

OM 2020 — Stage 1

Jakub Kądziołka

January 4, 2021

Contents

1 Series I (September)	1
1.1 Problem 1	1
1.2 Problem 3	1

1 Series I (September)

1.1 Problem 1

theory *SeriesI*

imports

Complex-Main

HOL-Analysis.Analysis

begin

Let a, b be real numbers. Let's assume that, for all real numbers x, y the inequality $|(ax + by)(ay + bx)| \leq x^2 + y^2$ is satisfied. Show that $a^2 + b^2 \leq 2$.

theorem *problem1*:

fixes $a\ b :: \text{real}$

assumes *given*: $\bigwedge x\ y :: \text{real}. |(a*x + b*y)*(a*y + b*x)| \leq x^2 + y^2$

shows $a^2 + b^2 \leq 2$

proof –

from *given* **[where** $x=1$ **and** $y=1$ **] have** $(a+b)^2 \leq 2$

by (*simp add: power2-eq-square*)

moreover from *given* **[where** $x=1$ **and** $y=-1$ **] have** $(a-b)^2 \leq 2$

by (*simp add: power2-eq-square right-diff-distrib'*)

ultimately have $(a+b)^2 + (a-b)^2 \leq 4$ **by** *auto*

moreover have $(a+b)^2 + (a-b)^2 = 2*(a^2 + b^2)$ **by** *algebra*

ultimately show $a^2 + b^2 \leq 2$ **by** *auto*

qed

1.2 Problem 3

Let's assume that a positive integer n has no divisor d that satisfies $\sqrt{n} \leq d \leq \sqrt[3]{n^2}$. Prove that n has a prime divisor $p > \sqrt[3]{n^2}$.

```

theorem problem3:
  fixes  $n :: \text{nat}$ 
  assumes [iff]:  $n \neq 0$ 
  assumes divrange:  $\bigwedge d :: \text{nat}. \text{sqrt } n \leq d \implies d \leq n \text{ powr } (2/3) \implies \neg d \text{ dvd } n$ 
  obtains  $p$  where prime  $p$  and  $p > n \text{ powr } (2/3)$ 
proof -
  have forbidden-range:  $\neg d \text{ dvd } n$  if  $n \text{ powr } (1/3) \leq d$  and  $d \leq n \text{ powr } (2/3)$ 
for  $d :: \text{nat}$ 
proof
  assume  $d \text{ dvd } n$ 
  from that consider
    (low)  $n \text{ powr } (1/3) \leq d \wedge d \leq \text{sqrt } n$  |
    (high)  $\text{sqrt } n \leq d \wedge d \leq n \text{ powr } (2/3)$ 
    by fastforce
  then show False
proof cases
  case low
    from  $\langle d \text{ dvd } n \rangle$  have mirror-divisor:  $(n \text{ div } d) \text{ dvd } n$  by auto

    have  $n/d \leq n / n \text{ powr } (1/3)$ 
      using low by (simp add: frac-le)
    also have  $\dots = n \text{ powr } 1 / n \text{ powr } (1/3)$  by auto
    also have  $\dots = n \text{ powr } (2/3)$  by (simp del: powr-one flip: powr-diff)
    finally have  $n/d \leq n \text{ powr } (2/3)$ .
    moreover from  $\langle d \text{ dvd } n \rangle$  have  $n/d = n \text{ div } d$  by auto
    ultimately have upper-bound:  $n \text{ div } d \leq n \text{ powr } (2/3)$  by auto

    from  $\langle d \text{ dvd } n \rangle$  have  $d \neq 0$ 
      by (meson  $\langle n \neq 0 \rangle \text{ dvd-0-left}$ )
    hence  $n/d \geq n / \text{sqrt } n$ 
      using low by (simp add: frac-le)
    also have  $n / \text{sqrt } n = \text{sqrt } n$ 
      using real-div-sqrt  $\langle n \neq 0 \rangle$  by auto
    finally have  $n/d \geq \text{sqrt } n$ .
    hence lower-bound:  $n \text{ div } d \geq \text{sqrt } n$  using  $\langle n/d = n \text{ div } d \rangle$  by auto

    show False using divrange [of  $n \text{ div } d$ ] mirror-divisor
      and lower-bound upper-bound by auto
  next
    case high
    then show False using divrange  $\langle d \text{ dvd } n \rangle$  by auto
qed
qed

have  $n > 1$ 
proof -
  {
    assume  $n = 1$ 
    with divrange [of 1] have  $\neg 1 \text{ dvd } 1$  by auto
  }

```

```

    moreover have 1 dvd (1::nat) by auto
    ultimately have False by contradiction
  }
  thus n > 1 using ⟨n ≠ 0⟩
    by fastforce
qed

let ?smallldivs = {d. d dvd n ∧ d < n powr (1/3)}
have finite ?smallldivs using finite-divisors-nat by fastforce
moreover have ?smallldivs ≠ {} proof -
  have 1 ∈ ?smallldivs using ⟨n > 1⟩ by auto
  thus ?thesis by auto
qed

moreover define a where a = Max ?smallldivs
ultimately have a ∈ ?smallldivs using Max-in by auto
hence a < n powr (1/3) and a dvd n by auto
hence a ≠ 0 using ⟨n ≠ 0⟩ by algebra
have ∧d. d dvd n ⇒ d > a ⇒ d ≥ n powr (1/3)
  using Max-ge ⟨finite ?smallldivs⟩ ⟨?smallldivs ≠ {}⟩ a-def
  by (metis (no-types, lifting) mem-Collect-eq not-le)
hence div-above-a: ∧d. d dvd n ⇒ d > a ⇒ d > n powr (2/3)
  using forbidden-range
  by force

note ⟨a < n powr (1/3)⟩
also have n powr (1/3) < n powr 1 using ⟨n > 1⟩ by (intro powr-less-mono)
auto
finally have a < n by auto
hence n div a > 1
  using ⟨a dvd n⟩ by fastforce
then obtain p where prime p and p dvd (n div a)
  by (metis less-irrefl prime-factor-nat)
hence p*a dvd n using ⟨a dvd n⟩ and ⟨n div a > 1⟩
  by (metis div-by-0 dvd-div-iff-mult gr-implies-not-zero)
with div-above-a [of p*a] have p*a > n powr (2/3)
  using ⟨prime p⟩ and prime-nat-iff by fastforce
moreover have a * n powr (1/3) < n powr (1/3) * n powr (1/3)
  using ⟨a < n powr (1/3)⟩ by auto
moreover have ... = n powr (2/3) by (simp flip: powr-add)
ultimately have p*a > a*n powr (1/3) by simp
hence p > n powr (1/3) using ⟨a ≠ 0⟩ by simp
hence p > n powr (2/3) using forbidden-range [of p] and ⟨p * a dvd n⟩ by
force
  moreover note ⟨prime p⟩
  ultimately show ?thesis using that [of p] by auto
qed
end

```