Pinter Consulting
New Series Nos. 16.
Spartan Old School Tutorials
(Rough Copy)

J K Pinter, Dr.Tech.

July 25, 2019

Motto

- Meg(g)y? Nem meg(g)y?
- Meg(g)y, de néha erőltetni kell az igényes matematikai továbbképzést.

- **"Der springt noch auf!"**
- Private studies for professional development:
- Socratic Programme
  - Analysis
  - Algebra and Number Theory
  - Geometry
  - Differential and Integral Equations
- Continuos improvement, corrections and last revision July 25, 2019.
- These are my principles, and if you don't like them ... well, then I have others: 

- - - -

Introduction

Pinter Consulting of Calgary, Alberta practices Mathematics, promotes clear thinking and offers Consultations, Tutorials and Seminars in Mathematics.

Summary

The Report is best viewed as an exercise book recording the systematic, diverse and high quality work under the direction of Dr Melvin No, Privatdozent, now retired. The notes were taken by Scholar Wagner at the Summer School of 2019. Dr Melvin No approves Scholar Wagner's efforts.

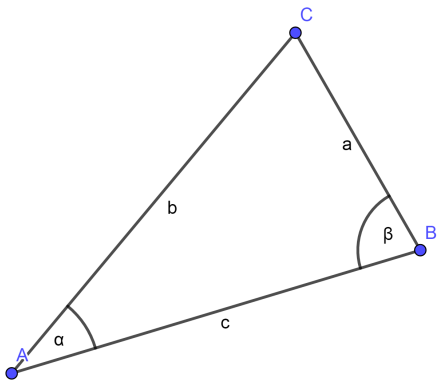
The Report was prepared May 15 through July 31, 2019.

Contents

19.0 Tutorial 6.

Summary

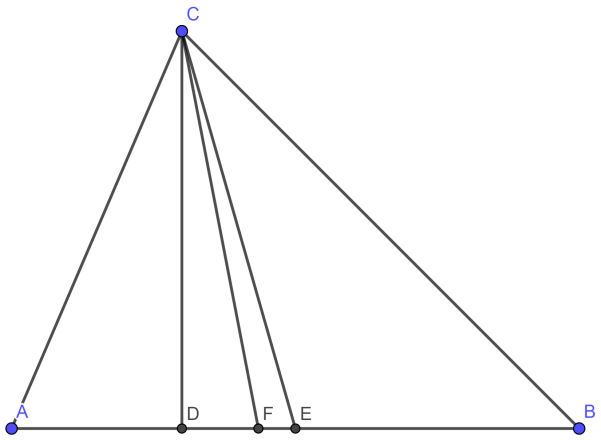
- *Geometry, Spartan Old School Tutorials*
- *Hajós et.; ELTE*
- Last revision July 25, 2019



Notation: Standard. $\triangle ABC$ has vertices A, B, and C ; sides AB, BC and CA, and angles α, β, γ. Vertices A, B, and C are in counterclockwise direction, the sides opposite to A, B, and C are denoted by a, b, and c, respectively. Angle α is at A; β at B; and γ at C. The angle at A can be marked as $\angle A$.

A *cevian* of a triangle is a line from a vertex to a point on the opposite side.(Giovanni Ceva, geometer, Italy, 17th century). An angle *bisector* of a triangle is a line that bisects an angle and extends to the opposite side. A *median* of a triangle is a line from a vertex to the midpoint of

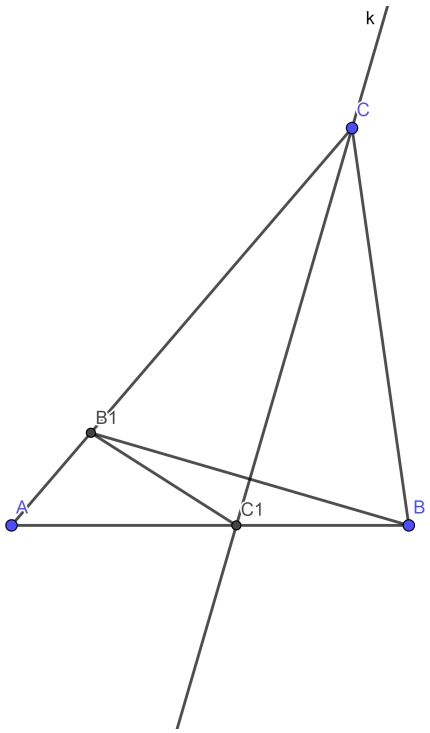
the opposite side. An *altitude* of a triangle is a line from a vertex perpendicular to the opposite side. Bisectors, medians, altitudes are cevians.



Sides and angles in a triangle 3.1

3. Let the bisector of $\angle C$ of $\triangle ABC$ cut the side AB at C_1 and let $AC > BC$. Prove that

$$AC_1 > C_1B; \quad \angle AC_1C > \angle BC_1C$$



Proof: (Recall Lemma on opposite sides and opposite angles: the greater side is opposite to the greater interior angle.)

Let B_1 be the reflected image of point B on line CC_1. Then B_1 is an inner point of AC, because $BC < AC$. In $\triangle ABC$

$$\angle A + \angle B + \angle C = \pi.$$

Since $AC > BC$, $\angle B > \angle A$; by Lemma on opposite sides and opposite angles. Moreover, by bisection

$$\angle ACC_1 = \angle BCC_1.$$

Therefore

$$\angle ACC_1 + \angle CC_1A + \angle A = \pi$$

$$\angle BCC_1 + \angle CC_1B + \angle B = \pi$$

$$\angle AC_1C > \angle BC_1C.$$

This proves the statement on angles.

Further, $\angle AB_1C$ is supplementary to AB_1C_1:

$$\angle AB_1C1 = \pi - \angle C_1B_1C = \pi - \angle B$$

Suppose, if possible,

$$\angle AB_1C_1 \leq \angle A$$

$$\pi - \angle B \leq \angle A$$

$$\pi \leq \angle A + \angle B$$

but this is absurd because $\angle A + \angle B + \angle C = \pi$. Therefore

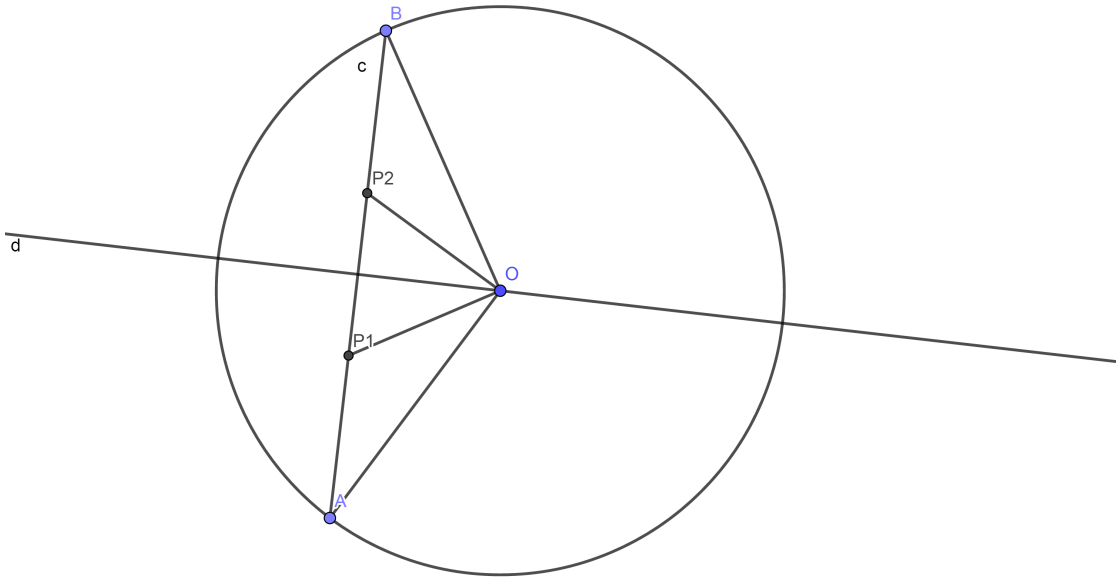
$$\angle AB_1C_1 > \angle A,$$

which implies

$$AC_1 > B_1C_1 = C_1B$$

by the Lemma.

