



Linköpings Universitet

TATA54 Talteori | Number Theory

TEN1 Skriftlig tentamen | Written Examination, 6 hp

Fördefinierad information

Startdatum: 03-06-21 14:00

Bedömningsform: Fyrgradig skala (5,4,3,U,1)

Slutdatum: 03-06-21 18:30

SIS-kod: 132137

Intern bedömare: (Anonymiserad)

Deltagare

FlowID nummer: 1

Information från deltagare

Sidor *: 9

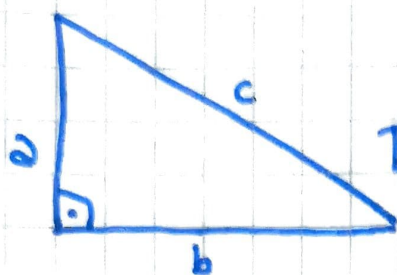
Försäkran på heder och samvete *: Ja

1	2	3	4	5	6	7	Σ	Grade
1	3	3	2	3	3	3	18	5

3.6.21

1)

T



a, b, c are positive integers.

The area of T is given by

$$A = \frac{1}{2} \cdot a \cdot b$$

To prove that A is an integer, I have to show that $a \cdot b$ is an even integer. But this is not always true, e.g. $a=b=c=1$ then the area of T is $\frac{1}{2}$ which is no integer!

Pythagoras: $a^2 + b^2 = c^2$

Case 1: c is even

Then c^2 is even and $a^2 + b^2$ is even

not possible { Either a^2 and b^2 are odd $\Rightarrow a$ and b are odd and $a \cdot b$ is odd \Rightarrow the area is no integer

Or a^2 and b^2 are even $\Rightarrow a$ and b are even and $a \cdot b$ is even

Case 2: c is odd

Then c^2 is odd and $a^2 + b^2$ is ^{odd} even

one of a, b must be even and the other one odd $\Rightarrow \frac{1}{2} \cdot a \cdot b$ is an integer

\Rightarrow to show that ^{the area of T} A is an integer, we need an extra requirement, e.g. at least one side has an even length

By Lemma 13.2, for a primitive PT z is odd. So if z is even in a (non-primitive) PT (x, y, z) then both x and y are even, as well.

1

$$2) x = [1; \overline{2, 3}]$$

$$\text{let } x = [1; y], y = [\overline{2, 3}] = [2; 3, y]$$

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

$$\Leftrightarrow y \cdot (3y + 1) = 2(3y + 1) + y$$

$$\Leftrightarrow 3y^2 + y - 6y - 2 - y = 0$$

$$\Leftrightarrow 3y^2 - 6y - 2 = 0$$

$$\Leftrightarrow y = \frac{6 \pm \sqrt{36 + 4 \cdot 2 \cdot 3}}{6} = \frac{3 \pm \sqrt{15}}{3}$$

$$\Rightarrow \text{the positive solution is } y = \frac{3 + \sqrt{15}}{3}$$

$$\Rightarrow x = 1 + \frac{1}{y} = 1 + \frac{1}{\frac{3 + \sqrt{15}}{3}} = 1 + \frac{3}{3 + \sqrt{15}}$$

3

3) a) $\text{Yes } \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$ means that there exists a solution $x^2 \equiv a \pmod{p}$ and $x^2 \equiv a \pmod{q}$
 \Rightarrow there exists a solution to the congruence
because CRT $x^2 \equiv a \pmod{pq}$

b) If $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$ then there exists no solutions to the congruences $x^2 \equiv a \pmod{p}$ and $x^2 \equiv a \pmod{q}$
but then the congruence $x^2 \equiv a \pmod{pq}$ cannot have a solution

c) If $\left(\frac{a}{p}\right) \neq \left(\frac{a}{q}\right)$, either $\left(\frac{a}{p}\right)$ or $\left(\frac{a}{q}\right)$ equals -1
which means that one of the congruences
 $x^2 \equiv a \pmod{p}$ or $x^2 \equiv a \pmod{q}$ has no solution
 $\Rightarrow x^2 \equiv a \pmod{pq}$ cannot have a solution

3

40) List all zeros of $f(x)$ in \mathbb{Z}_{125}

$$f(x) = 4x^3 \quad \text{and} \quad 125 = 5^3$$

$$\cancel{x^4 \equiv 1 \pmod{5}} \\ x^4 - 1 \equiv 0 \pmod{5} \Leftrightarrow x^4 \equiv 1 \pmod{5} \Leftrightarrow \cancel{x \equiv 1, 4 \pmod{5}} \\ x \equiv 1, 2, 3, 4 \pmod{5}$$

→ Thm 4.15

Apply Hensel's Lemma to get the zeros in \mathbb{Z}_{125} :

