5.2 Fermats teorem

Oppgave: Les seksjon 5.1 om Fermat og hvordan matematikken ble "gjenoppdaget" i Europa på 1100-tallet.

Eksempel: Se på $p=3$ og $a=4$. Har $3\nmid 4$, og $4^2 \equiv 1 \pmod 3$, dvs $a^{p-1} \equiv 1 \pmod p$.
Nytt eksempel: $p=5$ og $a=2$. Har $5\nmid 2$ og $2^4 \equiv 1 \pmod 5$, dvs $a^{p-1} \equiv 1 \pmod p$

Teorem 5.1 (Fermats teorem)
Hvis p er et primtall og a et tall med $p\nmid a$, så er $a^{p-1} \equiv 1 \pmod p$.

Bevis: Dette er standardbeviset. Se på de $p-1$ tallene

$$a, 2a, 3a, \dots, (p-1)a$$

Ingen av dem er delelig med p (hvorfor?), dvs $ma \not\equiv 0 \pmod p$ for $1 \le m \le p-1$. Videre er de innbyrdes inkongruente modulo p, dvs

$$ma \not\equiv na \pmod p$$

for to tall $1 \le m < n \le p-1$ (dvs to ulike m, n i mengden $\{1, 2, \dots, p-1\}$).
For hvis $ma \equiv na \pmod p$ kan vi dele ut a fordi $p\nmid a$ (så $\gcd(p,a)=1$), og få

$$m \equiv n \pmod p$$

dvs $p \mid (n-m)$. Men når $1 \le m < n \le p-1$ er $1 \le n-m \le p-2$, så $p \nmid (n-m)$.
Altså er de $p-1$ tallene $a, 2a, \dots, (p-1)a$ parvis inkongruente modulo p.
Tallene $0, 1, \dots, p-1$ representerer alle tallene modulo p, dvs at $\forall k \in \mathbb{Z}$ er $k \equiv t \pmod p$ for en $t \in \{0, 1, \dots, p-1\}$. Siden p ikke deler noen av tallene $a, 2a, \dots, (p-1)a$, og de er innbyrdes inkongruente, må de være kongruente med $1, 2, \dots, (p-1)$ i en eller annen rekkefølge.
Så $a \equiv t_1 \pmod p$ for en $t_1 \in \{1, \dots, p-1\}$, $2a \equiv t_2 \pmod p$ for en $t_2 \in \{1, \dots, p-1\}$ med $t_1 \neq t_2$, osv. Vi får $p-1$ kongruenser, og når vi multiplisere dem sammen får vi

$$a \cdot 2a \cdot \dots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \dots \cdot (p-1) \pmod p$$

dvs

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod p$$

Siden $p \nmid (p-1)!$ er $\gcd(p, (p-1)!) = 1$, så vi kan dele ut og få

$$a^{p-1} \equiv 1 \pmod p$$

□

Eksempler: (1) $13 \nmid 28$ så FT gir $28^{12} \equiv 1 \pmod{13}$

(2) Utsagnet holder ikke nødvendigvis hvis p ikke er prim:

$4 \nmid 2$ men $2^{4-1} \not\equiv 1 \pmod 4$

(3) Hva er siste sifter i tallet 47^{82}? Nå finne $0 \le n \le 9$ med $47^{82} \equiv n \pmod{10}$.

Siden $5 \nmid 47$ gir FT at $47^4 \equiv 1 \pmod 5$, som gir $(47^4)^{20} \equiv 1^{20} \pmod 5$ dvs $47^{80} \equiv 1 \pmod 5$. Har også $47 \equiv 1 \pmod 2$, så $47^{80} \equiv 1^{80} \pmod 2$, dvs $47^{80} \equiv 1 \pmod 2$. Så både 5 og 2 deler $47^{80} - 1$. Siden $\gcd(5,2) = 1$ vil derfor $5 \cdot 2 \mid (47^{80} - 1)$, dvs

$$47^{80} \equiv 1 \pmod{10}.$$

Så $47^{82} \equiv 47^{80} \cdot 47^2 \equiv 47^2 \equiv 2209 \equiv 9 \pmod{10}$. Siste sifter er derfor 9.

Korollar: Hvis p er et primtall så er $a^p \equiv a \pmod p$ $\forall\, a \in \mathbb{Z}$.

Bevis: Hvis $p \nmid a$ gir FT at $a^{p-1} \equiv 1 \pmod p$, så $a^{p-1} \cdot a \equiv 1 \cdot a \pmod p$, dvs $a^p \equiv a \pmod p$. Hvis $p \mid a$ er $a \equiv 0 \pmod p$, så $a^p \equiv 0 \pmod p$. Det gir $a^p \equiv 0 \equiv a \pmod p$. □

Merk: (1) Korollaret er ekvivalent med FT. For anta korollaret er sant, og se på utsagnet i FT. Siden $a^p \equiv a \pmod p$ og $\gcd(a,p) = 1$ (siden $p \nmid a$), kan vi dele ut og få $a^{p-1} \equiv a \pmod p$.

(2) Korollaret sier spesielt at $2^p \equiv 2 \pmod p$ $\forall$ primtall p. Lenge trodde man at det motsatte også gjaldt, altså at

$$2^n \equiv 2 \pmod n \implies n \text{ primtall}$$

Men i 1819 kom moteksempelet: $2^{341} \equiv 2 \pmod{341}$ men $341 = 11 \cdot 31$, så 341 er ikke prim.

Hvis n er et sammensatt tall (altså ikke prim) og $2^n \equiv 2 \pmod n$, så kalles n et <u>pseudoprimtall</u>. Konseptet kan generaliseres, og er svært viktig innenfor kryptografi.

Utfordring: Vis at hvis p er prim, så vil p dele $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ når $1 \le i \le p-1$.

Merk: Kan bruke dette hl å gi et alternativt bevis for korollaret (og derfor også FT). Viser først ved induksjon at når p er prim vil

$$a^p \equiv a \pmod p$$

$\forall a = 1, 2, 3, \ldots$

For $a=1$ er det sant. Anta så at det er sant for en a, dvs at $a^p \equiv a \pmod p$. Må vise at da stemmer det også for $a+1$, dvs at

$$(a+1)^p \equiv a+1 \pmod p.$$

Binomialteoremet gir

$$(a+1)^p = \binom{p}{0}a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + \binom{p}{p}$$

Siden $p \mid \binom{p}{i}$ for $1 \le i \le p-1$ vil $\binom{p}{i} \equiv 0 \pmod p$ for $1 \le i \le p-1$, så

$$(a+1)^p \equiv \binom{p}{0}a^p + \binom{p}{p} \equiv a^p + 1 \equiv a+1 \pmod p$$

siden vi har antatt at $a^p \equiv a \pmod p$. Så ved induksjon stemmer korollaret $\forall$ positive heltall $a = 1, 2, 3, \ldots$ For $a=0$ er det trivielt, og for $a<0$ kan vi bruke at det holder for $a>0$ (hvorfor!).

Eksempel: (1) Se på $p=7$. Har

$$\binom{7}{1}=7,\ \binom{7}{2}=21,\ \binom{7}{3}=35,\ \binom{7}{4}=35,\ \binom{7}{5}=21,\ \binom{7}{6}=7$$

så 7 deler alle disse, dvs $7 \mid \binom{7}{i}$ når $1 \le i \le 7-1$.

(2) Når n ikke er prim holder ikke nødvendigvis $n \mid \binom{n}{i}$ for $1 \le i \le n$.

Har $\binom{4}{2} = 6$, så $4 \nmid \binom{4}{2}$.