 105. 105 har primtalsfaktoriseringen $105 = 3 \cdot 5 \cdot 7$. Den enda faktorn av dessa som är kongruent med 1 modulo 4 är primtalet 5. Därför är

$$N = 5^{k_1} 3^{2j_2} 7^{2j_3} p_4^{k_4} \cdots p_r^{k_r}.$$

Eftersom $\sum_{i=0}^{k} p^{-i}$ är en växande funktion av k gäller

$$\frac{\sigma(N)}{N} \geq (1+\frac{1}{5})(1+\frac{1}{3}+\frac{1}{3^2})(1+\frac{1}{7}+\frac{1}{7^2}) > 2$$

vilket medför att N inte kan vara delbart med 105. $\blacksquare$

Lemma 6.3 Låt $a \neq 1$ vara ett heltal och p ett primtal sådant att $a \equiv 1 \pmod{p}$. Om $k \not\equiv 0 \pmod{p}$ och n är ett naturligt tal, så gäller det att talet

$$\frac{a^{kp^n}-1}{a-1}$$

är delbart med p^n men inte med p^{n+1}.

Bevis Låt $a \equiv 1 \pmod{p}$. Det innebär att vi kan skriva $a = mp+1$ för något heltal m. Låt också $k \not\equiv 0 \pmod{p}$. Vi ska gå igenom tre steg i detta bevis. Det första steget är att undersöka talet $(a^p-1)/(a-1)$. Vi ser att det är delbart med p ty

$$\frac{a^p-1}{a-1} = 1 + a + a^2 + \cdots + a^{p-1} \equiv p \equiv 0 \pmod{p}.$$

Vi noterar sedan att talet $(a^p-1)/(a-1)$ går att skriva som en summa

$$\frac{a^p-1}{a-1} = \frac{(mp+1)^p-1}{mp} = \sum_{n=0}^{\infty} p^n \binom{p}{1+n} m^n.$$

Vi ser att summan inte är delbar med p^2 ty

$$\sum_{n=0}^{\infty} p^n \binom{p}{1+n} m^n \equiv p + p\frac{p-1}{2}pm \equiv p \pmod{p^2}.$$

Alltså gäller det att

$$p \mid \frac{a^p-1}{a-1} \quad \text{och} \quad p^2 \nmid \frac{a^p-1}{a-1}. \tag{3}$$

Låt oss nu undersöka $(a^{p^n}-1)/(a-1)$. Talet går att skriva

$$\frac{a^{p^n}-1}{a-1} = \frac{a^{p^n}-1}{a^{p^{n-1}}-1} \cdot \frac{a^{p^{n-1}}-1}{a^{p^{n-2}}-1} \cdots \frac{a^p-1}{a-1}.$$

Varje faktor i högerledet, exakt n stycken, är delbar med p men inte med p^2 enligt (3). Detta medför att

$$p^n \mid \frac{a^{p^n}-1}{a-1} \quad \text{och} \quad p^{n+1} \nmid \frac{a^{p^n}-1}{a-1}. \tag{4}$$

Nu återstår det sista steget och det är att undersöka talet $(a^{kp^n}-1)/(a-1)$. Vi delar upp talet i två faktorer

$$\frac{a^{kp^n}-1}{a-1} = \frac{a^{kp^n}-1}{a^k-1} \cdot \frac{a^k-1}{a-1}.$$

Den första faktorn i högerledet delas av p^n men inte av p^{n+1} enligt (4). Eftersom $k \not\equiv 0 \pmod{p}$ och

$$\frac{a^k-1}{a-1} = 1 + a + a^2 + \cdots + a^{k-1} \equiv k \pmod{p}$$

är den andra faktorn i högerledet inte delbar med p. Detta medför att

$$p^n \mid \frac{a^{kp^n}-1}{a-1} \quad \text{och} \quad p^{n+1} \nmid \frac{a^{kp^n}-1}{a-1}. \blacksquare$$

Sats 6.4 Ett udda perfekt tal N kan inte innehålla endast tre primtalsfaktorer.

Bevis Antag att N innehåller precis tre faktorer. Vi noterar att

$$\frac{5}{4} \cdot \frac{7}{6} \cdot \frac{11}{10} < 2.$$

Eftersom $p/(p-1)$ är en avtagande funktion av p innebär det att 3 måste vara en faktor i N. Vidare är

$$\frac{3}{2} \cdot \frac{7}{6} \cdot \frac{11}{10} < 2$$

vilket av samma anledning som ovan innebär att 5 måste vara en faktor i N. Enligt lemma 6.2 kan då inte 7 vara den tredje faktorn. N måste alltså bestå av faktorerna $3, 5$ och q där $q > 7$. Vi noterar sedan att

$$\frac{3}{2} \cdot \frac{5}{4} \cdot \frac{17}{16} < 2$$

vilket innebär att $q = 11$ eller $q = 13$.

