MATEMATIK
Göteborgs universitet

LÖSNINGSFÖRSLAG TILL TENTAMEN I ELEMENTÄR TALTEORI 2001

1. (a) Se kapitel 1, definition 10.
   (b) Ja, ty 6, 6, 6, 6, 6, 10 och 15 är relativt prima, men $(6,6) = 6$, $(6,10) = 2$, $(6,15) = 3$ och $(10,15) = 5$.

2. (a) Vi ser att $1 = 6 \cdot 2 + 11 \cdot (-1)$ så $x = 6$, $y = -3$ är en lösning. Samtliga lösningar ges därför av
   $$\begin{cases} x = 6 + 11n \\ y = -3 - 6n \end{cases}$$
   där $n \in \mathbb{Z}$. Notera att $(6,11) = 1$.
   (b) Enligt (a) så ges lösningarna till $6x \equiv 3 \pmod{11}$ av $x = 6 + 11n$ där $n \in \mathbb{Z}$. Den minsta positiva lösningen är $x = 6$.

3. En heltalskvadrat är kongruent med 0 eller 1 modulo 4. Summan av två heltalskvadrater är därför kongruent med 0, 1 eller 2 modulo 4. Ett tal som är kongruent med 3 modulo 4 kan sålunda inte skrivas som summan av två heltalskvadrater.

4. Funktionen g_1 är inte multiplikativ ty
   $$g_1(1) = 2 \neq 2 \cdot 2 = g_1(1)g_1(1).$$
   Funktionen g_2 är multiplikativ då $n \mapsto n$ och ϕ är båda multiplikativa funktioner och det är klart att produkten av två multiplikativa funktioner är multiplikativ. Funktionen $\nu(n) = \sum_{d|n, d>0} 1$ är multiplikativ enligt en känd sats som säger att
   $$g(n) = \sum_{d|n, d>0} f(d)$$
   är multiplikativ om f är multiplikativ. Använder vi satsen igen får vi att
   $$g_3(n) = \sum_{d|n, d>0} \nu(d)$$
   är multiplikativ.

5. (a) En invers till 2 modulo 101 är 51 ($2 \cdot 51 = 202 = 101 + 1$). Det betyder att $2x^2 \equiv 1 \pmod{101}$ för något $x \in \mathbb{Z}$ precis då $x^2 \equiv 51 \pmod{101}$. Vi kan avgöra om denna sista kongruens är lösbar genom att beräkna värdet av Legendre-symbolen för 51 modulo 101:
   $$\left(\tfrac{51}{101}\right) = \left(\tfrac{3}{101}\right)\left(\tfrac{17}{101}\right) = \left(\tfrac{101}{3}\right)\left(\tfrac{101}{17}\right) = \left(\tfrac{-1}{3}\right)\left(\tfrac{-1}{17}\right) = -1.$$
   Alltså $2x^2 \equiv 1 \pmod{101}$ är inte lösbar.
   (b) *Lösning 1.* Det är klart att $x = 101$ inte är en lösning till $x^{103} \equiv 1 \pmod{101}$. Antag därför att $x \in \mathbb{Z}$ uppfyller $2 \leq x \leq 100$ och $x^{103} \equiv 1 \pmod{101}$. Fermats lilla sats säger då att
   $$1 \equiv x^{103} \equiv x^{100}x^3 \equiv x^3 \pmod{101}.$$
   Det betyder att ordningen av x modulo 101 måste dela 3, det vill säga $\operatorname{ord}_{101} x = 1$ eller $\operatorname{ord}_{101} x = 3$. Eftersom $\operatorname{ord}_{101} x = 1$ endast om $x \equiv 1 \pmod{101}$ så måste $\operatorname{ord}_{101} x = 3$. Vi vet också att ordningen av ett inverterbart element modulo 101 alltid delar $\phi(101) = 100$. I vårt fall betyder det att $3 \mid 100$. Detta är uppenbarligen inte sant vilket betyder att talet x inte kan existera.

