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

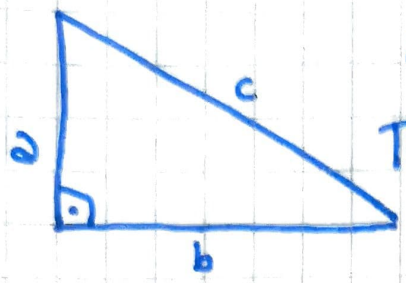
Information från deltagare

Sidor *:	9

Försäkran på heder och samvete *: Ja

TATASG TEN 1 3.6.21
FlowID number: 1
page 1

1)



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
Either a^2 and b^2 are odd ⇒ a and b are odd and $a \cdot b$ is odd ⇒ the area is no integer ↯
Or a^2 and b^2 are even ⇒ 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 ~~even~~ odd
one of a, b must be even and the other one odd
⇒ $\frac{1}{2} \cdot a \cdot b$ is an integer

⇒ to show that the area of T is an integer, we need an extra requirement, e.g. at least one side has an even length

TATASY TEN 1 3.6.21
FlowID number 1
page 2

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

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

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

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

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

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

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

$\Rightarrow$ 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) a) If $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$ means that there exists a solution $x^2 \equiv a \bmod p$ and $x^2 \equiv a \bmod q$
$\Rightarrow$ there exists a solution to the congruence $x^2 \equiv a \bmod pq$

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

TAT454 TEN1 3.6.21
Flow ID number 1
page 4

4a) List all zeros of $f(x)$ in $\mathbb{Z}_{125}$

$f'(x) = 4x^3$ and $125 = 5^3$

~~$x^4 \equiv 1 \bmod$~~

$x^4 - 1 \equiv 0 \bmod 5 \iff x^4 \equiv 1 \bmod 5 \iff$ ~~$x \equiv 1, 4 \bmod 5$~~
$x \equiv 1, 2, 3, 4 \bmod 5$

Apply Hensel's lemma (→ Thm 4.15) to get the zeros in $\mathbb{Z}_{125}$:

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

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

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

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

- $x \equiv 3 \bmod 5$: $f'(3) \equiv 3 \bmod 5$
  $\Rightarrow f(3+5t) \equiv 0 \bmod 5^2$ for a $0 \le t < 5$
  $f(3+5\cdot 3) \equiv 0 \bmod 5^2$

  $f'(18) \not\equiv 0 \bmod 5 \Rightarrow f(18+5^2 t) \equiv 0 \bmod 5^3$ for a $0 \le t < 25$
  $f(18 + 2 \cdot 25) = f(68) \equiv 0 \bmod 5^3$

- $x \equiv 4 \bmod 5$: $f'(4) \equiv 1 \bmod 5$
  $\Rightarrow f(4+5t) \equiv 0 \bmod 5^2$ for $0 \le t < 5$
  $f(4+4\cdot 5) \equiv 0 \bmod 5^2$

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

4a continued: $1, 57, 68$ and 124 are the zeros in $\mathbb{Z}_{125}$

4b) $49 = 7^2$

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

$\Leftrightarrow x \equiv 1$ or $6 \bmod 7$

- $x \equiv 1 \bmod 7$
  $f'(1) \equiv 4 \not\equiv 0 \bmod 7$
  $\Rightarrow$ exists unique t $(0 \leq t < 7)$ s.t. $f(1 + t \cdot 7) \equiv 0 \bmod 7^2$
  since $f(1) \equiv 0 \bmod 47$ $t = 0$

- $x \equiv 6 \bmod 7$
  $f'(6) = 4 \cdot 6^3 = 4 \cdot 6 \cdot 6^2 \equiv 3 \cdot 1 \equiv 3 \not\equiv 0 \bmod 7$
  $\Rightarrow$ $f(6 + t \cdot 7) \equiv 0 \bmod 7^2$ for a unique $0 \leq t < 7$
  $f(6 + 6 \cdot 7) \equiv 0 \bmod 7^2$.

