Merk: Alle oddetall er på form $4k+1$ eller $4k+3$. Hvordan fordeler de odde primtallene seg?

$4k+1$: $5, 13, 17, 29, \ldots$

$4k+3$: $3, 7, 11, 19, \ldots$

Teorem 3.6 Det finnes uendelig mange primtall på form $4k+3$

Bevis: Samme type bevis som for Teorem 3.4 (det finnes uendelig mange primtall). Anta 3 bare endelig mange primtall på form $4k+3$: $3, p_1, p_2, \ldots, p_t$ (vi behandler tallet 3 spesielt). Se på tallet $n = 4(p_1 \cdots p_t) + 3$. Dette er et oddetall. Siden $n > 2$ må det være delelig på minst ett primtall, som må være odde. Hvis n bare var delelig med primtall på form $4k+1$, ville n selv vært på denne formen (vis: produktet av to tall på form $4k+1$ er igjen på form $4k+1$). Derfor må n være delelig med et primtall på form $4k+3$. Men ingen av $3, p_1, \ldots, p_t$ deler n. □

Merk: (1) Skal se senere at det også finnes uendelig mange prim på form $4k+1$

(2) Mye mer generelt: hvis $\gcd(a,b) = 1$, finnes uendelig mange prim på form $ak+b$:

$2k+1, 3k+1, 3k+2, 4k+1, 4k+2, 5k+1, 5k+2, 5k+3, 5k+4, \ldots$

Uløst problem: Et primtall p kalles et tvillingprimtall dersom $p+2$ eller $p-2$ også er primtall: $(3,5), (5,7), (11,13), (41,43), \ldots$

Finnes det uendelig mange slike? Største hittil (sept 2018) er

$$(2996863034895 \cdot 2^{12900}) \pm 1$$

Bestemt framskritt i 2013.

Uløst problem: (Goldbachs formodning)

Alle partall ≥ 4 kan skrives som summen av to primtall.

$4 = 2+2$, $6 = 3+3$, $8 = 3+5$, $10 = 3+7 = 5+5$, $\ldots$?

Fra brev fra Goldbach til Euler i 1742. Verifisert $\forall$ partall

$n \leq 4 \cdot 10^{18}$ (minst)

4.2 Kongruenser

Notasjon innført av Gauss (les om ham!) i 1801, forenkler/forbedrer tallteorien betraktelig. Fikser en $n \geq 1$.

Def: To tall $a, b \in \mathbb{Z}$ er <u>kongruente modulo n</u> dersom $n \mid (a-b)$. Skriver da

$$a \equiv b \pmod{n}$$

Eksempel: $43 \equiv 8 \pmod 5$ siden $5 \mid (43-8)$, dvs $5 \mid 35$
$43 \not\equiv 6 \pmod 5$ siden $5 \nmid (43-6)$, dvs $5 \nmid 37$
$2 \equiv -12 \pmod 7$ siden $7 \mid (2-(-12))$, dvs $7 \mid 14$

Fra før: La $a \in \mathbb{Z}$. Div alg gir at a kan skrives unikt som

$$a = qn + r$$

hvor $0 \leq r \leq n-1$. Merk at $a \equiv r \pmod n$ siden $n \mid (a-r)$ fordi $a - r = (qn+r) - r = qn$.

<u>Teorem 4.1</u> $a \equiv b \pmod n \iff a$ og b gir samme rest når vi deler på n

Bevis: Anta a og b gir samme rest r når vi deler på n. Det betyr at $\exists\, q_1, q_2 \in \mathbb{Z}$ med $a = q_1 n + r$ og $b = q_2 n + r$. Får da

$$a - b = (q_1 n + r) - (q_2 n + r) = n(q_1 - q_2)$$

så $n \mid (a-b)$, dvs $a \equiv b \pmod n$.

Anta nå at a og b gir ulike rester når vi deler på n. Det betyr at $\exists\, q_1, q_2, r_1, r_2 \in \mathbb{Z}$ med $a = q_1 n + r_1$, $b = q_2 n + r_2$, $0 \leq r_1, r_2 \leq n-1$ og $r_1 \neq r_2$. Hvis da $a \equiv b \pmod n$ vil $n \mid (a-b)$, dvs $a - b = qn$ for en q. Gir

$$r_1 - r_2 = (a - q_1 n) - (b - q_2 n) = (a-b) - q_1 n + q_2 n$$
$$= n(q - q_1 + q_2)$$

så $n \mid (r_1 - r_2)$. Dette er umulig siden $0 \leq r_1, r_2 \leq n-1$ og $r_1 \neq r_2$. □

Eksempler: (1) $47 \equiv 12 \pmod 5$: 47 og 12 gir rest 2 når vi deler på 5

(2) $a \equiv 0 \pmod n \iff n \mid a$

(3) $a \equiv b \pmod 2 \iff a, b$ begge partall eller begge oddetall

(4) For $a, b \geq 0$: $a \equiv b \pmod{10} \iff a$ og b har samme siste siffer
$1998 \equiv 2018 \pmod{10}$

Merk: La $a \in \mathbb{Z}$. Da finnes et unikt tall $0 \leq r \leq n-1$ med $a \equiv r \pmod n$, nemlig resten når vi deler a på n: $a = qn + r$. Fra div. alg.

Teorem 4.2 (Egenskaper)

(a) $a \equiv a \pmod{n}$

(b) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$

(c) $a \equiv b \pmod{n}$ og $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$

(d) $a \equiv b \pmod{n}$ og $c \equiv d \pmod{n} \Rightarrow \begin{cases} a+c \equiv b+d \pmod{n} \\ ac \equiv bd \pmod{n} \end{cases}$ og

(e) $a \equiv b \pmod{n} \Rightarrow a+c \equiv b+c \pmod{n}$ og $ac \equiv bc \pmod{n}$

(f) $a \equiv b \pmod{n} \Rightarrow a^t \equiv b^t \pmod{n} \quad \forall\, t \geq 1$

Bevis: (a), (b) og (c) følger fra Teorem 4.1, mens (e) og (f) følger fra (a) og (d). Må derfor vise (d).

Hvis $a \equiv b \pmod{n}$ og $c \equiv d \pmod{n}$ vil $n \mid (a-b)$ og $n \mid (c-d)$, dvs $a-b = nq_1$ og $c-d = nq_2$. Gir

$$(a+c)-(b+d) = (a-b)+(c-d) = nq_1 + nq_2 = n(q_1+q_2)$$

$$ac - bd = (a-b)c + b(c-d) = nq_1 c + bnq_2 = n(q_1 c + bq_2)$$

Så $n \mid ((a+c)-(b+d))$ og $n \mid (ac-bd)$. □