Lösning 2. Enligt satsen om primitiva rötter existerar det en primitiv rot, säg r, modulo 101. Kongruensen $x^{103} \equiv 1 \pmod{101}$ är lösbar om och endast om kongruensen

$$103 \operatorname{ind}_r x \equiv \operatorname{ind}_r 1 \pmod{\phi(101)} \tag{1}$$

(i variablen $\operatorname{ind}_r x$) är lösbar. Vi har $\operatorname{ind}_r 1 = 0$ och $\phi(101) = 100$. Vidare är $103 \equiv 3 \pmod{100}$ och $(3, 100) = 1$ så det existerar en invers till 3 modulo 100. Tillsammans ger detta att kongruensen (1) är ekvivalent med kongruensen

$$\operatorname{ind}_r x \equiv 0 \pmod{100},$$

vilken i sin tur är ekvivalent med kongruensen

$$x \equiv r^0 \equiv 1 \pmod{101}.$$

Således satifierar inget x mellan 2 och 101 den ursprungliga kongruensen.

6. (a) Se kapitel 5, definition 2 och sats 5.19.
   (b) Enligt satsen om primitiva rötter existerar det en primitiv rot modulo $250 = 2 \cdot 5^3$. Enligt en annan känd sats finns det därför precis $\phi(\phi(250)) = 40$ primitiva rötter modulo 250. Det är enkelt att kontrollera att 2 är en primitiv rot modulo 5 och modulo 25. Enligt en känd sats är därför 2 en primitiv rot modulo $125 = 5^3$ och $127 = 2 + 125$ en primitiv rot modulo 250.

7. *Lösning 1.* Enligt proposition 5.3 är talen $1, 2, \ldots, p-1$ kongruenta med talen $r, r^2, \ldots, r^{p-1}$ (i någon ordning) modulo p. Alltså har vi

$$1 \cdot 2 \cdots (p-1) \equiv r \cdot r^2 \cdots r^{p-1} \pmod{p},$$

d.v.s.

$$(p-1)! \equiv r^{1+2+\cdots+p-1} \pmod{p}.$$

Resultatet följer nu av $1 + 2 + \cdots + p - 1 = p(p-1)/2$.

Lösning 2. Wilsons sats säger att $(p-1)! \equiv -1 \pmod{p}$ och Fermats lilla sats säger att

$$r^{p(p-1)/2} \equiv (r^p)^{(p-1)/2} \equiv r^{(p-1)/2} \pmod{p}.$$

Vidare så är $(r^{(p-1)/2})^2 \equiv 1 \pmod{p}$ enligt Fermats lilla sats så $r^{(p-1)/2} \equiv \pm 1 \pmod{p}$ enligt ett känt lemma (lemma 2.10). Men r är en primitiv rot modulo p så $r^{(p-1)/2} \not\equiv 1 \pmod{p}$. Alltså $(p-1)! \equiv p^{p(p-1)/2} \pmod{p}$.

8. Vi söker ett positivt heltal n sådant att n, $n+1$ och $n+2$ vart och ett är delbart med en heltalskvadrat större än 1. Vi kan utan vidare välja dessa kvadrater till att vara 2^2, 3^2 respektive 5^2. Vi söker därför en positiv lösning till följande system av kongruenser:

$$\begin{cases} n \equiv 0 \pmod{2^2} \\ n \equiv -1 \pmod{3^2} \\ n \equiv -2 \pmod{5^2} \end{cases}$$

Den första kongruensen ger $n = 4k$ för något $k \in \mathbb{Z}$. Sätter vi in $n = 4k$ i de två övriga kongruenserna får vi:

$$\begin{cases} 4k \equiv -1 \pmod{9} \\ 4k \equiv -2 \pmod{25} \end{cases}$$

Multiplicerar vi dessa kongruenser med 2 respektive 6 får vi:

$$\begin{cases} k \equiv 2 \pmod{9} \\ k \equiv 12 \pmod{25} \end{cases}$$

Nu är $25 \cdot 4 \equiv 1 \pmod{9}$ och $9 \cdot 14 \equiv 1 \pmod{25}$ så

$$k = 2 \cdot 25 \cdot 4 + 12 \cdot 9 \cdot 14 = 1712$$

är en lösning enligt kinesiska restsatsen. Vi kan likaväl välja $k = 137$ då lösningen endast är bestämd modulo $9 \cdot 25$. Talen 548, 549 och 550 har således de önskade egenskaperna (man kontrollerar enkelt att $548 = 2^2 \cdot 137$, $549 = 3^2 \cdot 61$ och $550 = 5^2 \cdot 22$).