4. On a circle of radius r and center O let A and D be two points, not diametrically opposite. Consider the chord AD and the associated arch which is less than a semi-circle. Let two radii, OB and OC *trisect* $\angle AOD$. Do they cut AD into 3 into equal parts?



No, $AP_1 = BP_2$, due to the symmetry about line d, on the other hand, $\triangle AOP_2$ satisfies the conditions of *Problem 3.* :

$$r = AO > OP_2; \quad \angle AOP_1 = \angle P_1OP_2.$$

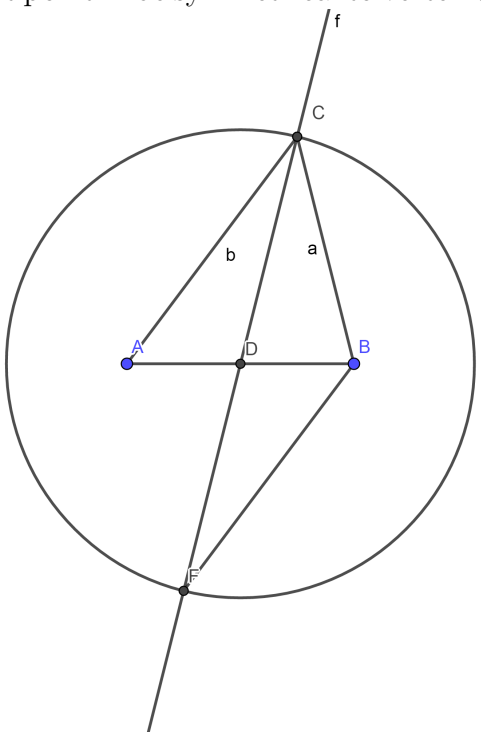
$$AP_1 = BP_2 > P_1P_2,$$

There are 3 unequal parts.

5. Let $AC > CB$ in $\triangle ABC$. If D is the midpoint of AB then

$$\angle ACD < \angle BCD; \quad \angle ADC > \angle BDC.$$

Proof: Let point F be symmetrical to vertex C with respect to midpoint D.



In $\triangle CFB$, $CB < FB$ because $FB = AC$, hence $\angle ACD = \angle BFC < \angle DCB$. Next, if we drop a permendicular to AB at D, then C is in the half- plane containing B, that means $\angle ADC$ is greater than a right angle, and $\angle CDB$, the complementary angle is less than a right angle:

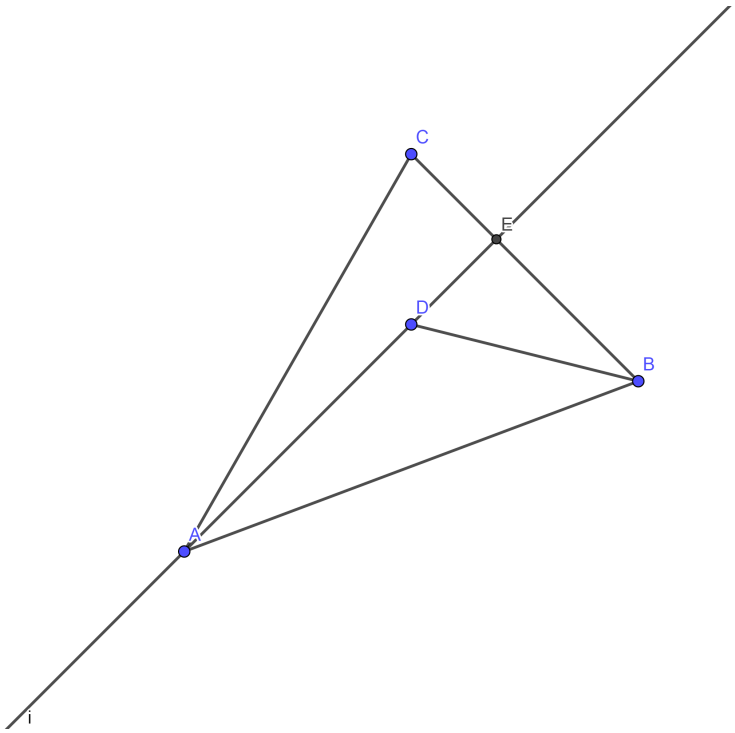
$$\angle ADC > \frac{\pi}{2} > \angle BDC.$$

Triangle Inequalities 3.2

The triangle inequality says that any side is less than the sum of the other two sides.

8. A point D is inside of triangle $\triangle ABC$. Prove that

$$AC + CB > AD + DB.$$



Proof:

$$AC + CB = AC + CE + EB = (AC + CE) + EB > AE + EB.$$

$$AE + EB = AD + DE + EB > AD + DB.$$

$$AC + CB > AD + DB.$$

9. Any side of a triangle ABC is less than half the perimeter.

Proof:

$$a < b + c;\ b < a + c;\ c < a + b;$$

$$a + a < b + c + a;\ b + b < a + c + b;\ c + c < a + b + c;$$

$$a < \frac{a + b + c}{2};\ b < \frac{a + b + c}{2};\ c < \frac{a + b + c}{2};$$

10. Given $\triangle ABC$. Let D be a point on AB. Then

$$\frac{1}{2}(AC + BC - AB) < CD < \frac{1}{2}(AC + BC + AB)$$

Proof: Let D be an inner point of AB.

$$AC + AD > CD$$

$$CB + DB > CD$$

$$AC + CB + (AD + DB) > 2CD$$

$$CD < \frac{AC + CB + AB}{2} = \frac{1}{2}(AC + BC + AB).$$

This proves the right-hand side. Moreover

$$AC < ACD + CD$$

$$BC < CDB + CD$$

$$AC + BC < AB + 2CD$$

$$AC + BC - AB < 2CD$$

$$\frac{AC + BC - AB}{2} < CD$$

This proves the left-hand side.

11. Draw a line from each vertex A, B, C of a triangle $\triangle ABC$ to an inner point on the opposite side, A_1, B_1, C_1, respectively. Show that the sum of the three resulting Cevians AA_1, BB_1, CC_1 is greater than half of the perimeter but less than three times half of the perimeter.

Proof: Corollary to 10.

