Norges teknisk–naturvitenskapelige universitet
Institutt for matematiske fag

MA1301 Tallteori
Høst 2020

Løsningsforslag — Øving 6

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

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

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

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

I tillegg har vi åpenbart at

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

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.

5.3.4 Vi observerer at $437 = 19 \cdot 23$. Fra Wilsons teorem har vi at $18! \equiv -1 \pmod{19}$, og at $22! \equiv -1 \pmod{23}$. I tillegg har vi at

$$\begin{aligned} 22 &\equiv -1 \pmod{23} \\ 21 &\equiv -2 \pmod{23} \\ 20 &\equiv -3 \pmod{23} \\ 19 &\equiv -4 \pmod{23} \end{aligned}$$

Derfor får vi at

$$\begin{aligned} 22! &\equiv 22 \cdot 21 \cdot 20 \cdot 19 \cdot 18! \pmod{23} \\ &\equiv (-1) \cdot (-2) \cdot (-3) \cdot (-4) \cdot 18! \pmod{23} \\ &\equiv 24 \cdot 18! \pmod{23} \\ &\equiv 18! \pmod{23} \end{aligned}$$

Altså er $18! \equiv 22! \equiv -1 \pmod{23}$. Siden vi også har at $18! \equiv -1 \pmod{19}$ gir dette at $18! \equiv -1 \pmod{19 \cdot 23}$, altså $18! \equiv -1 \pmod{437}$.

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

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

Dermed får vi at

$$(-1)^{\frac{p-1}{2}} \left[1^2 \cdot 3^2 \cdot 5^2 \cdot \ldots \cdot (p-2)^2\right] \equiv -1 \pmod{p}$$

som impliserer at

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

5.3.15 Fra Wilsons teorem har vi at $30! \equiv 30 \cdot 29! \equiv (-1) \cdot 29! \equiv -1 \pmod{31}$, og samme argument som i oppgave 5.3.1 gir at $29! \equiv 1 \pmod{31}$. Det betyr at $4(29!) \equiv 4 \pmod{31}$. Samtidig er $5! \equiv 120 \equiv 27 \pmod{31}$. Dermed får vi at

$$4(29!) + 5! \equiv 4 + 27 \equiv 31 \equiv 0 \pmod{31}.$$

Altså er $4(29!) + 5!$ delelig på 31.

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 tilfredsstilt samtidig, siden det ville medføre at $1 \equiv -1 \pmod{p}$, som ikke er mulig siden $p \geq 3$.

Eksamen V2011 oppg. 4 Vi observerer at $111 \equiv 3 \cdot 37$. Fermats lille teorem gir at $11^2 \equiv 1 \pmod{3}$ og at $11^{36} \equiv 1 \pmod{37}$. Det første gir også at $11^{36} \equiv (11^2)^{18} \equiv 1 \pmod{3}$, og dermed kan vi se at $11^{36} \equiv 1 \pmod{111}$. Dette gir videre at $11^{72} \equiv (11^{36})^2 \equiv 1 \pmod{111}$. Nå kan vi skrive om uttrykket

$$11^{73^n} = 11^{73 \cdot 73^{n-1}} = (11^{73})^{73^{n-1}} = (11 \cdot 11^{72})^{73^{n-1}},$$

og ved å bruke at $11^{72} \equiv 1 \pmod{111}$ ser vi at

$$11^{73^n} \equiv (11 \cdot 11^{72})^{73^{n-1}} \equiv (11 \cdot 1)^{73^{n-1}} \equiv 11^{73^{n-1}} \pmod{111}.$$

På denne måten kan vi redusere potensen i uttrykket, helt til vi står igjen med

$$11^{73^n} \equiv 11^{73^{n-1}} \equiv \ldots \equiv 11^{73^2} \equiv 11^{73} \equiv 11 \cdot 11^{72} \equiv 11 \pmod{111}.$$

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 same 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 $d \mid a$.