5.3 Wilsons teorem

Eksempel: $(2-1)!+1 = 2$ så 2 deler $(2-1)!+1$
$(3-1)!+1 = 3$ så 3 deler $(3-1)!+1$
$(4-1)!+1 = 7$ så 4 deler ikke $(4-1)!+1$
$(5-1)!+1 = 25$ så 5 deler $(5-1)!+1$
$(6-1)!+1 = 121$ så 6 deler ikke $(6-1)!+1$

Teorem 5.4 (Wilsons teorem)
Hvis p er et primtall så er $(p-1)! \equiv -1 \pmod p$

Bevis: Det holder for $p=2$ og $p=3$ (se eksempelet), så anta at $p \geq 5$. Se på de $p-3$ tallene

$$2, 3, \dots, p-2$$

Hvis a er blant disse så vil $p \nmid a$, så $\gcd(a,p)=1$ og den lineære kongr

$$ax \equiv 1 \pmod p$$

er løsbar (Teorem 4.7) og har en unik løsning modulo p. Det betyr at det finnes en unik $b \in \{0,1,\dots,p-1\}$ med $ab \equiv 1 \pmod p$. Hvis $b=0$ er $0 \equiv 1 \pmod p$, umulig. Hvis $b=1$ er $a \equiv 1 \pmod p$, dvs $p \mid (a-1)$. Men siden $a \in \{2,3,\dots,p-2\}$ er dette også umulig. Hvis $b=p-1$ er $1 \equiv a(p-1) \equiv ap-a \equiv -a \pmod p$, dvs $p \mid (a+1)$. Men dette er også umulig siden $a \in \{2,3,\dots,p-2\}$. Følgelig må $b \in \{2,3,\dots,p-2\}$. Hvis $b=a$ er $a^2 \equiv 1 \pmod p$, som gir $p \mid (a^2-1)$, dvs $p \mid (a+1)(a-1)$. Siden p er prim må da $p \mid (a+1)$ eller $p \mid (a-1)$, men som over er dette umulig. Så $a \neq b$
Konklusjon: for alle $a \in \{2,3,\dots,p-2\}$ finnes en $b \in \{2,3,\dots,p-2\}$ med $a \neq b$ og $ab \equiv 1 \pmod p$. Vi får da $(p-3)/2$ kongruenser, og kan multiplisere dem sammen og få

$$(p-2)(p-3)\cdots 3 \cdot 2 \equiv 1 \pmod p$$

dvs

$$(p-2)! \equiv 1 \pmod p$$

Det gir

$$(p-1)! \equiv (p-1)(p-2)! \equiv (p-1)\cdot 1 \equiv -1 \pmod p \qquad \square$$

Merk: (1) Vi så i beviset at $(p-2)! \equiv 1 \pmod p$. Dette er ekvivalent med Wilsons teorem (altså utsagnet "p prim $\Rightarrow (p-2)! \equiv 1 \pmod p$"). Siste del av beviset medfører at dette utsagnet gir Wilsons teorem. Motsatt, hvis Wilsons teorem holder er $(p-1)! \equiv -1 \pmod p$ for alle primtall p. Siden $-1 \equiv p-1 \pmod p$ får vi da $(p-1)! \equiv p-1 \pmod p$. Men $\gcd(p-1,p)=1$, så vi kan dele ut $p-1$ og få $(p-2)! \equiv 1 \pmod p$.

(2) Det motsatte av Wilsons teorem gjelder også. La n være et sammensatt tall. Da finnes to tall $1<a,b<n$ med $n=ab$. Både a og b er da faktorer i $(n-1)!$, dvs $a \mid (n-1)!$ (og samme for b). Hvis nå $(n-1)! \equiv -1 \pmod n$ vil også $(n-1)! \equiv -1 \pmod a$, men $(n-1)! \equiv 0 \pmod a$, så da får vi $-1 \equiv 0 \pmod a$, umulig.

Konklusjen: for alle $n \geq 2$ gjelder implikasjonen

$$(n-1)! \equiv -1 \pmod n \implies n \text{ primtall}$$

Implikasjonen $\Leftarrow$ er nettopp Wilsons teorem.

Eksempel: Eksamen H2011, oppg 4.

La $a = 77! - 1$. Finn et tall $1 < d < a$ med $d \mid a$.

Her lukter det Wilson, siden $d \mid a$ betyr at $77! \equiv 1 \pmod d$. Tallet 79 er prim, så Wilson gir $78! \equiv -1 \pmod{79}$. Siden $-1 \equiv 78 \pmod{79}$ får vi $78! \equiv 78 \pmod{79}$. Vi kan dele ut 78 siden $\gcd(78,79)=1$, og få

$$77! \equiv 1 \pmod{79},$$

dvs $79 \mid a$. (og $1 < 79 < a$).