Antag att $q = 13$ och att exponenten för 13 är ett udda tal $2i+1$. Detta ger då enligt sats 2.2 divisorsumman

$$\sigma(13^{2i+1}) = \frac{13^{2i+2}-1}{13-1}.$$

Eftersom $13 \equiv -1 \pmod 7$ medför det att $13^{2i+2} \equiv 1 \pmod 7$ vilket innebär att 7 delar $\sigma(13^{2i+1})$. Detta är en motsägelse då 7 inte är en faktor i N. Exponenten för 13 är alltså ett jämnt tal. Eftersom $3 \not\equiv 1 \pmod 4$ är även exponenten för 3 ett jämnt tal och divisorsummorna för 3 och 13 kan därför skrivas

$$\frac{3^{2i+1}-1}{3-1} \quad \text{resp.} \quad \frac{13^{2j+1}-1}{13-1}. \tag{5}$$

Eftersom N är delbart med 5, måste någon av divisorsummorna (5) vara delbar med 5, ty divisorsumman för 5 är ej det. Men $3 \equiv 13 \equiv -2 \pmod 5$ vilket medför att divisorsummorna för 3 och 13 inte heller är delbara med 5 och vi har fått en motsägelse. Det vill säga $q \neq 13$.

Antag att $q = 11$. Då måste

$$N = 5^{4k+1} \cdot 3^{2j} \cdot 11^{2i}$$

ty 5 är det enda primtalet av $3, 5, 11$ som är kongruent 1 modulo 4. Vi ska nu visa att $k = 0$. Antag att $k > 0$. Då är

$$\sigma(5^{4k+1}) = \frac{5^{4k+2}-1}{5-1} = \frac{5^{2k+1}-1}{5-1} \cdot \frac{5^{2k+1}+1}{5+1} \cdot \frac{5+1}{1}.$$

Om vi granskar högerledet ser vi att alla tre faktorerna är heltal och att de två första är relativt prima. Vi ser också att

$$3 \nmid \frac{5^{2k+1}-1}{5-1} \quad \text{ty} \quad 5 \equiv -1 \pmod 3.$$

Om

$$3 \mid \frac{5^{2k+1}+1}{5+1}$$

måste $2k+1 = 3m$ enligt lemma 6.3. Det medför att $5^{2k+1}+1$ innehåller faktorn

$$5^3 + 1 = 126 = 7 \cdot 18$$

vilket är en motsägelse då $7 \nmid N$. De två första faktorerna är därför varken delbara med 3 eller 5. Eftersom de är relativt prima innehåller deras produkt två olika primtal, som alltså varken kan vara 3 eller 5. Detta ger motsägelsen att N består av fler än tre olika primtal. Det måste alltså vara så att $k = 0$ och

$$N = 5 \cdot 3^{2j} \cdot 11^{2i}.$$

Divisorsumman

$$1 + 5 = 6 = 3 \cdot 2$$

för 5 innehåller faktorn 3 en gång. Divisorsumman för 3 innehåller inte faktorn 3. Detta innebär att divisorsumman

$$\frac{11^{2i+1}-1}{11-1}$$

för 11 måste innehålla faktorn 3 minst en gång. Så är inte är fallet ty $11 \equiv -1 \pmod 3$ och vi har fått en motsägelse även denna gång.

Eftersom q varken kan vara 13 eller 11, så har vi visat att det inte finns något udda perfekt tal med bara tre faktorer. ■

Följande lemma följer direkt av lemma 6.3.

Lemma 6.5 Låt a vara ett heltal, p ett primtal och n ett naturligt tal. Om $a \equiv 1 \pmod{p}$ och p^n delar talet

$$\frac{a^{2i+1}-1}{a-1} \tag{6}$$

så gäller det att

$$\frac{1}{p^n} \cdot \frac{a^{p^n}-1}{a-1}$$

är en faktor i talet (6). Samma gäller för talet $(a^{4i+2}-1)/(a-1)$.

Definition 6.6 Låt $\phi(n)$ där $n \geq 1$ beteckna antalet positiva heltal mindre än eller lika med n som är relativt prima med n.

Definition 6.7 Låt $n > 1$ och $\gcd(a, n) = 1$. *Ordningen av a modulo n* är det minsta positiva heltal k sådant att $a^k \equiv 1 \pmod{n}$.

Lemma 6.8 Låt heltalet a ha ordningen k modulo n. Då gäller det att

$$a^h \equiv 1 \pmod{n} \iff k \mid h$$

och speciellt gäller det att $k \mid \phi(n)$.

Bevis Antag att $k \mid h$. Det innebär att $h = km$ för något heltal m. Vi får då att

$$a^h \equiv a^{km} \equiv (a^k)^m \equiv 1 \pmod{n}.$$

Antag nu i stället att $a^h \equiv 1 \pmod{n}$. Enligt divisionsalgoritmen existerar det ett q och ett r sådant att $h = qk + r$ där $0 \leq r < k$. Detta ger

$$a^h \equiv a^{qk+r} \equiv (a^k)^q a^r \equiv a^r \equiv 1 \pmod{n}.$$

Eftersom $0 \leq r < k$ och k är ordningen av a modulo n så gäller endast kongruensen ovan då $r = 0$. Det vi har kvar då är $h = qk$ vilket innebär att $k \mid h$. ■

Lemma 6.9 Om a är ett heltal och 17 delar

$$\frac{a^{2i+1}-1}{a-1} \quad \text{eller} \quad \frac{a^{4i+2}-1}{a-1}$$

så är $a^2 - 1$ delbart med 17.