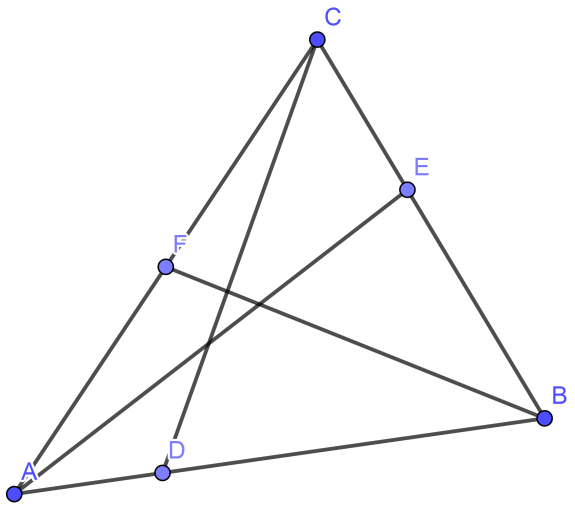
$$\frac{1}{2}(AC + BC - AB) < CC_1 < \frac{1}{2}(AC + BC + AB)$$

$$\frac{1}{2}(AC + AB - BC) < AA_1 < \frac{1}{2}(AC + BC + AB)$$

$$\frac{1}{2}(AB + BC - AC) < BB_1 < \frac{1}{2}(AC + BC + AB)$$

Adding these three lines

$$\frac{1}{2}(AB + BC + CA) < AA_1 + BB_1 + CC_1 < \frac{3}{2}(AC + BC + AB).$$



12. In a triangle $\triangle ABC$ the median s_c

$$\frac{1}{2}(a+b-c) < s_c < \frac{1}{2}(a+b).$$

Proof: The left-hand side of the inequality was proved in 10. The right-hand side follows from the triangle inequality on $\triangle BCF$. Let D be the midpoint on AB, extend the median s_c past D and draw a line parallel to side b through point B. These two intersect at point F.(See Figure to Problem 5.)

$$\angle ADC = \angle BDF$$

$$\angle CAD = \angle FBC$$

$$AD = DB$$

Therefore $\triangle ADC$ is congruent to $\triangle BDF$ and

$$CD = DF$$

$$2s_c < a + b$$

$$s_c < \frac{1}{2}(a+b).$$

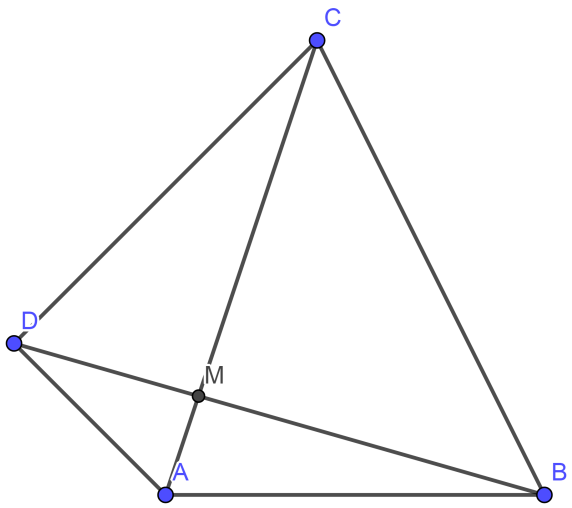
19. Let $ABCD$ be a convex quadrilateral. The sum of diagonals is greater than the sum of opposite sides.

Proof: Since $ABCD$ is convex, the diagonals AC, DB are in it. Diagonals intersect at M, which is in the interior of the quadrilateral. Consider $\triangle ABM$ and $\triangle CDM$. Apply triangle inequality.

$$AB < AM + MB$$

$$DC < CM + MD$$

$$AB + DC < (AM + MB) + (CM + MD) = AC + BD.$$



20. Let $ABCD$ be a convex quadrilateral. The sum of diagonals is less than the perimeter but greater than half of the perimeter.

Proof:

$$\frac{1}{2}(AB + BC + CD + DA) < AC + BD.$$

$$AC + BD < AB + BC + CD + DA.$$

22. In a convex quadrilateral there exists a side which is less than the greater diagonal. (See Figure to Problem 19.)

$$AB < AM + MB; \quad BC < BM + CM;$$

$CD < CM + DM; \quad DA < DM + AM.$

$4 \min (AB, BC, CD, DA) \leq (AB + BC + CD + DA) < 2(AC + BD)$

$2(AC + BD) \leq 4 \max (AC, BD).$

$\min (AB, BC, CD, DA) < \max (AC, BD).$

19.1 Tutorial 8.

Summary

- Elementary Number Theory *Niven, Davenport, Guy*
- *Spartan Old School*
- Last revision July 25, 2019

Section 2.1, pg 20, Pr 54, : Let a and b be positive integers such that $(1+ab)|(a^2+b^2)$. Show that the integer $(a^2+b^2)/(1+ab)$ must be a perfect square.

Proof: Write

$$\frac{a^2+b^2}{1+ab} = k$$

where k is an integer, $k > 0$. If $k = 1$ then there is nothing to prove, $k = 1 = 1^2$, a perfect square. We proceed to show that $k = 2$ is impossible. For if $k = 2$, then

$$\frac{a^2+b^2}{1+ab} = 2$$

$$a^2+b^2 = 2(1+ab)$$

$$a^2-2ab+b^2 = 2$$

$$(a-b)^2 = 2,$$

a contradiction: 2 is not a square of an integer. Therefore it is sufficient to consider $k \geq 3$.

We note that we cannot relax the condition $a > 0$, $b > 0$. If one of a and b is negative and the other is positive, then $ab < 0$. Hence $ab \leq -1$, thus $k(ab+1) \leq 0$. However $a^2+b^2 = k(ab+1)$ is strictly positive.

Next, we examine the curve $\Gamma \equiv x^2+y^2-k(xy+1) = 0$. Write

$$Ax^2+Bxy+Cy^2+Dx+Ey+F = 0$$

where $A = C = 1,\ B = -k,\ D = E = 0,\ F = -k$. Γ is a conic section with discriminant $B^2 - 4AC > 0$, for $B^2 \geq 9$ and $4AC = 4$. Therefore Γ represents a hyperbola.

We also note that the axis of symmetry which does not intersect the hyperbola on the real plane is $x = y$:

$$x^2 + x^2 - k(x^2 + 1) = 0.$$

$$(2 - k)x^2 = k.$$

The last equation is not satisfied by real x because $k \geq 3$. This shows further that $a = b$ is not a solution.

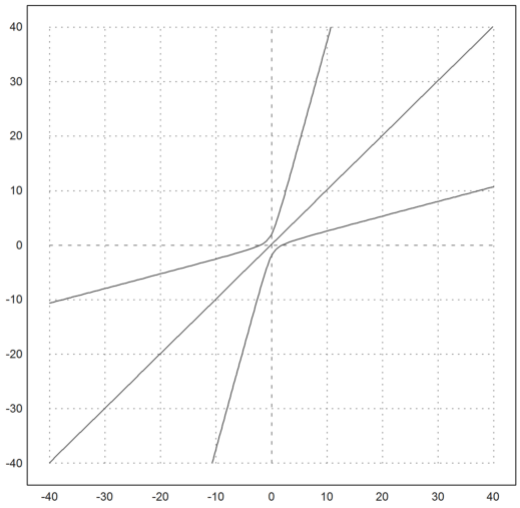


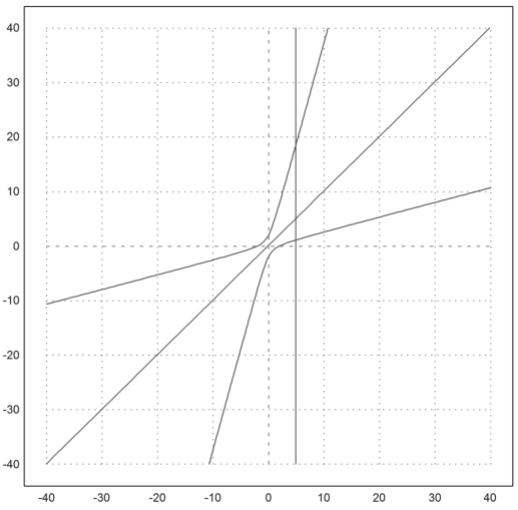
Illustration of $\Gamma \equiv x^2 + y^2 - k(xy + 1) = 0$ with $k = 4$ plus $x = y$ axis of symmetry.

Suppose now that $P = P(a, b)$ is a positive integer solution, $b > a$, that is point P is on the upper branch of the curve Γ and drop a vertical line through P. We substitute a and b into Γ to obtain

$$a^2 + b^2 = k(ab + 1).$$

Clearly, b is the root of the quadratic $z^2 - kaz + (a^2 - k) = 0$. By Vieta's formulas, (on roots and coefficients) we have $b + c = ka$, or $c = ka - b$, c is an integer. As $b > a$ $P(a, b)$ is on the upper branch and $Q(a, c)$ is on the lower branch, below $x = y$, hence $c < b$. Therefore from a hypothetical

solution $P(a, b)$ we arrive at another, smaller positive solution $Q(a, c)$ with



$c < b$.