$\Rightarrow$ 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 $\operatorname{ord}_n a = 4$
~~$\operatorname{ord}_n a = 4$~~ is a zero of the function in $\mathbb{Z}_n$

$\Rightarrow$ $1 + \#\{a \mid \operatorname{ord}_n a = 4\}$ 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
$\#\{a \mid \operatorname{ord}_5 a = 4\} = 4$ and in fact, these are ~~the~~ 4
~~zeros in $\mathbb{Z}_5$~~ of $f(x)$ in $\mathbb{Z}_5$

6 → see last page

TATA54 TEN1 3.6.21
Flow10 number 1
page 6

5) let $x = a+ib$ and $y = c+id$, a,b,c,d integers $\forall$, then

$$(2+i)x + (1+i)y = (2+i)(a+ib) + (1+i)(c+id) =$$
$$= 2a + 2ib + ia - b + c + id + ic - d$$
$$= (2a - b + c - d) + i(2b + a + d + c) = 0 + i$$

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

$\Leftrightarrow$ $c = b + d - 2a$ and $2b + a + d + c = 2b + a + d + b + d - 2a$
$= 3b + 2d - a = 1$
$\Leftrightarrow$ $a = 3b + 2d - 1$

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

~~$(5b + 2d - 1 + ib, -2b - d + 1 + id)$ are solutions to the Diophantine equation for every b, d integer~~ b, d

for every integer b and d

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

JATA54 TEN 1 3.6.21
Flow10 number 1
page 7

6) $7^x \equiv -5 \mod 29$

$\Leftrightarrow 7^x \equiv 24 \mod 29$

$\Leftrightarrow \operatorname{ind}_2(7^x) \equiv \operatorname{ind}_2(24) \mod 28$

$\Leftrightarrow x \cdot \operatorname{ind}_2 7 = \operatorname{ind}_2 24 \mod 28$ (Thm 9.16 iii) $\varphi(29) = 28$

$\Leftrightarrow 12x \equiv 8 \mod 28$ (see table)

$\Leftrightarrow 4x \equiv 12 \mod 28$ multiply with 4

$\Leftrightarrow x \equiv 3 \mod 7$ (Thm 4.5 : $(4, 28) = 4$)

TATA 54 TEN 1 3.6.21
Flow ID number 1
page 8

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

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

and then use the Möbius inversion formula.

- Thm 7.14 states that $\mu(d)$ is multiplicative;
then $\mu^2(d)$ is multiplicative, too:
m, n relatively prime positive integers, then
$\mu^2(m \cdot n) = \mu(m \cdot n)\mu(m \cdot n) = \mu(m)\mu(n)\mu(m)\mu(n) = \mu^2(m)\mu^2(n)$
and by Thm 7.8 $\sum_{d|n} \mu^2(d)$ is multiplicative

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

$$2^{\omega(nm)} \overset{\uparrow}{=} 2^{\omega(n)+\omega(m)} = 2^{\omega(n)} 2^{\omega(m)}$$

n, m don't share any prime factors

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

$2^{\omega(p^a)} = 2^1 = 2$
$\sum_{d|n} \mu^2(p^a) = \mu^2(p) + \mu^2(1) = 1 + 1 = 2$
$2^{\omega(1)} = 2^0 = 1$
$\sum_{d|1} \mu^2(d) = \mu^2(1) = 1$

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

$\Rightarrow$ Thm 7.16 $f(n) = \mu^2(d) = \sum_{d|n} \mu(d) F(\frac{n}{d}) = \sum_{d|n} \mu(d) 2^{\omega(\frac{n}{d})}$

□

TATA54 TEN1 3.6.21
FLOW ID number 1
page 9

4c) $1 + \#\{a \mid \mathrm{ord}_n a = 2 \text{ or } \mathrm{ord}_n a = 4\}$ 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 $\mathrm{ord}_n a = 2$ or $\mathrm{ord}_n a = 4$ is a zero of the function in $\mathbb{Z}_n$ since by definition then $a^4 = (a^2)^2 \equiv 1 \bmod n$

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