Bevis Antag att $a \not\equiv 1 \pmod{17}$. Då måste $a^{2i+1} \equiv 1 \pmod{17}$ i det första fallet. Ordningen av a modulo 17 måste då dela $2i+1$. Men ordningen av a modulo 17 måste även dela $\phi(17) = 16 = 2^4$. Eftersom ordningen är större än 1 blir detta en motsägelse vilket medför att $a \equiv 1 \pmod{17}$ och $a^2 \equiv 1 \pmod{17}$.

I det andra fallet skriver vi

$$\frac{a^{4i+2}-1}{a-1} = \frac{(a^2)^{2i+1}-1}{a^2-1}(a+1).$$

Om $a^2 \not\equiv 1 \pmod{17}$ så måste 17 dela den första faktorn i högerledet, och vi får en motsägelse även i detta fall. ■

Lemma 6.10 Om 17 är en faktor i ett udda perfekt tal N, måste N innehålla någon faktor som inte understiger 67.

Bevis 17 måste dela någon av divisorsummorna

$$\frac{p^{2i+1}-1}{p-1} \quad \text{och} \quad \frac{p^{4i+2}-1}{p-1}.$$

Enligt lemma 6.9 måste då 17 antingen dela $p+1$ eller $p-1$. Det är nu lätt att se att primtalet p måste vara minst 67. ■

Lemma 6.11 Om p och q är primtal så är den största gemensamma delaren till

$$\frac{q^p-1}{q-1} \quad \text{och} \quad \frac{q^{p^2}-1}{q^p-1}$$

lika med 1 eller p.

Bevis Låt r vara ett primtal som delar båda talen. Då är $r \neq q$. Eftersom r delar det första talet så är $q^p \equiv 1 \pmod{r}$. Enligt lemma 6.3 är det andra talet därför delbart med r bara då $r = p$. Det enda primtal som kan dela båda talen är alltså p och det följer av lemma 6.3 att det andra talet inte delas av p^2.

Sats 6.12 Ett udda perfekt tal N måste innehålla minst fem olika primtalsfaktorer.

Bevis Antag att N innehåller fyra primtalsfaktorer. Vi noterar att

$$\frac{5}{4} \cdot \frac{7}{6} \cdot \frac{11}{10} \cdot \frac{13}{12} < 2$$

vilket betyder att N måste innehålla faktorn 3. Vidare är

$$\frac{3}{2} \cdot \frac{11}{10} \cdot \frac{13}{12} \cdot \frac{17}{16} < 2$$

vilket innebär att N också måste innehålla någon av faktorerna 5 och 7, men inte båda samtidigt enligt lemma 6.2.

Antag att de två minsta faktorerna i N är 3 och 7. Eftersom

$$\frac{3}{2} \cdot \frac{7}{6} \cdot \frac{17}{16} \cdot \frac{19}{18} < 2$$

måste den tredje faktorn i N vara 11 eller 13.

Antag att 11 är den tredje faktorn. Eftersom

$$\frac{3}{2} \cdot \frac{7}{6} \cdot \frac{11}{10} \cdot \frac{29}{28} < 2$$

måste den fjärde faktorn i N vara antingen $13, 17, 19$ eller 23. Enligt lemma 6.10 kan vi utesluta faktorn 17. En av faktorerna i N måste vara kongruent med 1 modulo 4 vilket medför att 13 är den fjärde faktorn och

$$N = 13^{4k+1} \cdot 3^{2j} \cdot 7^{2i} \cdot 11^{2l}. \tag{7}$$

Enligt likheten (7) måste $9 \mid N$. Vi ska nu visa att detta leder till en motsägelse.

Antag att

$$9 \mid \frac{7^{2i+1}-1}{7-1}.$$

Eftersom $7 \equiv 1 \pmod 3$ medför lemma 6.5 att divisorsumman för 7 innehåller faktorn

$$\frac{1}{9} \cdot \frac{7^9-1}{7-1}$$

som i sin tur innehåller faktorerna

$$\frac{1}{3} \cdot \frac{7^3-1}{7-1} \quad \text{och} \quad \frac{1}{3} \cdot \frac{7^9-1}{7^3-1}.$$

Enligt lemma 6.11 är faktorerna relativt prima och varken delbara med 3 eller 7. Den första faktorn är heller inte delbar med 13 ty $7^3 \not\equiv 1 \pmod{13}$. Av samma anledning så kan inte ordningen av 7 modulo 13 vara 3. Ordningen måste dela $\phi(13) = 12$ vilket innebär att den inte kan dela 9 och det visar att den andra faktorn inte heller är delbar med 13. Divisorsumman för 7 måste alltså innehålla minst två udda primtal andra än $3, 7$ och 13 vilket är en motsägelse. Alltså gäller det att

$$9 \nmid \frac{7^{2i+1}-1}{7-1}.$$

Divisorsumman

$$\frac{11^{2l+1}-1}{11-1}$$

för 11 är ej delbar med 3 ty $11 \equiv -1 \pmod 3$. Eftersom divisorsumman för 3 inte heller är delbar med 3 måste det vara så att

$$3 \mid \frac{13^{4k+2}-1}{13-1}.$$

Eftersom $13 \equiv 1 \pmod 3$ måste då enligt lemma 6.5 divisorsumman för 13 innehålla faktorn

$$\frac{1}{3} \cdot \frac{13^3-1}{13-1} = 61.$$

Talet N måste då alltså innehålla minst fem primtalsfaktorer vilket är en motsägelse och primtalet 11 kan alltså inte vara den tredje faktorn i N.