This is the so-called Vieta-jumping. Moreover, by reflecting in the line and axis of symmetry $x = y$ we obtain a solution $P'(c, a)$, with $c < b$. By repeating the process we get smaller and smaller solutions until one of the coordinates is zero. Write $b = 0$, then $a^2 = k$, and the claim is proven.

Three easy problems: i) Show that for positive integer n , $n > 1$ there exist positive integers a, b such that

$$n^3 = a^2 - b^2.$$

Suppose n is odd. Then n^3 is odd, also, that is

$$n^3 = 2y + 1$$

for some y. Write $a = y + 1$, $b = y$.

$$a^2 = (y + 1)^2 = y^2 + 2y + 1; \quad b^2 = y^2;$$

$$n^3 = a^2 - b^2 = 2y + 1.$$

$$y = \frac{n^3 - 1}{2}.$$

Next, suppose n is even. Set $a = x + 2$; $b = x$.

$$n^3 = a^2 - b^2 = 4x + 4 = 4(x + 1).$$

$$x = \frac{n^3}{4} - 1.$$

Check the result: $n = 2$, $n^3 = 8 = 4(x+1)$, therefore $x = 1$. Next, $n = 4$, $n^3 = 64 = 4(x+1)$, therefore $x = 15$, $a^2 = 289$, $b^2 = 225$, $a^2 - b^2 = 64$.

ii) Find positive integers x, y, z; $z < y < x$ such that

$$\frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}.$$

We derive the solution from Pythagorean triple (a, b, c), one can consider $(3, 4, 5)$, $3^2 + 4^2 = 5^2$, for example.

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

The equation remains valid when divided by n^2.

$$\frac{a^2 + b^2}{n^2} = \frac{c^2}{n^2}$$

$$\frac{a^2}{n^2} + \frac{b^2}{n^2} = \frac{c^2}{n^2}$$

Set $n = abc$.

$$\frac{a^2}{a^2b^2c^2} + \frac{b^2}{a^2b^2c^2} = \frac{c^2}{a^2b^2c^2}$$

$$\frac{1}{b^2c^2} + \frac{1}{a^2c^2} = \frac{1}{a^2b^2}$$

$$\frac{1}{(bc)^2} + \frac{1}{(ac)^2} = \frac{1}{(ab)^2}; \quad bc > ac > ab$$

$$x = bc;\ y = ac;\ z = ab$$

Using the above Pythagorean triple

$$\frac{1}{20^2} + \frac{1}{15^2} = \frac{1}{12^2}$$

is a solution. Different triplets will result in different solutions.

iii) If n is odd, then $n^2 - 1$ is divisible by 8. Write $n = 2k + 1$, $n^2 = 4k^2 + 4k + 1$,

$$n^2 - 1 = 4k^2 + 4k = 4k(k+1)$$

Either k or $k+1$ is even, so $k(k+1)$ has factor 2. Therefore $4 * 2 = 8$ divides $n^2 - 1$.

Pythagorean triples and infinite descend This standard result is included here for the historical importance. Infinite descend is Fermat's proof.

(i) Prove that the quadratic Diophantine equation

$$x^2 + y^2 = z^2,\ x > 0,\ y > 0,\ z > 0,\ (x, y, z) = 1,$$

is satisfied by

$$x = 2uv,\ y = u^2 - v^2\ z = u^2 + v^2$$

where

$$u > v > 0;\ uv = 0 \text{ even}$$

moreover all solutions are of this form. The three integers x, y, z are called a Pythagorean triple.

Claim: For Pythagorean triple (x, y, z)

$$(x, y, z) = 1\ \Rightarrow (x, y) = 1 \wedge (x, z) = 1 \wedge (y, z) = 1$$

That is, if they are mutually prime, then they are pairwise prime. Suppose, if possible,

$$(x, y) = d > 1$$

and let p be a prime factor of d. Then

$$x = pk,\ y = pl, x^2 = p^2k^2,\ y^2 = p^2l^2$$

for some positive integers k, l.

$$x^2 + y^2 = p^2k^2 + p^2l^2 = p^2(k^2 + l^2) = z^2$$

and thus $p^2 \mid z^2$. Upon the unique factorization of z^2 we find $p^{2\alpha}$, thus z has a factor p^α, and the condition $(x, y, z) = 1$ is violated.

Suppose now, that

$$(x, z) = d > 1.$$

$$x = pk, z = pm$$

$$y^2 = z^2 - x^2 = p^2(k^2 - m^2)$$

If

$$y = p^{\beta} q^{\gamma} ... s^{\delta}$$

then

$$y^2 = p^{2\beta} q^{2\gamma} ... s^{2\delta}$$

where on the other hand

$$y^2 = z^2 - x^2 = p^2(k^2 - m^2)$$

Comparing the unique factorization to the last line, we see that $\beta \geq 1$ thus $p \mid y$. Contradiction.

Corollary: x and y cannot be both even.

Claim: Moreover, x and y cannot be both odd. Suppose again, if possible, that both x and y are odd. Then

$$x \equiv \pm 1; y \equiv \pm 1, \pmod 4$$

$$z^2 = x^2 + y^2 = 1 + 1 = 2 \pmod 4$$

Thus z^2 is even hence z is even yet z^2 is not divisible by 4. That is absurd.

Therefore we may state without loss of generality, that one of x and y, -say x - is even, y is odd and z is odd.

Knowing that x is even, write

$$\left(\frac{x}{2}\right)^2 = \frac{z^2 - y^2}{4} = \frac{z+y}{2} * \frac{z-y}{2}.$$

Both $\dfrac{z+y}{2}$ and $\dfrac{z-y}{2}$ are integers, because z and y are odd. Further

$$\left(\frac{z+y}{2}, \frac{z-y}{2}\right) = 1,$$

for if $d > 1$, and

$$d \mid \frac{z+y}{2}; \quad d \mid \frac{z+y}{2}$$

then sum and difference are divisible, as well,

$$d \mid \frac{z+y}{2} \pm \frac{z-y}{2} = \begin{cases} z \\ y \end{cases}$$

but this contradicts $(y, z) = 1$. Therefore there are no common prime factors in

$$\frac{z+y}{2}; \quad \frac{z-y}{2}$$

So $\left(\frac{x}{2}\right)^2$ is square number and each of its prime factor $p^{2\alpha}$ has an even exponent. But p cannot be factor in both terms, $\frac{z+y}{2}; \quad \frac{z-y}{2}$. Therefore $p^{2\alpha}$ is a factor in one and only one term. This makes the terms $\frac{z+y}{2}; \quad \frac{z-y}{2}$ square numbers:

$$\frac{z+y}{2} = m^2; \quad \frac{z-y}{2} = n^2; \quad (m, n) = 1.$$

Whence we obtain

$$z = m^2 + n^2; \quad y = m^2 - n^2; \quad x = 2nm.$$

In order to conform with the assumption on the parity of x and y, m, n are set to be odd, and $m > n$.

Let us check our results

$$(2nm)^2 + (m^2 - n^2)^2 = (m^2 + n^2)^2$$

$$(2nm)^2 + (m^2)^2 - 2m^2 * n^2 + (n^2)^2 = (m^2)^2 + 2m^2 * n^2 + (n^2)^2$$

$$4n^2 * m^2 + (m^2)^2 - 2m^2 * n^2 + (n^2)^2 = (m^2)^2 + 2m^2 * n^2 + (n^2)^2$$

$$(m^2)^2 + 2m^2 * n^2 + (n^2)^2 = (m^2)^2 + 2m^2 * n^2 + (n^2)^2; \ \surd$$

All solutions are of the form

$$z = (m^2 + n^2) * d; \quad y = (m^2 - n^2) * d; \quad x = 2nm * d$$

for d positive integer.