- $x \equiv 1 \pmod{5}$: $f'(1) = 4 \cdot 1^3 \equiv 4 \pmod{5} \not\equiv 0 \pmod{5}$
 \Rightarrow \exists unique integer $0 \leq t < 5$ s.t. $f(1+5t) \equiv 0 \pmod{5^2}$
 and: $t=0$ because $f(1) \equiv 0 \pmod{5^2}$

apply Hensel's lemma again to get $f(1) \equiv 0 \pmod{5^3}$

- $x \equiv 2 \pmod{5}$: $f'(2) \equiv 2 \not\equiv 0 \pmod{5}$
 $\Rightarrow f(2+5t) \equiv 0 \pmod{5^2}$ for some $0 \leq t < 5$
 $t=1$ and $f(7) \equiv 0 \pmod{5^2}$

apply Hensel's lemma again: $f'(7) \not\equiv 0 \pmod{5}$
 and $f(7+5^2t) \equiv 0 \pmod{5^3}$ for a unique $0 \leq t < 25$
 and we see that $f(7+5^2 \cdot 2) \equiv 0 \pmod{5^3}$

- $x \equiv 3 \pmod{5}$: $f'(3) \equiv 3 \pmod{5}$
 $\Rightarrow f(3+5t) \equiv 0 \pmod{5^2}$ for a $0 \leq t < 5$
 $f(3+5 \cdot 3) \equiv 0 \pmod{5^2}$

$$f'(18) \not\equiv 0 \pmod{5} \Rightarrow f(18+5^2t) \equiv 0 \pmod{5^3} \text{ for a } 0 \leq t < 25 \\ f(18+2 \cdot 25) = f(68) \equiv 0 \pmod{5^3}$$

- $x \equiv 4 \pmod{5}$: $f'(4) \equiv 1 \pmod{5}$
 $\Rightarrow f(4+5t) \equiv 0 \pmod{5^2}$ for $0 \leq t < 5$
 $f(4+4 \cdot 5) \equiv 0 \pmod{5^2}$

$$f'(24) \equiv 1 \pmod{5} \Rightarrow f(24+5^2t) \equiv 0 \pmod{5^3} \\ f(24+5^2 \cdot 4) \equiv 0 \pmod{5^3}$$

OK

4a continued: 1, 57, 68 and 124 are the zeros in \mathbb{Z}_{49}

4b) $49 = 7^2$

zeros of (x) in \mathbb{Z}_7 : $x^4 - 1 \equiv 0 \pmod{7} \Leftrightarrow x^4 \equiv 1 \pmod{7}$

$\Leftrightarrow x \equiv 1 \text{ or } 6 \pmod{7}$

- $x \equiv 1 \pmod{7}$

$f(1) \equiv 4 \not\equiv 0 \pmod{7}$

\Rightarrow exists unique t ($0 \leq t < 7$) s.t. $f(1+t \cdot 7) \equiv 0 \pmod{7^2}$
since $f(1) \equiv 0 \pmod{49}$ $t=0$

- $x \equiv 6 \pmod{7}$

$f(6) = 4 \cdot 6^3 = 4 \cdot 6 \cdot 6^2 \equiv 3 \cdot 1 \equiv 3 \not\equiv 0 \pmod{7}$

$\Rightarrow f(6+t \cdot 7) \equiv 0 \pmod{7^2}$ for a unique $0 \leq t < 7$
 $f(6+6 \cdot 7) \equiv 0 \pmod{7^2}$

\Rightarrow the zeros of $f(x)$ in \mathbb{Z}_{49} are 1 and 48

4c) ~~It is obvious that 1 is a zero of $f(x)$ in \mathbb{Z}_n
in addition to that every integer a with $\text{ord}_n a = 4$
 $\text{ord}_n a \equiv 4$ is a zero of the function in \mathbb{Z}_n~~

~~$\Rightarrow \varphi(n) \# \{a \mid \text{ord}_n a \equiv 4\}$ is a lower bound to the
number of zeros in \mathbb{Z}_n~~

~~This bound is sharp as we have seen in Ex: 4b:
because $\varphi(5) = 4$ and Fermat's Little Theorem exactly
 $\# \{a \mid \text{ord}_5 a \equiv 4\} = 4$ and in fact, there are 4
zeros in \mathbb{Z}_5 of $f(x)$ in \mathbb{Z}_5~~

