



5.2.1 Ved Fermats lille teorem er $11^{16} \equiv 1 \pmod{17}$. Vi ser at $104 = 16 \cdot 6 + 8$, som betyr at

$$11^{104} \equiv 11^{16 \cdot 6 + 8} \equiv (11^{16})^6 \cdot 11^8 \equiv 11^8 \pmod{17}.$$

Nå bruker vi at $11^2 \equiv 121 \equiv 2 \pmod{17}$ til å konkludere at

$$11^{104} \equiv 11^8 \equiv 121^4 \equiv 2^4 \equiv 16 \pmod{17}.$$

Så $11^{104} + 1 \equiv 16 + 1 \equiv 17 \equiv 0 \pmod{17}$. Dermed ser vi at $17 \mid 11^{104} + 1$

5.2.6a) Å finne sifferet som står på enerplassen til 3^{100} er det samme som å finne hva 3^{100} er kongruent med modulo 10. Merk at vi ikke kan bruke Fermats lille teorem direkte, siden $10 = 2 \cdot 5$ ikke er et primtall. Det vi kan si med Fermats teorem, er at

$$3^1 \equiv 1 \pmod{2} \quad \text{og} \quad 3^4 \equiv 1 \pmod{5}$$

Dermed får vi at

$$3^{100} \equiv 1^{100} \equiv 1 \pmod{2} \quad \text{og} \quad 3^{100} \equiv (3^4)^{25} \equiv 1^{25} \equiv 1 \pmod{5}.$$

Til sammen gir dette at $3^{100} \equiv 1 \pmod{10}$, så sifferet som står på enerplassen til 3^{100} er 1.

5.2.14 Hvis p og q er to ulike primtall, så gir Fermats lille teorem at

$$p^{q-1} \equiv 1 \pmod{q} \quad \text{og} \quad q^{p-1} \equiv 1 \pmod{p}.$$

I tillegg har vi åpenbart at

$$q^{p-1} \equiv 0 \pmod{q} \quad \text{og} \quad p^{q-1} \equiv 0 \pmod{p}.$$

Dermed får vi at

$$p^{q-1} + q^{p-1} \equiv 0 + 1 \equiv 1 \pmod{p}$$

og

$$p^{q-1} + q^{p-1} \equiv 1 + 0 \equiv 1 \pmod{q},$$

Som betyr at $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

5.3.1a) Ved Wilsons teorem er $16! \equiv -1 \pmod{17}$. Men $16 \equiv -1 \pmod{17}$, så vi kan skrive

$$16! \equiv 16 \cdot 15! \equiv (-1) \cdot 15! \equiv -1 \pmod{17}.$$

Ved å gange med -1 på begge sider får vi da at $15! \equiv 1 \pmod{17}$, så resten når vi deler $15!$ på 17 er 1 .

5.3.7) Om vi klarer å vise at det som p skal dele er kongruent med 0 modulo p , så vil dette være tilstrekkelig. Vi skal vise det for alle heltall a , og behandler først tilfellet $p \mid a$. Da vil $a \equiv 0 \pmod{p}$, og dermed er

$$a^p + (p-1)!a \equiv 0^p + (-1) \cdot 0 = 0 \pmod{p},$$

og

$$(p-1)!a^p + a \equiv (-1) \cdot 0^p + 0 = 0 \pmod{p}.$$

Det gjenstår å vise det samme når $p \nmid a$. I dette tilfellet kan vi bruke Fermats teorem og Wilsons teorem for å få

$$a^p + (p-1)!a = a^{p-1}a + (p-1)!a \equiv a - a = 0 \pmod{p},$$

og

$$(p-1)!a^p + a = (p-1)!a^{p-1}a + a \equiv -a + a = 0 \pmod{p}.$$

5.3.9) Fra Wilsons teorem har vi at $(p-1)! \equiv -1 \pmod{p}$. Vi observerer at

$$\begin{aligned} (p-1)! &\equiv [1 \cdot 3 \cdot 5 \cdot \dots \cdot (p-2)] \cdot [2 \cdot 4 \cdot 6 \cdot \dots \cdot (p-1)] \\ &\stackrel{\text{Hint}}{\equiv} [1 \cdot 3 \cdot 5 \cdot \dots \cdot (p-2)] \cdot (-1)^{\frac{p-1}{2}} [1 \cdot 3 \cdot 5 \cdot \dots \cdot (p-2)] \\ &\equiv (-1)^{\frac{p-1}{2}} [1^2 \cdot 3^2 \cdot 5^2 \cdot \dots \cdot (p-2)^2] \pmod{p}. \end{aligned}$$

