A. Appendix: Løse ender.

(A.1). I dette appendix giver vi et bevis for Bertrand's Postulat, nævnt i Kapitel 1. Som nævnt følger Postulatet af en tilstrækkelig nøjagtig vurdering af primtalsfunktionen $\pi(x)$. I forbindelse med primtallenes fordeling er der en række andre funktioner, der spiller en vigtig rolle, bl.a. følgende:

$$\vartheta(x) = \sum_{p \leqslant x} \log p \qquad \text{og} \qquad \psi(x) = \sum_{p^m \leqslant x} \log p.$$

Den første sum er over alle primtal $p \leqslant x$, den anden over alle primtalspotenser $p^m \leqslant x$. I den første sum er antallet af led lig med $\pi(x)$, og hvert led er højst lig med $\log x$. Altså er $\vartheta(x) \leqslant \pi(x) \log x$. Vurderinger af vurderinger af $\pi(x)$ medfører altså vurderinger af $\vartheta(x)$, og omvendt. Det er ikke så dybtliggende at vise, at

$$\pi(x) \log x \sim \vartheta(x) \sim \psi(x).$$

Primtalssætningen er altså ækvivalent med enhver af relationerne $\vartheta(x) \sim x$ og $\psi(x) \sim x$. Af vurderingen i Kapitel 1 følger, at $\vartheta(n) \leqslant 3n$ for alle $n \geqslant 1$. Den efterfølgende vurdering er lidt bedre; vi vil bruge den i beviset for Bertrand's Postulat.

(A.2) Sætning. *For alle $n \geqslant 1$ er $\vartheta(n) \leqslant (2\log 2)n$.*

Bevis. Beviset, ganske parallelt til beviset for (1.5), forløber ved fuldstændig induktion efter n. Uligheden er trivielt opfyldt for $n = 1$.

Lad der nu være givet en værdi $n > 1$, og antag, at uligheden gælder for alle mindre værdier. Sæt $k := \lfloor (n+1)/2 \rfloor$. Specielt er så $n/2 \leqslant k \leqslant (n+1)/2$. Betragt binomialkoefficienten,

$$b := \binom{n}{n-k} = \frac{n(n-1)\cdots(k+1)}{(n-k)(n-k-1)\cdot\cdots\cdot 2\cdot 1}.$$

Da $k+1 > n-k$, er faktorerne i tælleren er større end faktorerne i nævneren. Specielt kan primtallene blandt faktorerne i tælleren ikke forkortes med faktorer fra nævneren. Derfor er b delelig med produktet af disse primtal, og følgelig er $\log b$ mindst lig med logaritmen til produktet, dvs mindst lig med $\sum \log p$, hvor summen er over primtallene p med $k < p \leqslant n$. Den sidste sum er øjensynlig lig med $\vartheta(n) - \vartheta(k)$. Altså er

$$\vartheta(n) - \vartheta(k) \leqslant \log b.$$

Videre er b, som en binomialkoefficienterne $\binom{n}{l}$ for $n \geqslant 1$, højst lig med 2^{n-1}. Under brug af induktionsforudsætningen får vi derfor, at

$$\begin{aligned}\vartheta(n) = \vartheta(n) - \vartheta(k) + \vartheta(k) &\leqslant \log 2^{n-1} + (2\log 2)k \\ &\leqslant (n-1)\log 2 + (2\log 2)(n+1)/2 = (2\log 2)n,\end{aligned}$$

som ønsket. □

(A.3) Bertand's Postulat. *For ethvert* $n \geqslant 1$ *findes et primtal* p *med* $n < p \leqslant 2n$.

Bevis. Uligheden $p \leqslant 2n$ må naturligvis være skarp, med mindre $n = 1$ og $p = 2$.

Af postulatet fremgår specielt, at hvis p_k er det k'te primtal, så er $p_{k+1} < 2p_k$. Den sidste påstand er faktisk ækvivalent med Bertrand's postulat. Mere generelt er det let at se, at hvis $q_1, q_2, q_3, \dots$ er en voksende følge af primtal, der opfylder ulighederne $q_k < 2q_{k-1}$ for $k = 2, \dots, l$, så gælder Bertrand's Postulat for alle n med $q_1/2 \leqslant n < q_l$. Øjensynlig er uligheden $q_k < 2q_{k-1}$ opfyldt for det k'te primtal i følgen,

$$3, 5, 7, 13, 23, 43, 83, 163, 317, 631.$$

Derfor gælder Bertrand's postulat for alle $n < 631$.