Antag att den tredje faktorn i N är 13. Eftersom

$$\frac{3}{2} \cdot \frac{7}{6} \cdot \frac{13}{12} \cdot \frac{23}{22} < 2$$

måste den fjärde faktorn i N vara 17 eller 19, men enligt lemma 6.10 kan vi bortse från 17. De fyra faktorerna är då $3, 7, 13$ och 19. Eftersom 13 är den enda faktorn som är kongruent med 1 modulo 4 så är

$$N = 13^{4k+1} \cdot 3^{2j} \cdot 7^{2i} \cdot 19^{2l}. \tag{8}$$

Enligt likheten (8) måste $9 \mid N$. Vi ska nu visa att detta leder till en motsägelse.

Antag att

$$3 \mid \frac{13^{4k+2}-1}{13-1}.$$

Eftersom $13 \equiv 1 \pmod 3$ måste då enligt lemma 6.5 divisorsumman för 13 innehålla faktorn

$$\frac{1}{3} \cdot \frac{13^3-1}{13-1} = 61.$$

Detta är en motsägelse och medför att

$$3 \nmid \frac{13^{4k+2}-1}{13-1}.$$

Samma gäller för divisorsumman för 19. Om divisorsumman för 19 är delbar med 3 måste den enligt lemma 6.5 innehålla faktorn

$$\frac{1}{3} \cdot \frac{19^3-1}{19-1} = 127$$

vilket också är en motsägelse och det medför att

$$3 \nmid \frac{19^{2l+1}-1}{19-1}.$$

Eftersom varken divisorsumman för $3, 13$ eller 19 är delbar med 3 måste alltså divisorsumman för 7 innehålla faktorn 9. Antag att så är fallet. Enligt lemma 6.5 innehåller då divisorsumman för 7 följande faktorer

$$\frac{1}{3} \cdot \frac{7^3-1}{7-1} \quad \text{och} \quad \frac{1}{3} \cdot \frac{7^9-1}{7^3-1}.$$

Som tidigare visats är ingen av faktorerna delbar med $3, 7$ eller 13. Eftersom faktorerna är relativt prima och den första faktorn är lika med 19 så kan den andra faktorn inte heller vara delbar med 19. Detta visar att N måste innehålla minst fem primfaktorer, vilket är en motsägelse och den fjärde faktorn i N kan alltså inte vara 13.

Vi har nu visat att de två minsta faktorerna i N inte kan vara 3 och 7. Antag i stället att 3 och 5 är de minsta faktorerna i N. Antag också att 5 är den faktor i N som är upphöjd till $4k+1$.

Antag sedan att exponenten för faktorn 3 är 2. Divisorsumman för 3 är då

$$\frac{3^{2+1}-1}{3-1} = 13.$$

13 måste alltså vara den tredje faktorn i N. Divisorsumman för 5 är

$$\frac{5^{4k+2}-1}{5-1}.$$

Antag att $k > 0$. Eftersom

$$5^4 \equiv 1 \pmod{13} \quad \text{och} \quad 5^2 \equiv -1 \pmod{13}$$

medför det att divisorsumman för 5 inte är delbar med 13. Så som tidigare finner vi nu att divisorsumman för 5 måste innehålla två primtalsfaktorer andra än $3, 5$ och 13, vilket är en motsägelse. Alltså måste $k = 0$ och divisorsumman för 5 vara lika med $5 + 1 = 6$.

Antag att divisorsumman för 13 inte innehåller faktorn 3. Eftersom divisorsumman för 3 inte innehåller faktorn 3 och divisorsumman för 5 bara innehåller faktorn 3 en gång måste 3 ingå i divisorsumman för en fjärde primtalsfaktor p i N. Eftersom p inte kan vara 7 enligt lemma 6.2 så är det minsta möjliga värdet på p lika med 19. Om $p \geq 19$ så gäller det att

$$\frac{1+3+3^2}{9} \cdot \frac{1+5}{5} \cdot \frac{13}{12} \cdot \frac{p}{p-1} \leq \frac{1+3+3^2}{9} \cdot \frac{1+5}{5} \cdot \frac{13}{12} \cdot \frac{19}{18} < 2. \tag{9}$$

Detta visar att divisorsumman för 13 måste innehålla faktorn 3. Enligt lemma 6.5 måste då divisorsumman för 13 också innehålla faktorn

$$\frac{1}{3} \cdot \frac{13^3 - 1}{13 - 1} = 61.$$

Detta innebär att N måste innehålla samma faktor vilket är en motsägelse enligt olikheten (9). Exponenten för 3 kan alltså inte vara lika med 2.