Dermed får vi at

$$(-1)^{\frac{p-1}{2}} [1^2 \cdot 3^2 \cdot 5^2 \cdot \dots \cdot (p-2)^2] \equiv -1 \pmod{p},$$

som impliserer at

$$[1^2 \cdot 3^2 \cdot 5^2 \cdot \dots \cdot (p-2)^2] \equiv -(-1)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

Eksamen H2009 oppg. 7) Fra Fermats lille teorem har vi at $a^{p-1} \equiv 1 \pmod{p}$. Merk at siden $p \geq 3$ er et primtall vil $p-1$ være et partall, som betyr at $\frac{p-1}{2}$ er et heltall. Dermed kan vi skrive

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

som gir at p deler $(a^{\frac{p-1}{2}})^2 - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1)$. Siden p er et primtall gir Euklids lemma at $p \mid a^{\frac{p-1}{2}} - 1$ eller $p \mid a^{\frac{p-1}{2}} + 1$. Med andre ord har vi at $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ eller $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Dette viser at minst en av disse kongruensene holder. Begge kan ikke være tilfredsstillt samtidig, siden det ville medføre at $1 \equiv -1 \pmod{p}$, som ikke er mulig siden $p \geq 3$.

Eksamen H2011 oppg. 4 Siden oppgaven inneholder fakultet av et stort tall mistenker vi at vi skal bruke Wilsons teorem på en eller annen måte. Wilsons teorem sier at $(p-1)! \equiv -1 \pmod{p}$ dersom p er et primtall, så vi prøver å finne et primtall som er større enn 77, slik at vi kan bruke teoremet. Åpenbart er ikke 78 et primtall, men 79 er det. Dermed gir Wilsons teorem at $78! \equiv -1 \pmod{79}$. På samme måte som tidligere får vi at $77! \equiv 1 \pmod{79}$. Fra definisjonen av kongruens betyr dette at $79 \mid 77! - 1$. Altså vil $d = 79$ være et tall $0 < d < a$ slik at $d \mid a$.

Eksamen K2021 oppg. 3 Vi skal vise at 61 deler $2 \cdot (59!) + 5!$. Det er det samme som å vise at $2 \cdot (59!) + 5!$ er kongruent med 0 modulo 61. Vi kan betrakte leddene i summen hver for seg, og vi begynner med $59!$. Det første vi legger merke til er at 61 er et primtall, noe som betyr at vi kan bruke Wilsons teorem. Dermed vet vi at

$$60! \equiv -1 \pmod{61}.$$

Videre vet vi at $60! = 60 \cdot 59!$, og siden $60 \equiv -1 \pmod{61}$ gir det at

$$60! \equiv 60 \cdot 59! \equiv (-1) \cdot 59! \pmod{61}.$$

Kombinert med Wilsons teorem gir det at $-59! \equiv -1 \pmod{61}$, og ved å gange med -1 på begge sider får vi at

$$59! \equiv 1 \pmod{61}.$$

Nå betrakter vi leddet $5!$, og regner ut at $5! = 120 = 2 \cdot 61 - 2$, som betyr at

$$5! \equiv -2 \pmod{61}$$

Vi kan nå kombinere dette, og får da

$$2 \cdot (59!) + 5! \equiv 2 \cdot 1 + (-2) \equiv 2 - 2 \equiv 0 \pmod{61}.$$

Dette viser at $2 \cdot (59!) + 5!$ er delelig på 61, og vi er ferdige.