Nu vises påstanden med et indirekte bevis. Antag, at der for et naturligt tal n ikke findes primtal p med $n < p \leqslant 2n$. Specielt er så $n \geqslant 631$. Betragt binomialkoefficienten,

$$b = \binom{2n}{n} = \frac{(2n)(2n-1)\cdots(n+1)}{n(n-1)\cdots 2{\cdot}1}.$$

Lad p være en primdivisor i b, og lad p^{ν_p} være den potens, der indgår i primopløsningen af b. Af antagelsen følger, at ingen af faktorerne i tælleren er primtal. Derfor er $p \leqslant n$. Yderligere er $p \leqslant \frac{2}{3}n$. Et primtal q med $\frac{2}{3}n < q \leqslant n$ forekommer nemlig én gang blandt faktorerne i nævneren, og i tælleren går q kun op i faktoren $2q$. De to forekomster af q forkortes mod hinanden; derfor er b ikke delelig med q.

Altså er $p \leqslant \frac{2}{3}n$ for enhver primfaktor p i b. Af (A.2) følger derfor:

$$\sum_{p\,|\,b} \log p \leqslant \sum_{p \leqslant \frac{2}{3}n} \log p = \vartheta(\tfrac{2}{3}n) \leqslant (\tfrac{4}{3}\log 2)n.$$

Da $p^{\nu_p} \,|\, b$, følger det af (1.6), at $p^{\nu_p} \leqslant 2n$. Hvis $\nu_p \geqslant 2$, så er $p^2 \leqslant 2n$, og derfor er $p \leqslant \sqrt{2n}$; specielt er der højst $\sqrt{2n}$ primdivisorer p i b med $\nu_p \geqslant 2$, og for hver af dem er $\nu_p \log p \leqslant \log(2n)$. Derfor får vi vurderingen,

$$\sum_{p\,|\,b,\ \nu_p \geqslant 2} \nu_p \log p \leqslant \sqrt{2n}\log(2n).$$

Heraf fås:

$$\log b \leqslant \sum_{p\,|\,b,\ \nu_p \geqslant 1} \log p + \sum_{p\,|\,b,\ \nu_p \geqslant 2} \log p \leqslant (\tfrac{4}{3}\log 2)n + \sqrt{2n}\log(2n). \tag{A.3.1}$$

På den anden side giver binomialformlen:

$$2^{2n} = 2 + \binom{2n}{1} + \binom{2n}{2} + \cdots \binom{2n}{2n-1},$$

hvor de to yderste binomialkoefficienter er slået sammen til $1+1=2$. Der er $2n$ led på højesiden, og b er det største. Derfor er $2^{2n} \leqslant (2n)b$, og altså

$$(2\log 2)n \leqslant \log(2n) + \log b. \tag{A.3.2}$$

Af (A.3.1) og (A.3.2) følger:

$$(2\log 2)n - \log(2n) < \log b < (\tfrac{4}{3}\log 2)n + \sqrt{2n}\log(2n).$$

Den opnåede ulighed kan omskrives til $(\frac{2}{3}\log 2)n \leqslant (1+\sqrt{2n})\log(2n)$, eller

$$\tfrac{1}{3}\log 2 \leqslant \frac{1+\sqrt{2n}}{\sqrt{2n}}\,\frac{\log(2n)}{\sqrt{2n}}\,.$$

De to brøker på højresiden er aftagende som funktioner af n (den sidste for $2n \geqslant e^2$). Værdien på højresiden, for $n \geqslant 631$, er derfor mindre end værdien for $n = 512 = 2^9$. Altså er

$$\tfrac{1}{3}\log 2 < \frac{1+2^5}{2^5}\,\frac{10\log 2}{2^5} = \tfrac{330}{1024}\log 2.$$

Men den ulighed er øjensynlig gal. Hermed er den søgte modstrid opnået, hvormed Bertrand's Postulat er bevist. ▯

(A.4) Sætning. *For alle naturlige tal* $n \geqslant 7$ *er* $(\log 2)n \leqslant \psi(n)$. *Ækvivalent, hvis* $\mathrm{LCM}(n)$ *betegner det mindste fælles multiplum af alle tallene* $1, 2, \ldots, n$*, så er*

$$2^n \leqslant \mathrm{LCM}(n) \quad \textit{for } n \geqslant 7. \tag{A.4.1}$$

Bevis. (Efter [Nair].) Det mindste fælles multiplum $\mathrm{LCM}(n)$ er øjensynlig lig med produktet af primtalspotenserne $p^k \leqslant n$ med, for hvert primtal p, den størst mulige eksponent k. Alternativt er $\mathrm{LCM}(n)$ lig med produktet af primfaktorer p, hvor hver faktor p medtages én gang for potens p^m med $p^m \leqslant n$. Med den alternative beskrivelse er det klart, at $\log \mathrm{LCM}(n) = \psi(n)$. Derfor er de to anførte uligheder ækvivalente.