Kvadratiske kongruenser:

En kvadratisk kongruens $ax^2+bx+c \equiv 0 \pmod n$ kan være løsbar eller ikke. For eksempel er $x^2+x+1 \equiv 0 \pmod 2$ ikke løsbar: a partall $\implies a \equiv 0 \pmod 2 \implies a^2 \equiv 0 \pmod 2 \implies a^2+a+1 \equiv 0+0+1 \equiv 1 \pmod 2$, og a odde $\implies a \equiv 1 \pmod 2 \implies a^2 \equiv 1 \pmod 2 \implies a^2+a+1 \equiv 1+1+1 \equiv 1 \pmod 2$.

Derimot er $x^2 \equiv -1 \pmod 5$ løsbar: en løsning er $x=2$ (eller $x=3$).

Teorem 5.5 La p være et odde primtall. Da gjelder

$$x^2 \equiv -1 \pmod p \text{ løsbar} \iff p \equiv 1 \pmod 4$$

Bevis: Anta først at $p \equiv 1 \pmod 4$, dvs $p = 4k+1$ for en $k \geq 1$. Se på tallene $-1, -2, \dots, -2k$. Her $-1 \equiv p-1 \pmod p$, $-2 \equiv p-2 \pmod p$, $\dots$, $-2k \equiv 2k+1 \pmod p$ så Wilsons teorem gir

$$\begin{aligned} -1 &\equiv (p-1)! \equiv (p-1)(p-2)\cdots(2k+1)2k(2k-1)\cdots 2\cdot 1 \\ &\equiv (-1)(-2)\cdots(-2k)\cdot 2k(2k-1)\cdots 2\cdot 1 \equiv (-1)^{2k}(n!)^2 \\ &\equiv (n!)^2 \pmod p \end{aligned}$$

hvor $n! = (2k)!$. Så $x = (2k)!$ er en løsn av $x^2 \equiv -1 \pmod p$.

Motsatt, anta $p \equiv 3 \pmod 4$, dvs $p = 4k+3$ for en $k \geq 1$. Hvis $x^2 \equiv -1 \pmod p$ er løsbar finnes $a \in \mathbb{Z}$ med $a^2 \equiv -1 \pmod p$, og $p \nmid a$ for da er jo $-1 \equiv a^2 \equiv 0 \pmod p$, umulig. Fermats teorem gir $a^{p-1} \equiv 1 \pmod p$, så vi får

$$1 \equiv a^{p-1} \equiv (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \equiv (-1)^{2k+1} \equiv -1 \pmod p$$

men dette er umulig. Så $x^2 \equiv -1 \pmod p$ er ikke løsbar. □

Merk: Fra beviset ser vi at en løsn av $x^2+1 \equiv 0 \pmod p$ (for $p \equiv 1 \pmod 4$), vil være $(\frac{p-1}{2})!$

Eksempler: (1) $x^2+1 \equiv 0 \pmod 3$ og $x^2+1 \equiv 0 \pmod 7$ er ikke løsbare.

(2) $x^2+1 \equiv 0 \pmod 5$ er løsbar siden $5 \equiv 1 \pmod 4$. Vi så tidligere at $x=2$ og $x=3$ er løsninger. Løsningen fra beviset er $(\frac{5-1}{2})! = 2$.

(3) $x^2+1 \equiv 0 \pmod{13}$ er løsbar siden $13 \equiv 1 \pmod 4$. En løsning er $x = (\frac{13-1}{2})! = 6! = 720$. Ser også at $x=5$ er en løsn, siden $5^2+1 \equiv 0 \pmod{13}$. Men $720 \equiv 5 \pmod{13}$, så dette er "samme" løsning.

Har sett: Vi viste tidligere i kurset at det finnes ∞ mange primtall p med $p \equiv 3 \pmod 4$. Nå kan vi vise det samme for $p \equiv 3 \pmod 4$

Teorem 9.3 (hører like gjerne til her)

Det finnes ∞ mange primtall p med $p \equiv 1 \pmod 4$.

Bevis: La $p_1, \dots, p_t$ være primtall med $p_i \equiv 1 \pmod 4$, og se på tallet

$$n = (2p_1p_2\cdots p_t)^2 + 1$$

Da er n odde, så $\exists$ et odde primtall p med $p \mid n$, dvs

$$(2p_1p_2\cdots p_t)^2 + 1 \equiv 0 \pmod p.$$

Da har $x^2+1 \equiv 0 \pmod p$ en løsning, så Teorem 5.5 gir at $p \equiv 1 \pmod 4$

Men $p \neq p_i$ for alle $i \in \{1, 2, \dots, t\}$, for hvis $p_i \mid n$ får vi

$$0 \equiv (2p_1p_2\cdots p_t)^2 + 1 \equiv 1 \pmod{p_i}$$

som er umulig. □