Claim: $x^4 + y^4 = z^2$ **has no solution in positive integers**

1. Lemma If positive integers u and v are relative prime numbers whose product uv is a perfect square, then u and v are both perfect squares.

Proof: Let p be a prime that divides u, and let α be the exact power of p in u. Since u and v are relative prime, p does not divide p, therefore the exact power of p in uv is α. But uv is a perfect square, so α must be even. Since this holds for all primes p dividing u, it follows that u is a perfect square. Same applies to v.

2. Hypothesis:

$x^4 + y^4 = z^2$, x,y,z positive integer, z minimal

Proof is by contradiction, we shall find a smaller z, so we could construct a sequence of descending z-s

$$z_1 > z_2 > z_3 > \dots$$

But this is absurd, because a set of positive integers is bounded by 0 from below.

3. (x,y,z)=1 Suppose p divides x, y, z. Then

$$p^4 \mid x^4 + y^4 \Rightarrow p^4 \mid z^4 \Rightarrow p^2 \mid z^2$$

$$\frac{x^4 + y^4}{p^4} = \frac{z^2}{p^4} \Rightarrow \left(\frac{x}{p}\right)^4 + \left(\frac{y}{p}\right)^4 = \left(\frac{z}{p^2}\right)^2$$

This implies

$$\left(\frac{z}{p^2}\right) < z$$

which is a contradiction, for z is minimal. Therefore $(x, y, z) = 1$; and in particular, all three variables x, y, z cannot be even.

4. x even, y odd We start proving this statement by supposing that x and y are odd. Then $x \equiv 1$, $y \equiv 1 \pmod 8$. Write

$$x = 2a + 1$$

$$x^4 = (2a)^4 + 4(2a)^3 + 6(2a)^2 + 4(2a) + 1$$

$$x \equiv 1, \pmod 8$$

Same for y,

$$y \equiv 1, \pmod 8$$

$$x^4 + y^4 \equiv 2 \pmod 8 \Rightarrow z^2 \equiv 2, \pmod 8 .$$

Write $z = 8k + b$. Calculate z^2 in (mod 8).

b	0	1	2	3	4	5	6	7
b^2	0	1	4	1	0	1	4	1

Clearly, there is no solution for $z^2 \equiv 2, \pmod 8$. Hence x, y are of different parity, we set x even and y odd. This makes z^2 odd, too.

5. Claim: $((z - x^2), (z + x^2)) = 1$ Write

$$y^4 = z^2 - x^4 = (z - x^2)(z + x^2)$$

If p divides $(z - x^2)$ and $(z + x^2)$ then p divides their product, sum and difference, so p would divide y^4, $2z$, $2x^2$. but this is absurd, because y is odd, $2z$ is even, and $2x^2$ is even, moreover $(x, y, z) = 1$. There is no p dividing both $(z - x^2)$, $(z + x^2)$, thus they are relative prime numbers.

By the Fundamental Theorem

$$y = p_1^{\alpha_1} \dots p_n^{\alpha_n}, y^4 = p_1^{4\alpha_1} \dots p_n^{4\alpha_n}, y^4 = (p_1^{4\alpha_1} \dots)(\dots p_n^{4\alpha_n})$$

$$(z - x^2) = u^4, \quad (z + x^2) = v^4, \quad (v^2 - u^2)(v^2 + u^2) = 2x^2$$

5. Claim: $v^2 - u^2 = a^2, v^2 + u^2 = 2b^2$

$$(z - x^2) \equiv 1, \mod 2; \quad (z + x^2) \equiv 1, \mod 2$$

$$u \equiv v \equiv 1, \mod 2; \quad u^2 + v^2 \equiv 2 \mod 4;$$

There is no prime p that divides $v^2 - u^2$, and $v^2 + u^2$ because $(u, v) = 1$. Therefore $v^2 - u^2$ is a square and $v^2 + u^2$ is twice a square.

6. Claim: $v^2 = a^2 + u^2$; **Pythogorean triple** From $v^2 - u^2 = a^2, v^2 + u^2 = 2b^2$ we have a $v^2 = a^2 + u^2$ Pythogorean triple; so

$$v = r^2 + s^2; \quad u = r^2 - s^2; \quad a = rs$$

where r, s positive integers.

$$v^2 = r^4 + 2r^2s^2 + s^4; \quad u^2 = r^4 - 2r^2s^2 + s^4;$$

$$v^2 + u^2 = 2r^4 + 2u^4$$

$$\frac{1}{2}(v^2 + u^2) = r^4 + u^4$$

$$b^2 = r^4 + u^4$$

It is the same form as $x^4 + y^4 = z^2$. We arrive at a contradiction if $b < z$, for z is assumed to be minimal.

6. Claim: $z \geq b$**, contradiction.**

$$u = v = 1 \text{ impossible}$$

$$z - x^2 = u^4 = 1$$

$$z + x^2 = v^4 = 1$$

$$(z - x^2) - (z + x^2) = 0 \Rightarrow x^2 = 0$$

$$z - x^2 = u^4; \quad z + x^2 = v^4 \quad \Rightarrow 2z = u^4 + v^4$$

$$z = \frac{u^4 + v^4}{2} > \frac{u^2 + v^2}{2} = b^2 > b.$$

This shows that z is not minimal, which is a contradiction. Therefore only trivial solutions exist: $x = 0,\ y,\ z = \pm y^2$, and $x\ y = 0,\ z = \pm x^2$.

7. Claim: $x^4 + y^4 = z^4 = (z^2)^2$ **has no solution in positive integers.**

19.2 Tutorial 9.

Summary

- Mathematical Modelling and Numerical Analysis
- *Spartan Old School*
- Last revision July 25, 2019

Preliminaries: In what follows, we review two frequently used numerical methods

- Simpson's rule of integration,
- Runge-Kutta method for the numerical solution of first order differential equation.

Both methods rely on Taylor-expansions for one and two variables. As a reference, we quote the expansions here:

Taylor expansion for single variable:

$$y(x_0 + h) = \sum_{k=0}^{n} \left(h \frac{\partial}{\partial x} \right)^k y(x_0) + R_n(h)$$

Assuming that all derivatives exist up to order $n + 1$ and

$$|y^{n+1}| \leq M;$$

then

$$|R_n(h)| \leq \frac{M}{(n+1)!} h^{n+1}.$$

Taylor expansion for two variables:

$$f(x_0+h, y_0+k) = f(x_0,y_0) + \left(h\frac{\partial}{\partial x} + k\frac{\partial}{\partial y}\right) f(x_0,y_0) +$$

$$\frac{1}{2}\left(h\frac{\partial}{\partial x} + k\frac{\partial}{\partial y}\right)^2 f(x_0,y_0) + \ldots + \frac{1}{n!}\left(h\frac{\partial}{\partial x} + k\frac{\partial}{\partial y}\right)^n f(x_0,y_0) + R_n$$

where the remainder term R_n is given by

$$R_n = \frac{1}{(n+1)!}\left(h\frac{\partial}{\partial x} + k\frac{\partial}{\partial y}\right)^{n+1} f(x_0+\theta h, y_0+\theta k); \quad 0<\theta<1.$$