Beviset for den sidste ulighed tager udgangspunkt i følgende formel, for $1 \leqslant k \leqslant n$:

$$\sum_{r=0}^{n-k} (-1)^r \binom{n-k}{r} \frac{1}{r+k} = \frac{1}{k\binom{n}{k}}\,.$$

For at vise formlen bemærkes, at begge formlens sider er lig med det bestemte integral $I := \int_0^1 x^{k-1}(1-x)^{n-k}dx$: At integralet er lig med venstresiden fås ved at anvende binomialformlen på faktoren $(1-x)^{n-k}$ og så integrere de fremkomne potenser x^i. At integralet er lig med højresiden ses ved gentagne partielle integrationer: integrer potensen x^i og differentier potensen $(1-x)^j$.

For at vise den anførte ulighed bemærkes, at alle nævnerne $r+k$ på venstresiden er mindre end eller lig med n. Derfor er alle nævnerne $r+k$ divisorer i $\mathrm{LCM}(n)$. Multipliceres med $\mathrm{LCM}(n)$, fås altså et helt tal ud fra venstresiden, og derfor også ud fra højresiden. Det sidste betyder, at nævneren på højresiden er divisor i $\mathrm{LCM}(n)$, altså

$$k\binom{n}{k} \,\Big|\, \mathrm{LCM}(n). \tag{A.4.2}$$

Relationen (A.4.2) medfører følgende to relationer, for $k \geqslant 1$:

$$k\binom{2k}{k} \,\Big|\, \mathrm{LCM}(2k+1) \qquad \text{og} \qquad (2k+1)\binom{2k}{k} \,\Big|\, \mathrm{LCM}(2k+1). \tag{A.4.3}$$

Den første relation i (A.4.3) fås nemlig ved at anvende (A.4.2) med $n := 2k$ og udnytte, at $\mathrm{LCM}(2k) \,\big|\, \mathrm{LCM}(2k+1)$. Den anden relation i (A.4.3) fås ved at anvende (A.4.2) med $n := 2k+1$ og $k := k+1$; udnyt, at $(k+1)\binom{2k+1}{k+1} = (2k+1)\binom{2k}{k}$.

I de to relationer i (A.4.3) er de to faktorer k og $2k+1$ primiske. De to relationer medfører derfor følgende:

$$k(2k+1)\binom{2k}{k} \,\Big|\, \mathrm{LCM}(2k+1). \tag{A.4.4}$$

Øjensynlig er $2^{2k} = \sum_i \binom{2k}{i}$. I summen er der $2k+1$ binomialkoefficienter $\binom{2k}{i}$ for $i = 0, \dots, 2k$, og af dem er $\binom{2k}{k}$ den største. Derfor er $2^{2k} \leqslant (2k+1)\binom{2k}{k}$. Relationen i (A.4.4) medfører derfor uligheden,

$$k2^{2k} \leqslant \mathrm{LCM}(2k+1). \tag{A.4.5}$$

Heraf ses, for $k \geqslant 2$, at $2^{2k+1} \leqslant \mathrm{LCM}(2k+1)$; uligheden (A.4.1) gælder derfor, når n er ulige og $n \geqslant 5$. Videre er $\mathrm{LCM}(2k+1) \leqslant \mathrm{LCM}(2k+2)$, så af (A.4.5) følger, for $k \geqslant 4$, at $2^{2k+2} \leqslant \mathrm{LCM}(2k+2)$; uligheden (A.4.1) gælder derfor, når n er lige og $n \geqslant 10$. I området $n \geqslant 7$ mangler altså kun uligheden for $n = 8$. Her finder vi:

$$2^8 = 2^3 \cdot 2 \cdot 2^2 \cdot 2^2 \leqslant 2^3 \cdot 3 \cdot 5 \cdot 7 = \mathrm{LCM}(8),$$

hvormed også den manglende ulighed er eftervist. □

(A.5) Opgaver.

1. Vis, at $\psi(x) = \sum_{p \leqslant x} \lfloor \log x / \log p \rfloor \log p$, og at $\psi(x) \leqslant \pi(x) \log x$.

2. Gælder uligheden $2^n \leqslant \mathrm{LCM}(n)$ for $n = 6$? Vis, at uligheden $\pi(n) \geqslant (\log 2)n/\log n$ gælder for naturlige tal $n \geqslant 4$.

3. Brug Lemma (1.6) til at vise, at enhver binomialkoefficient $\binom{n}{k}$ er divisor i $\mathrm{LCM}(n)$, og giv herved et simpelt bevis for (den svagere ulighed) $2^n \leqslant (n+1)\,\mathrm{LCM}(n)$.