Antag att exponenten för 3 är minst 4.

Vi har tidigare sett att divisorsumman för 5 bara kan innehålla faktorn 3 en gång. Vi vet också att divisorsumman för 3 inte innehåller 3, därför måste divisorsumman för en annan faktor p i N innehålla faktorn 3. Alltså måste $p \equiv 1 \pmod 3$. Om divisorsumman innehåller faktorn $3^2 = 9$ innehåller den också enligt lemma 6.5 faktorn

$$\frac{1}{9} \cdot \frac{p^9 - 1}{p - 1}$$

som i sin tur innehåller faktorerna

$$\frac{1}{3} \cdot \frac{p^9 - 1}{p^3 - 1} \quad \text{och} \quad \frac{1}{3} \cdot \frac{p^3 - 1}{p - 1}. \tag{10}$$

Enligt lemma 6.11 är de relativt prima och inte delbara med p eller 3.

Antag att 5 delar divisorsumman för p. Då måste $p \not\equiv -1 \pmod 5$. Om $p \equiv 2 \pmod 5$ är $p^9 \equiv 2 \pmod 5$. Om $p \equiv -2 \pmod 5$ så är $p^9 \equiv 3 \pmod 5$. För att 5 ska dela summan krävs det alltså att $p \equiv 1 \pmod 5$. Eftersom $5 \nmid 9$ kan det enligt lemma 6.3 inte vara så att 5 delar divisorsumman. Varken $3, 5$ eller p delar alltså faktorerna (10), därför måste deras produkt innehålla två andra primtal än dessa. Detta är en motsägelse då N bara innehåller fyra primtal och därför kan divisorsumman för p alltså bara innehålla faktorn 3 en gång. Samma sak måste gälla för den fjärde faktorn q. Faktorn 3 kan alltså bara ingå i N högst tre gånger, vilket är en motsägelse.

Vi har nu visat att elementet 5 inte kan vara upphöjt till $4k + 1$. Antag därför att exponenten för 5 är 2j.

Vi noterar att

$$\frac{3}{2} \cdot \frac{5}{4} \cdot \frac{31}{30} \cdot \frac{37}{36} < 2.$$

Detta medför att N måste innehålla ett primtal p, där $p \leq 29$. Vi ska nu visa att p inte kan dela divisionsumman för 5. Antag motsatsen, det vill säga, antag att

$$p \mid \frac{5^{2j+1} - 1}{5 - 1}.$$

Låt m vara ordningen för elementet 5 modulo p. Då gäller det att m måste vara udda och $m \mid (p-1)$. Eftersom p är något av primtalen $11, 13, 17, 19, 23, 29$ måste m vara något av talen $3, 5, 7, 9, 11$, där de fyra sista endast motsvarar talen $11, 29, 19$ resp. 23.

Det kan inte vara så att $m = 3$ är ordningen för p eftersom $(5^3 - 1)/(5 - 1) = 31$ inte är delbar med p.

Antag att ordningen är $m = 5$. Då måste $(5^5 - 1)/(5 - 1) = 11 \cdot 71$ dela divisorsumman. Alltså måste N innehålla faktorerna $3, 5, 11$, och 71. Men eftersom alla faktorerna utom 5 är kongruenta med 3 modulo 4 så har vi en motsägelse och ordningen kan alltså inte vara 5.

Antag att ordningen är $m = 7$. Då är $p = 29$. Men eftersom

$$5^7 \equiv (-4)^3 \cdot 5 \equiv -1 \pmod{29}$$

kan inte ordningen vara 7.

Antag att ordningen är $m = 9$. Då är $p = 19$. $19 \mid (5^9 - 1)$ och eftersom $(5^3 - 1)/(5 - 1) = 31$ också är en delare måste N innehålla faktorerna $3, 5, 19$ och 31. Då alla faktorerna utom 5 är kongruenta med 3 modulo 4 har vi en motsägelse och ordningen kan alltså inte vara 9.

Då återstår bara fallet $m = 11$. Om ordningen är 11 måste $p = 23$. Eftersom

$$5^{11} \equiv (2)^5 \cdot 5 \equiv -1 \pmod{23}$$

kan heller inte ordningen vara 11.

Vi har därmed visat att p inte kan dela divisorsumman för 5.

