Lösningsförslag till Talteori TATA54 3 juni 2023

1) Tag 2-logaritmer och erhåll

$$2x + 3y + 5z = 1.$$

Det är en linjär Diofantisk ekvation med lösningar

$$(x, y, z) = (0, 2, -1) + n(1, 1, -1) + m(0, 5, -3)$$

2) Sätt $f(x) = x^5 + 2x + 3$. Prövning ger att $f(x)$ har nollställena $x \equiv -1 \mod 5$, och nollställena $x \equiv 3 \mod 7$ samt $x \equiv -1 \mod 7$.

Eftersom $f'(x) = 5x^4 + 2 \equiv 2 \mod 5$ så lyfter nollstället $x \equiv 4 \mod 5$ till ett unikt $x \equiv 4 + 5r \mod 25$. Eftersom $f(-1) = 0$ i $\boldsymbol{Z}$ så är $f(-1) \equiv 0$ modulo alla modulus! Följaktligen är det unika lyftet

$$x \equiv -1 \mod 25.$$

Modulo 7 så är $f'(x) = 5x^4 + 2 \equiv 5x^4 + 2 \mod 7$ med $f'(3) \equiv 1 \mod 7$, så detta nollställe lyfter unikt, till

$$x \equiv -4 \mod 49.$$

Däremot så är $f'(-1) \equiv 0 \mod 7$. Därför är antingen alla, eller inga, av lyften av -1 nollställen $\mod 49$. Återigen, $f(-1) = 0$ i $\boldsymbol{Z}$ så $f(-1) \equiv 0$ modulo alla modulus. Så alla lyften är nollställen, dessa är

$$x \equiv -1, 6, 13, 20, 27, 34, 41 \mod 49.$$

Slutligen så använder vi kinesiska restsatsen för att lösa

$$\begin{aligned} x &\equiv -1 \mod 25 \\ x &\equiv -1, 6, 13, 20, 27, 34, 41, -4 \mod 49 \end{aligned}$$

och får

$$x \equiv -1, 349, 699, 1049, 174, 524, 874, 1074 \mod 1225$$

3) Den minsta primitiva roten modulo 7 är 3. Exponenttabell respektive diskret logaritmtabell blir

x	3^x	$\log(x)$
0	1	-
1	3	0
2	2	2
3	6	1
4	4	4
5	5	5
6	1	3

Om $x \equiv 0 \mod 7$ men $x \neq 0$ så blir $x^x \equiv 0 \mod 7$, så det blir en (trivial) lösning. Däremot är 0^0 antingen odefinierat eller 1, beroende på vem man frågar, så det är ingen lösning.

Antag hädanefter att $x \neq 0 \mod 7$.

Ekvationen $x^x \equiv x \mod 7$ blir $x \log x \equiv \log x \mod 6$ dvs

$$6|(x-1)\log x$$

när vi tar diskreta logaritmer.

Om $\text{sgd}(6, \log(x)) = 1$, vilket inträffar då $x \equiv 3, 5 \mod 7$, så gäller att $6|x-1$ dvs att $x \equiv 1 \mod 6$. Så med KRS har vi att $x \equiv 31, 19 \mod 42$.

Om $\text{sgd}(6, \log(x)) = 2$, vilket inträffar då $x \equiv 2, 4 \mod 7$, så gäller att $3|x-1$ dvs att $x \equiv 1 \mod 3$. Så med KRS får vi att $x \equiv 16, 4 \mod 21$.

Om $\text{sgd}(6, \log(x)) = 3$, vilket inträffar då $x \equiv 6 \mod 7$, så gäller att $2|x-1$ dvs att $x \equiv 1 \mod 2$. Så med KRS har vi att $x \equiv 13 \mod 14$.

Slutligen, om $\text{sgd}(6, \log(x)) = 1$ så är $\log(x) = 6$ varför $x \equiv 1 \mod 7$.

Sammanfattningsvis: x är en icke-trivial lösning till ursprungsekvationen omm

$$x \equiv 31, 19, 16, 37, 4, 25, 13, 27, 41, 1, 8, 15, 22, 29, 36 \mod 42$$

Vidare är $x \equiv 0 \mod 7$, $x \neq 0$ också (triviala) lösningar.

4) Eftersom ϕ och identitetsfunktionen I är multiplikativa så räcker det att kontrollera den första identitetet då $n = p^k$ är en primtalspotens. Vi får att

$$\sum_{d|p^k} \phi(d) = \sum_{\ell=0}^{k} \phi(p^\ell) = 1 + \sum_{\ell=1}^{k} (p^\ell - p^{\ell-1}) = p^k$$

Från $I(n) = n = \sum_{d|n} \phi(d)$ följer med möbiusinversion att

$$\phi(n) = \sum_{d|n} I(d)\mu(n/d) = \sum_{d|n} d\mu(n/d)$$

5) Eftersom $11 \equiv 3 \mod 4$ så är

$$\left(\frac{11}{p}\right) = \begin{cases} \left(\frac{p}{11}\right) & p \equiv 1 \mod 4 \\ -\left(\frac{p}{11}\right) & p \equiv 3 \mod 4 \end{cases}$$

Det udda primtalet p uppfyller alltså antingen $p \equiv 1 \mod 4$ och p KR modulo 11, elller $p \equiv 3 \mod 4$ och p IKR modulo 11.

Prövning ger att de kvadratiska residyerna modulo 11 är

$$1, 3, 4, 5, 9$$

medan de kvadratiska icke-residuerna är

$$2, 6, 7, 8, 10$$

Om $p \equiv 1 \mod 4$ och p KR mod 11 så är

$$p \equiv 1, 25, 37, 5, 9 \mod 44.$$

Om $p \equiv 3 \mod 4$ och p IKR mod 11 så är

$$p \equiv 35, 39, 7, 19, 43 \mod 44.$$

6) Vi beräknar kedjebråksutvecklingen

$$\sqrt{11} = [3; \overline{3, 6}]$$

med första tre konvergenter $3, 10/3, 63/19, 199/60$. Vi har att $(x, y) = (10, 3)$ är den "minsta" positiva heltalslösningen till $x^2 - 11y^2 = 1$. Nästa lösning i ordningen kan vi få genom att expandera

$$(10 + 3\sqrt{11})^2 = 199 + 60\sqrt{11}$$

från vilket vi ser att $(x, y) = (199, 60)$ är en lösning. Vi påstår att $199/60$ är en tillräckligt bra approximation till $\sqrt{11}$.

Vi kan skriva ekvationen som

$$1 = (x + \sqrt{11}y)(x - \sqrt{11}y)$$

så vi får att

$$|199/60 - \sqrt{11}| = \frac{1}{60}\left|199 - 60\sqrt{11}\right| = \frac{1}{60} \times \frac{1}{199 + 60\sqrt{11}} < \frac{1}{60 * 199} < 10^{-4}$$

7) Vi har att $87 = 3 * 29$, med $3 = 1^2 + 1^2 + 1^2$ och $29 = 5^2 + 2^2$. Vi bildar kvaternionprodukten

$$(i + j + k)(5i + 2j) = -7 - 2i + 5j - 3k$$

och tar normen och får att $87 = (-7)^2 + (-2)^2 + (5^2) + (-3)^2$.

Modulo 8 så är varje kvadrat kongruent med 0, 1, eller 4, varför summan av tre kvadrater är kongruent med 0,1,2,3,4,5, eller 6 modulo 8. Inget tal kongruent med 7 modulo 8 kan alltså skrivas som summan av 3 kvadrater.