We use the operator notation :

$$\left(h\frac{\partial}{\partial x} + k\frac{\partial}{\partial y}\right) f(x_0,y_0) = hf_x(x_0,y_0) + kf_y(x_0,y_0)$$

$$\left(h\frac{\partial}{\partial x} + k\frac{\partial}{\partial y}\right)^2 f(x_0,y_0) = h^2 f_{xx}(x_0,y_0) + 2hkf_{xy}(x_0,y_0) + k^2 f_{yy}(x_0,y_0)$$

$$\left(h\frac{\partial}{\partial x} + k\frac{\partial}{\partial y}\right)^n f(x_0,y_0) = \left(h\frac{\partial}{\partial x} + k\frac{\partial}{\partial y}\right)\left(h\frac{\partial}{\partial x} + k\frac{\partial}{\partial y}\right)^{n-1} f(x_0,y_0)$$

If partial derivatives of f of order $n+1$ are bounded by M then

$$|R_n| \le \frac{M}{(n+1)!}(h+k)^{n+1}.$$

Integration of f(x) on [a,b] by Simpson's rule for n intervals Forward differences, standard notation, differentiability assumed throughout:

$x_{k+1} - x_k = h$

$\Delta y_k = y_{k+1} - y_k$

$\Delta^2 y_k = \Delta(\Delta y_k) = \Delta y_{k+1} - \Delta y_k = y_{k+2} - 2y_{k+1} + y_k$

$\Delta^n y_k = \Delta(\Delta^{n-1} y_k)$

$p_k = y_0 + k\Delta y_0 + \frac{1}{3}\Delta^2 y_0$; Newton's forward formula, 2nd degree

$$\int_{x_0}^{x_2} = p(x)dx = h\int_0^2 p_k dk = h\left(2y_0 + 2\Delta y_0 + \frac{1}{3}\Delta^2 y_0\right) = \frac{h}{3}\left(y_0 + 4y_1 + y_2\right)$$

Truncation error is estimated by Taylor-expansion:

$$\frac{h}{3}\left(y_0 + 4y_1 + y_2\right) = \frac{h}{3}\left[y_0 + 4\left(y_0 + hy_0' + \frac{h^2}{2}y_0" + \frac{h^3}{6}y_0^{(3)} + \frac{h^4}{24}y_0^{(4)} + \ldots\right) +\right.$$

$$\left.\left(y_0 + 2hy_0' + 2h^2 y_0" + \frac{4}{3}h^3 y_0^{(3)} + \frac{2}{3}h^4 y_0^{(4)} + \ldots\right)\right] =$$

$$\frac{h}{3}\left[6y_0 + 6hy_0' + 4h^2 y_0" + 2h^3 y_0^{(3)} + \frac{5}{6}h^4 y_0^{(4)} + \ldots\right]$$

.

$$\int_{x_0}^{x_2} y(x)dx = F(x_2) - F(x_1) = 2hF'(x_0) +$$

$$\frac{1}{2}(2h)^2 F"(x_0) + \frac{1}{6}(2h)^3 F^{(3)}(x_0) + \frac{1}{24}(2h)^4 F^{(4)}(x_0) + \frac{1}{120}(2h)^5 F^{(5)}(x_0) + \ldots =$$

$$2hy_0 + 2h^2 y_0' + \frac{4}{3}h^3 y_0" + \frac{2}{3}h^4 y_0^{(3)} + \frac{4}{15}h^5 y_0^4 + \ldots$$

Upon subtracting one from the other

$$\int_{x_0}^{x_2} y(x)dx - \frac{h}{3}\left(y_0 + 4y_1 + y_2\right) = -\frac{1}{90}h^5 y_0^4 + \ldots$$

The truncation error is estimated by the first term

$$-\frac{1}{90}h^5 y_0^{(4)}(\xi); \quad (x_0 < \xi < x_n).$$

Write

$$x_0 = a, \quad x_n = b, \quad b - a = nh.$$

Set n even, and sum up the intervals of length $2h$

$$\frac{h}{3}\left(y_0 + 4y_1 + y_2\right) + \frac{h}{3}\left(y_2 + 4y_3 + y_4\right) + \ldots \frac{h}{3}\left(y_{n-2} + 4y_{n-1} + y_n\right)$$

$$\int_{x_0}^{x_2} y(x)dx \approx \frac{h}{3}\left[y_0 + 4y_1 + 2y_2 + 4y_3 + \ldots + 2y_{n-2} + 4y_{n-1} + y_n\right]$$

and this is the formula to calculate (approximate) the integral. The truncation error for $[a.b]$ y and h is as follows:

$$E(y) = \frac{(b-a)h^4}{180} y_\xi^{(4)}.$$

For comparison,

$$E_1(y) = \frac{(b-a)(2h)^4}{180} y_\xi^{(4)};\ E_2(y) = \frac{(b-a)h^4}{180} y_\xi^{(4)}$$

$$E_2(y) = \frac{E_1(y)}{16},$$

refinement of interval $2h$ to h reduces the error by a factor of 16. The round-off error of the calculation is :

$$y(x_k) = y_k + \epsilon_k;\ \ \max|\epsilon_k| = \epsilon$$

$$\frac{h}{3}\left[\epsilon_0 + 4\epsilon_1 + 2\epsilon_2 + 4\epsilon_3 + \ldots + 2\epsilon_{n-2} + 4\epsilon_{n-1} + \epsilon_n\right] \leq$$

$$\frac{h\epsilon}{3}\left[1 + 4\frac{1}{2}n + 2\left(\frac{1}{2}n - 1\right) + 1\right] = (b-a)\epsilon.$$

The programing of the Simpson's rule takes only a couple of lines. This Fortran source code was developed by Alex Godunov, Dept. of Physics, Old Dominion Univ. VA, USA (used here under Creative Commons License).

```
 Subroutine simpson(f,a,b,integral,n)
!============================================================
! Integration of f(x) on [a,b]
! Method: Simpson rule for n intervals
! written by: Alex Godunov (October 2009)
! checked by: Dr Melvin No, Privatdozent (July 2019)
!------------------------------------------------------------
! IN:
! f   - Function to integrate (supplied by a user)
! a   - Lower limit of integration
! b   - Upper limit of integration
! n   - number of intervals
! OUT:
```

```
! integral - Result of integration
!=============================================================
implicit none
double precision f, a, b, integral,s
double precision h, x
integer nint
integer n, i

! if n is odd we add +1 to make it even
if((n/2)*2.ne.n) n=n+1

! loop over n (number of intervals)
s = 0.0
h = (b-a)/dfloat(n)
do i=2, n-2, 2
x   = a+dfloat(i)*h
s = s + 2.0*f(x) + 4.0*f(x+h)
end do
integral = (s + f(a) + f(b) + 4.0*f(a+h))*h/3.0
return
end subroutine simpson
```

Numerical experiment

$$a = 0,\ b = \pi \ \int_a^b \sin(x)dx = -\cos(b) - (-\cos(a)) = 2$$

Results:

```
nint   Simpson
2     2.094395E+00
4     2.004560E+00
8     2.000269E+00
16    2.000017E+00
32    2.000001E+00
64    2.000000E+00
128   2.000000E+00
256   2.000000E+00
```

Introduction to Runge-Kutta method The first order differential equation to be solved is

$$y' = f(x, y) \tag{19.1}$$

with initial condition

$$y(x_0) = y_0. \tag{19.2}$$

We shall approximate $y(x + h)$ within error $\approx h^5$ by calculating

$$\begin{aligned} k_1 &= hf(x, y) \\ k_2 &= hf(x + \frac{1}{2}h, y + \frac{1}{2}k_1) \\ k_3 &= hf(x + \frac{1}{2}h, y + \frac{1}{2}k_2) \\ k_4 &= hf(x + h, y + k_3) \\ y(x + h) &= y(x) + \frac{1}{6}(k_1 + 2k_2 + 2k_3 + k_4) \end{aligned}$$

in succession.

