MATEMATIK
Göteborgs universitet

LÖSNINGSFÖRSLAG TILL TENTAMEN I ELEMENTÄR TALTEORI
2002-01-03

1. (b) Talen 4147 och 396231 är inte relativt prima ty båda är delbara med 11.
Svar: Nej!

2. Den minst signifikanta siffran i decimalutvecklingen av 17^{103} är så klart resten vid division av 17^{103} med 10, vilken vi finner med hjälp av Eulers sats som i det här fallet säger att

$$7^{\phi(10)} \equiv 1 \pmod{10}.$$

Eftersom $\phi(10) = 4$ har vi

$$17^{103} \equiv 7^{103} \equiv 7^{4\cdot 25+3} \equiv (7^4)^{25} \cdot 7^3 \equiv 7^3 \equiv 3 \pmod{10}.$$

Svar: 3.

3. Vi har att $3p \mid 3^{p^2-1} + p^2 - 1$ om och endast om

$$\begin{cases} 3^{p^2-1} + p^2 - 1 \equiv 0 \pmod{3} \\ 3^{p^2-1} + p^2 - 1 \equiv 0 \pmod{p}. \end{cases}$$

Den första kongruensen gäller för alla $p \neq 3$ ty $1^2, 2^2 \equiv 1 \pmod{3}$. Den andra kongruensen följer av konjugatregeln, $p^2 - 1 = (p+1)(p-1)$, och Fermats lilla sats som i det här fallet säger

$$3^{p-1} - 1 \equiv 0 \pmod{p}.$$

4. (a) Låt $a = p_1^{a_1} \cdots p_n^{a_n}$ och $b = p_1^{b_1} \cdots p_n^{b_n}$ där $a_i, b_i \geq 0$. Då är

$$\begin{aligned} \lambda(ab) &= \lambda(p_1^{a_1+b_1} \cdots p_n^{a_n+b_n}) \\ &= (-1)^{(a_1+b_1)+\cdots+(a_n+b_n)} \\ &= (-1)^{(a_1+\cdots+a_n)+(b_1+\cdots+b_n)} \\ &= (-1)^{a_1+\cdots+a_n}(-1)^{b_1+\cdots+b_n} \\ &= \lambda(a)\lambda(b). \end{aligned}$$

(b) Funktionen

$$f(n) = \begin{cases} 1 & \text{om } n \text{ är en heltalskvadrat,} \\ 0 & \text{annars} \end{cases}$$

är uppenbarligen multiplikativ (dock inte fullständigt multiplikativ). Enligt sats i boken så är

$$g(n) = \sum_{d|n, d>0} \lambda(d)$$

multiplikativ. Vi har alltså att $f = g$ om och endast om $f(p^n) = g(p^n)$ för alla primtalspotenser p^n. Detta sista påstående är enkelt att kontrollera:

$$f(p^n) = \begin{cases} 1 & \text{om } n \text{ är jämnt,} \\ 0 & \text{om } n \text{ är udda,} \end{cases}$$

och

$$g(p^n) = \sum_{k=0}^{n} (-1)^k = \begin{cases} 1 & \text{om } n \text{ är jämnt,} \\ 0 & \text{om } n \text{ är udda.} \end{cases}$$

5. Antag att r och s är primitiva rötter modulo det udda primtalet p. Det betyder att

$$\operatorname{ord}_p(r) = \operatorname{ord}_p(s) = \phi(p) = p - 1.$$

Låt k vara ett tal sådant att $1 \leq k \leq p-1$ och $s = r^k$. Om k är jämnt, säg $k = 2n$, så är

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

Detta är omöjligt då $\operatorname{ord}_p(s) = p - 1$. Alltså k är udda. Om vi sätter $k = 2n+1$ har vi

$$(rs)^{(p-1)/2} \equiv r^{(k+1)(p-1)/2} \equiv r^{(2n+2)(p-1)/2} \equiv (r^{p-1})^{n+1} \equiv 1 \pmod{p},$$

vilket visar att $\operatorname{ord}_p(rs) \leq (p-1)/2$. Alltså rs är inte en primitiv rot modulo p.

6. (b) Det är bara att räkna på:

$$\left(\frac{518}{787}\right) = \left(\frac{2}{787}\right)\left(\frac{7}{787}\right)\left(\frac{37}{787}\right) = -\left(\frac{7}{787}\right)\left(\frac{37}{787}\right) = \left(\frac{787}{7}\right)\left(\frac{787}{37}\right) =$$
$$= \left(\frac{3}{7}\right)\left(\frac{10}{37}\right) = -\left(\frac{7}{3}\right)\left(\frac{2}{37}\right)\left(\frac{5}{37}\right) = \left(\frac{5}{37}\right) = \left(\frac{37}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

<u>Svar</u>: Nej!

7. (a) <u>Svar</u>: Ja, ty $x = 0$, $y = 1$ och $z = 2$ är en lösning.

(b) Om det finns en lösning så finns det en modulo 4, men $4x^2 - y^2 \equiv 9 \pmod{4}$ om och endast om $y^2 \equiv 3 \pmod{4}$ och denna sista kongruens saknar lösningar ($0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 0$, $3^2 \equiv 1 \pmod{4}$).

<u>Svar</u>: Nej!

8. Vi söker heltal $x, y_1, \ldots, y_n$ sådana att

$$\begin{aligned} x + 1 &\equiv 0 \pmod{y_1^2} \\ 2x + 1 &\equiv 0 \pmod{y_2^2} \\ &\vdots \\ nx + 1 &\equiv 0 \pmod{y_n^2}. \end{aligned}$$

Låt t.ex. y_i vara det i:te primtalet p_i. Då är $p_i > i$ så $p_i \nmid i$. Det betyder att det finns en invers till i modulo p_i^2. Vi kan beteckna inversen med i'. Vårt system ovan kan nu skrivas

$$\begin{aligned} x &\equiv -1 \pmod{2^2} \\ x &\equiv -2' \pmod{3^2} \\ x &\equiv -3' \pmod{5^2} \\ &\vdots \\ x &\equiv -n' \pmod{p_n^2}. \end{aligned}$$

Enligt kinesiska restsatsen finns det en unik lösning x modulo $p_1^2 \cdots p_n^2$ till detta system av kongruenser.