Svar eller kortfattade lösningar till tentamen i Elementär talteori, MMG100
28:e september 2019

1. Vi har $2^p \equiv 2\ (mod\ p)$ enligt Fermats lilla sats. Så $2^p + 1 = 2^p - 2 + 3$ är delbart med p enbart om 3 är delbart med p.
   Svar: $p = 3$

2. Kongruensen är lösbar om och endast om $(-1)^{\frac{p-1}{d}} \equiv 1\ (mod\ p)$ där $d = (4, p-1)$
   Fyra fall:
   $p = 8k+1 \quad \Rightarrow \quad d = 4$ och $\frac{p-1}{d} = 2k$
   $p = 8k+3 \quad \Rightarrow \quad d = 2$ och $\frac{p-1}{d} = 4k+1$
   $p = 8k+5 \quad \Rightarrow \quad d = 4$ och $\frac{p-1}{d} = 2k+1$
   $p = 8k+7 \quad \Rightarrow \quad d = 2$ och $\frac{p-1}{d} = 4k+3$
   Svar: alla primtal på formen $8k+1$

3. Låt $p = 15n + 7$. Då är $p + 2$ delbart med 3 och $p - 2$ delbart med 5. Så p kan inte vara en primtalstvilling. Men enligt Dirichlet innehåller följden $\{15n + 7\}$ oändligt många primtal.

4. Ja, till exempel $n = 2021! + 2$. Då är *n* delbart med 2, $n + 1$ delbart med 3 osv fram till $n + 2019$ som är delbart med 2021

5. $\phi(n) = 36 \cdot 70$ som är delbart med 2, 3, 5 och 7. Eftersom $\big(e, \phi(n)\big) = 1$, *e* är sammansatt och $e < 200$, finns bara fyra möjligheter för *e*: $e = 121$, $e = 143$, $e = 169$ samt $e = 187$.
   Om till exempel $e = 143$ söker vi inversen modulo $\phi(n) = 2520$. Med hjälp av Euklides algoritm och tålamod får vi $d = 1727$

6. Påståendet är trivialt sant om n=1.
   För induktionssteget, betrakta $2n + 2$ punkter och leta upp en blå som följs närmast av en röd. Om vi tillfälligt ignorerar dessa punkter återstår $2n$ punkter som enligt antagandet erbjuder en behaglig promenad. Men då kan vi lägga tillbaks de 2 punkterna utan att förstöra något; vi kommer fortfarande att i varje givet ögonblick

ha passerat minst lika många blå som röda.

7. Sätt $A = 2^{p-2} + 3^{p-2} + 6^{p-2}$. Då är $6A \equiv 3 + 2 + 1 \equiv 6 \pmod{p}$
   Om nu $(p, 6) = 1$ följer att $A \equiv 1 \pmod{p}$.
   Så kongruensen är uppfylld för att primtal $p > 3$. Man undersöker fallen $p = 2$ eller $p = 3$ för sig.
   Svar: Alla $p \neq 3$

8. Låt *g* vara en primitiv rot till *p*. Då är 2, 3, 4, … ,p-1 kongruenta med $g, g^2, \ldots g^{p-2}$ i någon ordning. Så $S_n \equiv 1 + g^n + g^{2n} + \cdots + g^{(p-2)n}$.
   Antag nu att $p - 1$ delar n så att $n = (p - 1)t$. Då blir
   $g^{kn} = g^{k(p-1)t} \equiv 1 \pmod{p}$.
   Det följer att $S_n \equiv -1 \pmod{p}$
   Antag i stället att $p - 1$ ***inte*** delar n. Multiplicera kongruensen för S_n ovan med $1 - g^n$. Då får vi $(1 - g^n)S_n \equiv 1 - g^{(p-1)n} \pmod{p}$ (jämför formeln för geometrisk summa.) Högerledet är $\equiv 0$ och eftersom $1 - g^n$ ***inte*** är $\equiv 0 \pmod{p}$ (*g* har ju ordning $p - 1$ som inte delar *n*) följer att $S_n \equiv 0 \pmod{p}$