Antag att q^{4k+1} är en faktor i N. Vi skall då visa att $k = 0$. Antag att $k > 0$. Då kan divisorsumman för q skrivas

$$\frac{q^{4k+2} - 1}{q - 1} = -\frac{q^{2k+1} - 1}{q - 1} \cdot \frac{(-q)^{2k+1} - 1}{(-q) - 1} \cdot (q + 1). \tag{11}$$

Det är lätt att se att de två första faktorerna i högerledet är relativt prima. Låt r vara något av primtalen 3 och 5. För att r ska dela den första faktorn i högerledet måste $q \equiv 1 \pmod{r}$. Enligt lemma 6.5 följer det då att den första faktorn innehåller

$$\frac{1}{r} \cdot \frac{q^r - 1}{q - 1}$$

som i sin tur inte innehåller faktorn r. Skulle den första faktorn vara delbar med både 3 och 5 följer det att faktorn måste delas av

$$\frac{1}{15} \cdot \frac{q^{15} - 1}{q - 1}$$

som i sin tur varken delas av 3 eller 5. Samma resonemang kan användas på den andra faktorn i högerledet i ekvationen (11). Divisorsumman måste alltså vara delbar med två primtal andra än $3, 5$ och q, vilket är en motsägelse och $k = 0$. Divisorsumman för q blir då $q + 1$.

Låt p vara den tredje faktorn förutom 3 och 5 som är upphöjd till $2j$. Om divisorsumman för p innehåller faktorn 3 två gånger men inte faktorn 5, innehåller den faktorerna

$$\frac{1}{3} \cdot \frac{p^9 - 1}{p^3 - 1} \quad \text{och} \quad \frac{1}{3} \cdot \frac{p^3 - 1}{p - 1}$$

enligt lemma 6.5. Enligt lemma 6.11 är de båda faktorerna relativt prima och varken delbara med $3, 5$ eller p. Det finns alltså ytterligare två primtalsfaktorer som ingår i faktoriseringen av N vilket är en motsägelse.

På samma sätt visas att divisorsumman för p inte kan innehålla faktorn 5 två gånger samtidigt som den inte innehåller faktorn 3.

Antag att $3 \cdot 5$ ingår i divisorsumman av p. Då innehåller den faktorerna

$$\frac{1}{3} \cdot \frac{(p^5)^3 - 1}{p^5 - 1} \quad \text{och} \quad \frac{1}{5} \cdot \frac{p^5 - 1}{p - 1}$$

som är relativt prima och inte delbara med $3, 5$ eller p. Detta ger samma motsägelse som tidigare och divisorsumman för p kan inte innehålla faktorn $3 \cdot 5$.

Divisorsumman för det exceptionella talet q och divisorsumman för p måste tillsammans innehålla faktorn 3 två gånger och faktorn 5 två gånger eftersom divisorsummorna för 3 och 5 inte innehåller just de faktorerna. Som vi just har visat kan divisorsumman p bara innehålla

faktorerna 3 och 5 högst en gång och inte båda samtidigt och därför måste divisorsumman för q innehålla faktorn $3^2 \cdot 5$ eller $3 \cdot 5^2$. Det exceptionella talet q är alltså

$$q = 2k \cdot 3^2 \cdot 5 - 1 \quad \text{eller} \quad q = 2k \cdot 3 \cdot 5^2 - 1.$$

Vi ser nu att $q \geq 89$ vilket innebär att $q \neq p$ där $p \leq 29$ är det primtal vi diskuterade tidigare och vi kan skriva $q = 30\lambda - 1$.

Eftersom N bara innehåller primtalet q en gång och divisorsumman för 5 inte innehåller faktorerna $3, 5$ eller p, måste divisorsumman för 5 innehålla q och inte några andra primtalsfaktorer. Detta medför att

$$\frac{5^t - 1}{5 - 1} = q = 30\lambda - 1$$

för något positivt heltal t. Det följer att

$$5^t - 120\lambda + 3 = 0$$

vilket är omöjligt.

Beviset är nu slutfört. ■

7 Primtalsfaktorernas storlek

Definition 7.1 Låt n vara ett naturligt tal och p är ett primtal. Om $u \geq 0$ skriver vi $p^u \,||\, n$ om

$$p^u \mid n \quad \text{och} \quad p^{u+1} \nmid n.$$

Sats 7.2 Låt p vara en primtalsfaktor i ett udda perfekt tal N. Då gäller det att

$$p < (3N)^{1/3}.$$

Bevis Vi noterar först att

$$\sigma(y) < \frac{3y}{2} \tag{12}$$

om y är en potens av ett udda primtal.

Antag att $p^j \,||\, N$. Vi betraktar först fallet $j \geq 2$. Det gäller att $\sigma(p^j) \mid 2N$, ty σ är en multiplikativ funktion. Eftersom p^j och $\sigma(p^j)$ är relativt prima gäller det att $2N = \sigma(N)$ är delbar med

$$p^j \sigma(p^j) > p^{2j} \geq p^4$$

vilket medför att

$$p < (2N)^{1/4}.$$

Antag nu att $j = 1$. Då måste p vara det exceptionella elementet. Eftersom p inte delar sin divisorsumma, måste p dela $\sigma(q^{2i})$ för någon ordinär primtalsfaktor q till N, sådan att $q^{2i} \,||\, N$. Vi kan skriva

$$N = pq^{2i}m^2.$$

Antag att $q \nmid \sigma(p)$. Vi vet också att $p \nmid \sigma(p)$, vilket medför att

$$p \cdot q^{2i} \mid \sigma(q^{2i}m^2). \tag{13}$$

Med (13) och (12) får vi

$$2N = \sigma(N) = (p+1)\sigma(q^{2i}m^2) > p^2 \cdot q^{2i} > \frac{2p^2\sigma(q^{2i})}{3} \geq \frac{2p^3}{3}$$

vilket medför att $(3N)^{1/3} > p$.