First, we introduce the operator notation :

$$\left(h\frac{\partial}{\partial x} + k\frac{\partial}{\partial y}\right) f(x_0, y_0) = hf_x(x_0, y_0) + kf_y(x_0, y_0)$$

$$\left(h\frac{\partial}{\partial x} + k\frac{\partial}{\partial y}\right)^2 f(x_0, y_0) = h^2 f_{xx}(x_0, y_0) + 2hkf_{xy}(x_0, y_0) + k^2 f_{yy}(x_0, y_0)$$

$$\left(h\frac{\partial}{\partial x} + k\frac{\partial}{\partial y}\right)^n f(x_0, y_0) = \left(h\frac{\partial}{\partial x} + k\frac{\partial}{\partial y}\right)\left(h\frac{\partial}{\partial x} + k\frac{\partial}{\partial y}\right)^{n-1} f(x_0, y_0)$$

If partial derivatives of f of order $n + 1$ are bounded by M then

$$|R_n| \leq \frac{M}{(n+1)!}(h + k)^{n+1}.$$

With notation

$$\frac{d}{dx}y \equiv y',$$

we extrapolate $y(x)$ to $y(x+h)$ by the $4-th$ degree Taylor-polynomial

$$y(x+h) \simeq y(x) + y'(x)h + \frac{1}{2}y"(x)h^2 + \frac{1}{6}y^{(3)}h^3 + \frac{1}{24}y^{(4)}h^4 \qquad (19.3)$$

The task is to match the coefficients of the powers of h in the above single variable Taylor-expansion to the coefficients of the multivariable Taylor-expansion below, where k_1, k_2, k_3, k_4 are expressed algebraically with h, whereby the two, conceptually different Taylor-expansions become comparable. Schema is

$$h \mapsto k_1 \mapsto k_2 \mapsto k_3 \mapsto k_4.$$

Coefficients a, b, c, d as well as m, n, p are to be determined in the calculation.

$$\begin{aligned} y(x+h) &\simeq y(x) + ak_1 + bk_2 + ck_3 + dk_4 && (19.4)\\ k_1 &= hf(x,y) && (19.5)\\ k_2 &= hf(x+mh, y+mk_1) && (19.6)\\ k_3 &= hf(x+nh, y+nk_2) && (19.7)\\ k_4 &= hf(x+ph, y+pk_3) && (19.8) \end{aligned}$$

Notation

$$F_1 = f_x + ff_y, \quad F_2 = fxx + 2ff_{xy} + f^2 f_{xy}$$

$$F_3 = f_{xxx} + 3ff_{xxy} + 3f^2 f_{xyy} + f^3 f_{yyy}$$

$$\frac{d}{dx}y' = \frac{d}{dx}f(x,y) \Rightarrow y" = f_x + f_y y' = f_x + f_y f = F_1$$

$$y^{(3)} = f_{xx} + 2ff_{xy} + f^2 f_{yy} + f_y(f_x + ff_y) = F_2 + f_y F_1$$

$$y^{(4)} = f_{xxx} + 3ff_{xxy} + f^3 f_{yyy} + f_y(f_{xx} + 2ff_y + f^2 f_{yy})$$

$$+3(f_x + ff_y)(f_{xy} + f_{yy}) + f^2(f_x + ff_y)$$

$$= F_3 + f_y F_2 + 3F_1(f_{xy} + ff_{yy}) + f^2 F_1$$

$$y(x+h) \simeq f + hf + \frac{1}{2}h^2 F_1 + \frac{1}{6}h^3(F_2 + f_y F_1) +$$

$$\frac{1}{24}h^4(F_3 + f_y F_2 + 3F_1(f_{xy} + ff_{yy}) + f^2 F_1) + \ldots$$

$$y(x+h) \simeq y(x) + ak_1 + bk_2 + ck_3 + dk_4$$

Next, we expand k_1, k_2, k_3, k_4 by Taylor expansion of two variables and and replace k with expressions with h only.

$$k_1 = hf(x,y)$$

$$k_2 = h\left(f + mhF_1 + \frac{1}{2}m^2h^2F_2 + \frac{1}{6}m^2h^2F_3 + \ldots\right)$$

$$k_3 = h\left(f + nhF_1 + \frac{1}{2}h^2(n^2F_2 + 2mnf_yF_1\right)$$

$$+\frac{1}{6}h^3(n^3F_3 + 3m^2nf_yF_2 + 6mn^2(f_{xy} + ffyy)F_1 + \ldots)$$

$$k_4 = h\left(f + phF_1 + \frac{1}{2}h^2(p^2F_2 + 2npf_yF_1) + \frac{1}{6}h^3\left[p^3F_3 + 3n^2pf_yF_2 + 6mnpf_y^2F_1\right] + \ldots\right)$$

" Ach Gott! die Kunst is lang, Und kurz ist unser Leben " as Scholar Wagner would put it, so we skip some algebra:

$$y(x+h) = y(x) + (a+b+c+d)hf + (bm+cn+dp)h^2F_1 +$$

$$\frac{1}{2}(bm^2+cn^2+dp^2)h^3F_2 + \frac{1}{6}(bm^3+cn^3+dp^3)h^4F_3 + (cmn+dnp)f_yF_1$$

$$\frac{1}{2}(cm^2n+dnp^2)h^4f_yF_2 + (cmn^2+dnp^2)h^4(f_{xy}+ff_{yy})F_1 + dmpnh^4f_y^2F_1 + \ldots$$

Upon comparing the coefficients we obtain the following equations

$$a+b+c+d=1, \quad cmn+dnp=\frac{1}{6}, \quad bm+cn+dp=\frac{1}{2}, \quad cmn^2+dnp^2=\frac{1}{8},$$

$$bm^2+cn^2+dp^2=\frac{1}{3}, \quad cm^2n+dn^2p=\frac{1}{12}, \quad bm^3+cn^3+dp^3==\frac{1}{4}, \quad dmnp=\frac{1}{24}.$$

One set of solution is

$$m=n=\frac{1}{2}, \quad p=1, \quad a=d=\frac{1}{6}, \quad b=c=\frac{1}{3}$$

which is the same as the statement at the beginning of the note.

```
  subroutine RK4d11(dx,ti,xi,tf,xf)
!=================================================
! Solution of a single 1st order ODE dx/dt=f(x,t)
! Method: 4th-order Runge-Kutta method
! Alex G. February 2010
! checked by Dr Melvin No, Privatdozent, July 2019
!-------------------------------------------------
! input ...
! dx(t,x)- function dx/dt (supplied by a user)
! ti - initial time
! xi  - initial position
! tf  - time for a solution
! output ...
! xf  - solution at point tf
!=================================================
implicit none
double precision dx,ti,xi,tf,xf
double precision h,k1,k2,k3,k4

h  = tf-ti

k1 = h*dx(ti,xi)
k2 = h*dx(ti+h/2.0,xi+k1/2.0)
k3 = h*dx(ti+h/2.0,xi+k2/2.0)
k4 = h*dx(ti+h,xi+k3)

xf = xi + (k1 + 2.0*(k2+k3) + k4)/6.0

end subroutine RK4d11
```

Numerical experiment Initial value problem:

$$\frac{dx}{dt} = (-1.0) * x, \quad x(0) = 1$$

Solution $x(t) = \exp(-t)$.

```
1st order single ODE
Runge-Kutta 4th order
t         x(t)
0.00000   1.00000
0.10000   0.90484   0.90484
0.20000   0.81873   0.81873
0.30000   0.74082   0.74082
0.40000   0.67032   0.67032
0.50000   0.60653   0.60653
0.60000   0.54881   0.54881
0.70000   0.49659   0.49659
0.80000   0.44933   0.44933
0.90000   0.40657   0.40657
1.00000   0.36788   0.36788
1.10000   0.33287   0.33287
1.20000   0.30119   0.30119
1.30000   0.27253   0.27253
1.40000   0.24660   0.24660
1.50000   0.22313   0.22313
1.60000   0.20190   0.20190
1.70000   0.18268   0.18268
1.80000   0.16530   0.16530
1.90000   0.14957   0.14957
2.00000   0.13534   0.13534
```

19.3 Tutorial 12.

Summary

- Algebra
- *Spartan Old School*
- Last revision July 25, 2019

Computer Programs for Elementary Number Theory

1. Euclid's algorithm

$a = bq_1 + r_2$;

$b = r_2q_2 + r_3$;

$r_2 = r_3q_3 + r_4$;

. . . . . .