6 \rightarrow see last page

2

a, b, c, d integers

5) let $x = a + ib$ and $y = c + id$, then

$$\begin{aligned}(2+2i)x + (1+i)y &= (2+2i)(a+ib) + (1+i)(c+id) = \\&= 2a + 2ib + ia - b + c + id + ic - d \\&= (2a - b + c - d) + i(2b + a + d + c) = 0 + i\end{aligned}$$

$$\Leftrightarrow 2a - b + c - d = 0 \text{ and } 2b + a + d + c = 1$$

$$\begin{aligned}\Leftrightarrow c &= b + d - 2a \text{ and } 2b + a + d + c = 2b + a + d + b + d - 2a \\&= 3b + 2d - a = 1 \\&\Leftrightarrow a = 3b + 2d - 1\end{aligned}$$

$$\begin{aligned}\Leftrightarrow c &= b + d - 2(3b + 2d - 1) \text{ and } a = 3b + 2d - 1 \\&= \cancel{2b} - d + 4 - 5b - 3d + 2\end{aligned}$$

~~$(3b + 2d - 1 + ib, -2b - d + 1 + id)$ are solutions to the Diophantine equation for every b, d integers b, d~~

for every integers b and d

$(3b + 2d - 1 + ib, -5b - 3d + 2 + id)$ is a solution to the diophantine equation

3

$$6) 7^x \equiv -5 \pmod{29}$$

$$\Leftrightarrow 7^x \equiv 24 \pmod{29}$$

$$\Leftrightarrow \text{ind}_2(7^x) \equiv \text{ind}_2(24) \pmod{28}$$

$$\Leftrightarrow x \cdot \text{ind}_2 7 \equiv \text{ind}_2 24 \pmod{28}$$

$$\Leftrightarrow 12x \equiv 8 \pmod{28}$$

$$\Leftrightarrow 4x \equiv 12 \pmod{28}$$

$$\Leftrightarrow x \equiv 3 \pmod{7}$$

$$(\text{Thm 9.16 iii}) \phi(29) = 28$$

(see table)

multiply with 4

$$(\text{Thm 4.5: } (4, 28) = 4)$$

3

$$7) \nu(n)^2 = \sum_{d|n} \nu(d) 2^{\omega(n/d)}$$

I will first show that $\sum_{d|n} \nu^2(d) = 2^{\omega(n)}$

and then use the Möbius inversion formula.

- Thm 7.14 ^{states} that $\nu(d)$ is multiplicative, then $\nu^2(d)$ is multiplicative, too:

m, n relatively prime positive integers, then

$$\nu^2(m \cdot n) = \nu(m \cdot n) \nu(m \cdot n) = \nu(m) \nu(n) \nu(m) \nu(n) = \nu^2(m) \nu^2(n)$$

and by Thm 7.8 $\sum_{d|n} \nu^2(d)$ is multiplicative

$2^{\omega(n)}$ is multiplicative, because if m, n are rel. prime pos. integers then

$$\sum_{d|m \cdot n} \nu^2(d) = \sum_{\substack{d_1|m \\ d_2|n \\ d_1, d_2 \text{ don't share any prime factors}}} \nu^2(d_1 d_2) = \sum_{d_1|m} \nu^2(d_1) \sum_{d_2|n} \nu^2(d_2) = 2^{\omega(m)} 2^{\omega(n)}$$

\Rightarrow both sides of $\sum_{d|n} \nu^2(d) = 2^{\omega(n)}$ are multiplicative, so it suffices to prove the identity only for $n = p^a$ p prime, a a pos. integer and $n = 1$

$$2^{\omega(p^a)} = 2^1 = 2$$

$$\sum_{d|p^a} \nu^2(d) = \nu^2(p) + \nu^2(1) = 1 + 1 = 2$$

$$2^{\omega(1)} = 2^0 = 1$$

$$\sum_{d|1} \nu^2(d) = \nu^2(1) = 1$$

- Let $f(d) = \nu^2(d)$ is an arithmetic function and $F(n) = 2^{\omega(n)} = \sum_{d|n} f(d)$ is the summatory function of f

$$\Rightarrow \text{Thm 7.16} \quad f(n) = \nu^2(n) = \sum_{d|n} \nu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \nu(d) 2^{\omega\left(\frac{n}{d}\right)}$$

3

□

TATA54 TEN1 3.6.21
FLOWID number 1
page 9

4c) $1 + \# \{a \mid \text{ord}_n a = 2 \text{ or } \text{ord}_n a = 4\}$ is a lower bound to the number of zeros in \mathbb{Z}_n .

It is obvious that 1 is a zero of $f(x)$ in \mathbb{Z}_n and in addition to that every integer with $\text{ord}_n a = 2$ or $\text{ord}_n a = 4$ is a zero of the function in \mathbb{Z}_n since by definition then $a^4 = (a^2)^2 \equiv 1 \pmod n$

The bound is sharp as is shown in 4b:
 $x^4 - 1 \equiv 0 \pmod 7$ has exactly 2 solutions
and $\text{ord}_7 6 = 2$

What I intended was: at least 2
zeros.

Your condition, while true, is less useful.

○