Antag nu att $q \mid \sigma(p)$. Beteckna $u = \sigma(q^{2i})/p$. Eftersom

$$\sigma(q^{2i}) \equiv 1 \pmod{q} \quad \text{och} \quad p \equiv -1 \pmod{q}$$

medför det att

$$u \equiv -1 \pmod{q}.$$

Efterson u är ett udda tal gäller också att $u \neq q-1$ vilket medför

$$u \geq 2q - 1. \tag{14}$$

Låt $q^k \mid\mid \sigma(p)$ där $k \geq 1$. k är alltså antalet primtalsfaktorer q som ingår i $\sigma(p)$. Resten av faktorerna q, dvs $2i-k$ stycken, måste ingå i $\sigma(m^2)$, ty $q \nmid \sigma(q)$. Alltså gäller det att

$$q^{2i-k} \mid\mid \sigma(m^2) \quad \text{där} \quad k \leq 2i$$

och

$$\sigma(m^2) \geq q^{2i-k}. \tag{15}$$

Vi har nu att

$$q^{2i+1} - 1 = (q-1)\sigma(q^{2i}) = (q-1)up = (q-1)u\sigma(p) - (q-1)u$$

vilket medför att

$$(q-1)u \equiv 1 \pmod{q^k}$$

som i sin tur medför

$$(q-1)u > q^k. \tag{16}$$

Olikheterna (15) och (16) ger tillsammans olikheten

$$u\sigma(m^2) > \frac{q^{2i}}{q-1}. \tag{17}$$

Vi har nu

$$2N = \sigma(N) = \sigma(p)\sigma(q^{2i})\sigma(m^2) = (p+1)up\sigma(m^2).$$

Detta tillsammans med (17), (12) och (14) medför att

$$2N > \frac{q^{2i} \cdot p^2}{q-1} > \frac{2\sigma(q^{2i})p^2}{3(q-1)} = \frac{2up^3}{3(q-1)} \geq \frac{2(2q-1)p^3}{3(q-1)} > \frac{4p^3}{3}.$$

Vi får alltså att $p < (\frac{3N}{2})^{1/3}$ och beviset är nu komplett. ■

8 Dicksons resultat

Definition 8.1 Antag att (x_n) är en följd av element i det kompakta metriserbara rummet $\mathbb{R} \cup \{\infty\} = \hat{\mathbb{R}}$, där $\{\infty\}$ är ett element. Då gäller följande

$$x_n \to a \quad \text{då} \quad n \to \infty$$

om a är ett reellt tal och om $x_n \to a$ i vanlig mening och

$$x_n \to \infty \quad \text{då} \quad n \to \infty$$

om $|x_n| \to \infty$ då $n \to \infty$ i vanlig mening.

Definition 8.2 Låt $\mathbb{N}$ beteckna mängden av alla naturliga tal. Vi säger att N är ett *supernaturligt tal* om

$$N = \prod_p p^{\nu_p} = p_1^{\nu_{p_1}} p_2^{\nu_{p_2}} p_3^{\nu_{p_3}} \cdots$$

där p_i är följden av primtal uppräknade i storleksordning och varje $\nu_{p_i} \in \mathbb{N} \cup \{\infty\} = \hat{\mathbb{N}}$. Vi betecknar mängden av alla supernaturliga tal med $\mathcal{S}$ och skriver $\nu_p(N)$ för exponenten till p i N.

Anmärkning 8.3 Alla udda perfekta tal är supernaturliga tal.

Definition 8.4 Om N och D är supernaturliga tal säger vi att D är en *enhetsdelare* till N och skriver $D \mid\mid N$ om $\nu_p(D) = \nu_p(N)$ för varje primtal p som delar D.

Lemma 8.5 $\hat{\mathbb{N}}$ är en sluten delmängd i $\hat{\mathbb{R}}$ och eftersom $\hat{\mathbb{R}}$ är ett kompakt metriserbart rum så är också $\hat{\mathbb{N}}$ det, vilket medför att varje följd i $\hat{\mathbb{N}}$ har en konvergent delföljd.

Vi kan identifiera varje supernaturligt tal med följden av exponenter, dvs

$$p_1^{\nu_{p_1}} p_2^{\nu_{p_2}} p_3^{\nu_{p_3}} \cdots \sim (\nu_{p_1}, \nu_{p_2}, \nu_{p_3}, \ldots)$$

där varje $\nu_{p_i} \in \hat{\mathbb{N}}$. Alltså gäller följande:

$$\mathcal{S} \sim \prod_p \hat{\mathbb{N}}_p = \hat{\mathbb{N}} \times \hat{\mathbb{N}} \times \hat{\mathbb{N}} \times \cdots .$$

Att en följd N_i konvergerar mot ett supernaturligt tal N_∞ tolkar vi som att

$$(\nu_{p_{i1}}, \nu_{p_{i2}}, \nu_{p_{i3}}, \ldots) \to (\nu_{p_1}, \nu_{p_2}, \nu_{p_3}, \ldots)$$

med punktvis konvergens. Med hjälp av lemma 8.5 kan man visa följande lemma.

