Talteori 6hp, Kurskod TATA54, Provkod TEN1
17 augusti 2023
LINKÖPINGS UNIVERSITET
Matematiska Institutionen
Examinator: Jan Snellman

Alla problem ger maximalt 3 poäng. Full poäng kräver fullständig lösning. 8p räcker för betyg 3, 11p för betyg 4, 14p för betyg 5.

Med μ avses Möbiusfunktionen, den multiplikativa funktion som uppfyller $\mu(1) = 1$, $\mu(p) = -1$ för p primtal, och $\mu(n) = 0$ för alla $n > 1$ som delas av kvadraten av ett heltal. Med ϕ avses Eulers phi-funktion, som räknar antalet multiplikativt inverterbar kongruensklasser modulo n.

1) Observera först att $\text{sgd}(55, 77) = 11 > 1$. Sätt $x = 7 + 55m = 18 + 77n$ så att

$$55m - 77n = 11 \quad \Longleftrightarrow \quad 5m - 7n = 1.$$

Denna linjära Diofantiska ekvation har lösningarna $(m, n) = (3, 2) + s(7, 5)$ så

$$x = 7 + 55 * (3 + 7s) = 172 + s * 7 * 55$$

dvs $x \equiv 172 \mod 7 * 5 * 11$.

2) Om m, n är relativt prima så är de primtal som ingår i faktoriseringen av m distinkta från de som ingår i faktoriseringen av n, varför $\omega(mn) = \omega(m) + \omega(n)$. Det följer att 2^ω är multiplikativ.

Vi beräknar $f(n) = \sum_{d|n} 2^{\omega(d)}$. Eftersom 2^ω är multiplikativ så är även f det. För $n = p^s$ så

$$f(p^s) = \sum_{r=0}^{s} 2^{\omega(p^r)} = 2^0 + 2^1 + \cdots + 2^1 = 1 + 2s$$

Det följer att för $n = p_1^{a_1} \cdots p_r^{a_r}$ så är

$$f(n) = (1 + 2a_1)(1 + 2a_2) \cdots (1 + 2a_r).$$

3) Genom prövning ser vi att 5 är en primitiv rot modulo $p = 23$. Eftersom $(a+p)^{11} \equiv -1 \mod p^2$ så är $(a + p)^{22} \equiv 1 \mod p^2$, så $a + p$ är ingen primitiv rot modulo p^2. Det följer (satser i kursboken) att a är en primitiv rot modulo p^2, och följaktligen också en primitiv rot modulo p^k för $k \geq 3$. Alltså är

$$\text{ord}_{p^3}(a) = \phi(p^3) = p^2(p - 1) = 11638.$$

4) Vi har att

$$\alpha/\beta = 114/25 - 27/25i = 4.56 - 1.08i$$

Så om vi avrundar till de fyra omkringliggande gitterpunkterna får vi att

$$(\gamma, \rho) \in \{(5 - i, -1 - 2i), (4 - i, 2 + 2i), (5 - 2i, 5 - i), (4 - 2i, -2 + 5i)\}$$

De första två paren uppfyller normvillkoret.

5) Antag att $p_1, \ldots, p_n$ är primtal, $p_j \equiv 3 \mod 8$. Sätt $y = \prod_j p_j$, $N = y^2 + 2$. Vi visar att N har en primtalsdelare $q \equiv 3 \mod 8$ som inte är en av $p_1, \ldots, p_n$.

För det första så är y udda, så $y^2 \equiv 1 \mod 8$ och $N \equiv 3 \mod 8$. Om alla primdelare till N vore $\equiv 1 \mod 8$ så skulle $N \equiv 1 \mod 8$, vilket inte gäller; så finns primdelare $q|N$ som är kongruent med $-1, -3$, eller 3 mod 8.

Eftersom $N \equiv 0 \mod q$ så är $-2 \equiv y^2 \mod q$. Alltså är -2 en kvadratisk residy modulo q, vilket inträffar (andra supplementet) omm $q \equiv 1 \mod 8$ eller $q \equiv 3 \mod 8$. Med vad vi tidigare visade får vi att $q \equiv 3 \mod 8$.

Det återstår att visa att $q = p_j$ inte är möjligt. Om så vore fallet så $q|y^2$, $q|y^2 + 2$ vilket ger $q|2$, vilket är omöjligt.

6) Vi skriver om ekvationen som

$$x^2 + y^2 = (u + v)^2.$$

Klassificeringen av primitiva pytagoriska tripplar ger att alla lösningar ges av

$$\begin{aligned} x &= m^2 - n^2 \\ y &= 2mn \\ u + v &= m^2 + n^2 \end{aligned}$$

med $1 \leq n < m$, $\mathrm{sgd}(m, n) = 1$, $m \neq n \mod 2$. Vi sätter $v = m^2 + n^2 - u$ och har att $u \leq m^2 - n^2$ samt att $m^2 + n^2 - u \leq 2mn$, så

$$(m - n)^2 \leq u \leq (m + n)(m - n).$$

Så lösningen ges av

$$\begin{aligned} x &= m^2 - n^2 \\ y &= 2mn \\ u &= r \\ v &= m^2 + n^2 - r \\ 1 \leq n &< m \\ \mathrm{sgd}(m, n) &= 1 \\ m &\neq n \mod 2 \\ (m - n)^2 &\leq r \\ r &\leq (m + n)(m - n) \end{aligned}$$

7) Kedjebråksutvecklingen till $279/599$ är $[0; 2, 6, 1, 4, 8]$ med konvergenter

$$[0, 1/2, 6/13, 7/15, 34/73, 279/599]$$

Den tredje konvergenten duger:

$$|279/599 - 7/15| = 8/8985 < 10^{-3}.$$