LÖSNINGSFÖRSLAG
Talteori 6hp, Kurskod TATA54, Provkod TEN1
Juni 03, 2021
LINKÖPINGS UNIVERSITET
Matematiska Institutionen
Examinator: Jan Snellman

1) Låt T vara en rätvinklig triangel vars sidlängder är heltal. Visa att arean av T är ett heltal.

Lösning: Sidlängderna (a, b, c) utgör en pytagorisk trippel, och är alltså $d * (A, B, C)$, där (A, B, C) är en primitiv sådan. Vi har karakteriserat sådana och vet att det finns u, v heltal så att $A = u^2 - v^2$, $B = 2uv$. Arean för den ursprungliga triangeln är alltså

$$\frac{ab}{2} = \frac{dAdB}{2} = \frac{d^2(u^2 - v^2)(2uv)}{2} = d^2(u^2 - v^2)uv,$$

ett heltal.

2) Låt x ha den så småningom periodiska kedjebråksutvecklingen $[1; \overline{2, 3}]$. Bestäm x.

Lösning: Sätt $y = x - 1 = [0; \overline{2, 3}]$. Då gäller att

$$y = \frac{1}{2 + \frac{1}{3+y}}$$

vilket är en andragradsekvation i y med positiv rot $\frac{-3+\sqrt{15}}{2}$. Följaktligen så är $x = y + 1 = \frac{-1+\sqrt{15}}{2}$.

3) Låt $2 < p < q$ vara primtal, och antag att heltalet a är relativt primt med p och med q.

(a) Om $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$, vad kan sägas om lösbarheten för kongruensekvationen

$$x^2 \equiv a \mod pq$$

(b) Om $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$?

(c) Om $\left(\frac{a}{p}\right) \neq \left(\frac{a}{q}\right)$?

Lösning: Om $x^2 \equiv a \mod pq$ så $x^2 \equiv a \mod p$ och $x^2 \equiv a \mod q$, så $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$. Detta är alltså ett nödvändigt krav för att kongruensekvationen mod pq skall vara lösbar. Svaret för (b) och (c) blir alltså "ej lösbar".

Om däremot $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$, så finns u, v med $u^2 \equiv a \mod p$, $v^2 \equiv a \mod q$. Det finns ett unikt $w \mod pq$ så att $w \equiv u \mod p$, $w \equiv v \mod q$, och $w^2 \equiv a \mod p$, $w^2 \equiv a \mod q$, så $w^2 \equiv a \mod pq$, och kongruenseskvationen är lösbar.

4) Låt $f(x) = x^4 - 1$.

(a) Ange alla nollställen till $f(x)$ i $\mathbf{Z}_{125}$

(b) Ange alla nollställen till $f(x)$ i $\mathbf{Z}_{49}$

(c) Om $n > 2$, ge en skarp undre gräns för antalet nollställen till $f(x)$ i $\mathbf{Z}_n$.

Lösning: Om $n > 2$ så är $1, -1$ två distinkta nollställen. För $n = 7$ är dessa de enda, så denna undra gräns är skarp. Hensels lemma ger att varje nollställe modulo ett primtal lyfter unikt, så det finns precis två nollställen modulo 49. Dessa är $\pm 1, \pm 23$.

Modulo 5 så är $\pm 1, \pm 2$ alla nollställen. De lyfter till $\pm 1, \pm 7$ modulo 25, och vidare till $\pm 1, \pm 57$ modulo 125.

5) Hitta alla lösningar i par (x, y), med x, y Gaussiska heltal, till den linjära Diofantiska ekvationen

$$(2+i)x + (1+i)y = i$$

Lösning: Uppenbarligen så är

$$1 = (2+i) * 1 + (1+i) * (-1)$$

så

$$i = (2+i) * i + (1+i) * (-i)$$

Samtliga lösningar ges då av

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} i \\ -i \end{pmatrix} + (n+im) \begin{pmatrix} 1+i \\ -2-i \end{pmatrix}, \qquad n, m \in \mathbf{Z}.$$

6) Följande tabell visar att 2 är en primitiv rot modulo 29.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$2^k \bmod 29$	1	2	4	8	16	3	6	12	24	19	9	18	7	14	28

k	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$2^k \bmod 29$	27	25	21	13	26	23	17	5	10	20	11	22	15	1

Lös nu

$$7^x \equiv -5 \mod 29$$

Lösning: Vi tar index m.a.p. den primitiva roten 2 och får

$$\begin{aligned} \text{ind}(7^x) &\equiv \text{ind}(-5) \mod 28 \\ x * \text{ind}(7) &\equiv \text{ind}24 \mod 28 \\ x * 12 &\equiv 8 \mod 28 \\ 3x &\equiv 2 \mod 7 \\ x &\equiv 3 \mod 7 \end{aligned}$$

7) Visa att för varje positivt heltal n så

$$\mu(n)^2 = \sum_{d|n} \mu(d) 2^{\omega(n/d)}$$

där $\omega(k)$ anger antalet distinkta primfaktorer i k.

Lösning: Uppgiften är från kursboken.