Lemma 8.6 Varje följd av supernaturliga tal har en konvergent delföljd.

Definition 8.7 Givet ett positivt heltal n, låt $\omega(n)$ vara antalet olika primtalsfaktorer i n,

$$\omega(n) = \sum_{p \mid n} 1.$$

Sats 8.8 För varje positivt heltal k finns högst ändligt många udda perfekta tal N med $\omega(N) \leq k$.

Bevis Låt k vara fixt och antag att det finns oändligt många udda perfekta tal N med $\omega(N) \leq k$. Låt N_i vara en oändlig följd av olika sådana udda perfekta tal N. Följden har en konvergent delföljd enligt lemma 8.6 och vi kan anta att $N_i \to N_\infty$ där $N_\infty \in \mathcal{S}$. Eftersom $\omega(N_i) \leq k$ för alla i medför det att $\omega(N_\infty) \leq k$ och vi kan skriva

$$N_\infty = N' N''^{\infty}$$

där N' är produkten av de primtalspotenser vilkas exponenter stabiliseras då $i \to \infty$ och N'' produkten av de primtal vilkas exponenter går mot oändligheten. Låt oss kalla de primtalsfaktorerna som ingår i N' för q och de som ingår i N'' för r. Vi ser att N' och N'' är relativt

prima och att deras produkt är ett udda tal. Vi kan också anta att N'' inte innehåller några kvadrater.

Låt $h(n) = \sigma(n)/n$. Då är $h(n) = 2$ då n är ett perfekt tal och vi definierar

$$h(p^\infty) = \lim_{\nu\to\infty} h(p^\nu) = \lim_{\nu\to\infty}\left(1 + \frac{1}{p} + \cdots + \frac{1}{p^\nu}\right) = \frac{p}{p-1}.$$

Vi vet att $N' \mid\mid N_i$ för alla utom ändligt många i och att $N' = N_i$ för högst ett i. N' är alltså en äkta delare till N_i för alla stora i. Detta medför att

$$h(N') < h(N_i) = 2.$$

Eftersom $h(N_\infty) = 2$ innebär det att $N' \neq N_\infty$ och $N'' > 1$. Det existerar alltså minst en primtalsfaktor r i N''. Vi har nu

$$2 = h(N_\infty) = h(N')h(N''^\infty) = \prod_q \left(\frac{q^{\nu_q+1}-1}{q^{\nu_q}(q-1)}\right)\prod_r \frac{r}{r-1}$$

vilket är ekvivalent med

$$2\left(\prod_q q^{\nu_q}\right)\prod_r (r-1) = \prod_q \left(\frac{q^{\nu_q+1}-1}{q-1}\right)\prod_r r.$$

Detta medför att

$$\prod_r r \mid \prod_r (r-1)$$

ty varje r och $2\prod_q q^{\nu_q}$ är relativt prima. Men detta är omöjligt och vi har fått en motsägelse, vilket innebär att det endast finns högst ändligt många udda perfekta tal N med $\omega(N) \leq k$. ■

Referenser

[1] Acquaah, P., Konyagin, S. (2012). *On Prime Factors of Odd Perfect Numbers.* International Journal of Number Theory, 8(6), 1537–1540

[2] Burton, D. M. (2011). *Elementary Number Theory, Seventh Edition.* New York: McGraw-Hill

[3] Dickson, L. E. (1913). *Finiteness of the Odd Perfect and Primitive Abundant Numbers with n Distinct Prime Factors.* American Journal of Mathematics, 35(4), 413–422

[4] Holdener, J. A. (2002). *A theorem of Touchard on the Form of Odd Perfect Numbers.* The American Mathematical Monthly, 109(7), 661–663

[5] Miller, S. (2004). *Reading Classics: Euler.* Ohio State University

[6] Nielsen, P. P. (2007) *Odd Perfect Numbers Have at Least Nine Distinct Prime Factors.* Mathematics of Computation, 76, 2109–2126

[7] Ochem, P., Rao, M. (2012). *Odd Perfect Numbers Are Greater Than* 10^{1500}. Mathematics of Computation, 81 , 1869–1877

[8] Pollack, P. (2012). *Finiteness Theorems for Perfect Numbers and Their Kin.* The American Mathematical Monthly, 119(8), 670–681

[9] Sylvester, J. J. (1888). *Comptes Rendus.* CVI, 403–405, 446–450, 552–526, 641–642

[10] Sylvester, J. J. (1888). *Mathesis.* VIIL, 57–61

[11] Sylvester, J. J. (1912) *The Collected Mathematical Papers of James Joseph Sylvester.* Cambridge: University Press

[12] Van der Pol, P. (1951). *On a Non-linear Partial Differential Equation Satisfied by the Logarithm of the Jacobian Theta-functions, With Arithmetical Applications* I, II. Nederl. Akad. Wetensch. Proc. Ser. A. 54 = Indag. Math. 13(1951), 261–271, 272–284.