$r_{n-2} = r_{n-1}q_{n-1} + r_n$;

$r_{n-1} = r_nq_n$;

Discussion of this algorithm can be found in any good textbook.

7. The sieve of Erathosthenes
List of natural numbers less than 101.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Keep the least prime, 2, and delete all its multiples

1	2	3	∗	5	∗	7	∗	9	∗
11	∗	13	∗	15	∗	17	∗	19	∗
21	∗	23	∗	25	∗	27	∗	29	∗
31	∗	33	∗	35	∗	37	∗	39	∗
41	∗	43	∗	45	∗	47	∗	49	∗
51	∗	53	∗	55	∗	57	∗	59	∗
61	∗	63	∗	65	∗	67	∗	69	∗
71	∗	73	∗	75	∗	77	∗	79	∗
81	∗	83	∗	85	∗	87	∗	89	∗
91	∗	93	∗	95	∗	97	∗	99	∗

Keep the next prime, 3, and delete all its multiples

1	2	3	∗	5	∗	7	∗	∗	∗
11	∗	13	∗	∗	∗	17	∗	19	∗
∗	∗	23	∗	25	∗	∗	∗	29	∗
31	∗	∗	∗	35	∗	37	∗	∗	∗
41	∗	43	∗	∗	∗	47	∗	49	∗
∗	∗	53	∗	55	∗	∗	∗	59	∗
61	∗	∗	∗	65	∗	67	∗	∗	∗
71	∗	73	∗	∗	∗	77	∗	79	∗
∗	∗	83	∗	85	∗	∗	∗	89	∗
91	∗	∗	∗	95	∗	97	∗	∗	∗

Keep the next prime, 5, and delete all its multiples

1	2	3	∗	5	∗	7	∗	∗	∗
11	∗	13	∗	∗	∗	17	∗	19	∗
∗	∗	23	∗	∗	∗	∗	∗	29	∗
31	∗	∗	∗	∗	∗	37	∗	∗	∗
41	∗	43	∗	∗	∗	47	∗	49	∗
∗	∗	53	∗	∗	∗	∗	∗	59	∗
61	∗	∗	∗	∗	∗	67	∗	∗	∗
71	∗	73	∗	∗	∗	77	∗	79	∗
∗	∗	83	∗	∗	∗	∗	∗	89	∗
91	∗	∗	∗	∗	∗	97	∗	∗	∗

Keep the next prime, 7, and delete all its multiples

1	2	3	$*$	5	$*$	7	$*$	$*$	$*$
11	$*$	13	$*$	$*$	$*$	17	$*$	19	$*$
$*$	$*$	23	$*$	$*$	$*$	$*$	$*$	29	$*$
31	$*$	$*$	$*$	$*$	$*$	37	$*$	$*$	$*$
41	$*$	43	$*$	$*$	$*$	47	$*$	$*$	$*$
$*$	$*$	53	$*$	$*$	$*$	$*$	$*$	59	$*$
61	$*$	$*$	$*$	$*$	$*$	67	$*$	$*$	$*$
71	$*$	73	$*$	$*$	$*$	$*$	$*$	79	$*$
$*$	$*$	83	$*$	$*$	$*$	$*$	$*$	89	$*$
$*$	$*$	$*$	$*$	$*$	$*$	97	$*$	$*$	$*$

$\sqrt{100} = 10$;

List of primes less than 101

2	3	5	7	11
13	17	19	23	29
31	37	41	43	47
53	59	61	67	71
73	79	83	89	97

Discussion of this algorithm can be found in any good textbook.

4. Basic Fermat's factoring relies on the fact that every odd integer N can be written as a difference of two squares.

$$N = a^2 - b^2 = (a + b) * (a - b)$$

If $(a + b) = N$ and $(a - b) = 1$ then N is prime.

5. Brute Force Factoring uses odd divisors which make a superset of odd primes.

6. Calculation of highest common factor of two positive integers. Highest common factor of a and b:

```
program hcfactor
!
! demo program for calculating the highest common
! factor of two positive integers, a and b by
! the Euclidean divison algorithm
!
implicit none
integer a,b,q,r,step,flag,rold
! enter a and b
! input variable
print*, " a, b pos integers less than 10 000 000"
write(*,'(" input a: ")' , advance ='no')
read(*, '(i8)') a
write(*,'(" input b: ")' , advance ='no')
read(*, '(i8)') b
! check numbers
open (unit=6, file='hcfactor.dat')
print*, " Highest common factor of a and b:"
print*, " a =", a
print*, " b =", b
!
if (a.ge.1.and.b.ge.1) then
q=0
r=b
flag=1
step=0
else
print*, " error in step=", step
stop
endif
print*, " pass step=", step
! check for multiples
if(a == (a/b)*b) then
print*, " a is a multiple of b"
stop
```

```
endif
if(b == (b/a)*a) then
print*, " b is a multiple of a"
stop
endif
! division starts here
do while (r > 0)
step=step+1
rold=r
print*, " step=", step
call euclid(a,b,q,r,flag)
! check, redundant
if(flag.eq.-1) then
print*, "false"
STOP
endif
!
print*, a,b,q,r
!
! swap : divider by remainder
a=b
b=r
! next step
end do
! last non-zero remainder
print*, "last non-zero remainder =", rold
!
end program
!
subroutine euclid(a,b,q,r,flag)
! calculates division of a by b w/
! quotient q and remainder r
implicit none
integer a,b,q,r,flag
! check condition
if(a.ge.1.and.b.ge.1) then
flag=1
else
```

```
flag=-1
return
end if
!
q=a/b
r=mod(a,b)
!
return
end subroutine
```

Test run 1:

```
a =         504
b =         372
pass step=           0
step=           1
504         372           1         132
step=           2
372         132           2         108
step=           3
132         108           1          24
step=           4
108          24           4          12
step=           5
24          12           2           0
last non-zero remainder =          12
```

Test run 2:

```
Highest common factor of a and b:
a =        6188
b =        4709
pass step=           0
step=           1
6188        4709           1        1479
step=           2
4709        1479           3         272
step=           3
1479         272           5         119
```

```
step=           4
272         119           2          34
step=           5
119          34           3          17
step=           6
34          17          2           0
last non-zero remainder =          17
```

Test run 3:

```
Highest common factor of a and b:
a =        3989
b =        1024
pass step=           0
step=           1
3989        1024           3         917
step=           2
1024         917           1         107
step=           3
917         107           8          61
step=           4
107          61           1          46
step=           5
61          46          1          15
step=           6
46          15           3           1
step=           7
15           1          15           0
last non-zero remainder =           1
```

7. Sieve of Erathostenes on $n = 1, 2, \ldots 100$

```
program sieve
! sieve of Eratosthenes
implicit none
integer i,j, p, r, q ,n
parameter (n=100)
integer, dimension (n) :: vect
```

```
!
open (unit=6, file='sieve.dat')
! list of integers
do i=1,n
vect(i)=i
end do
! do loop running on vector
do i=2, 10
p=vect(i)

if (p==0) then
cycle
else
print*, " divisor=", p
do j= p+1,n
q=vect(j)
if(q == 0 ) then
cycle
else
r=mod(q,p)
if(r==0)  vect(j)=0
endif
end do
!
end if
print*, " end of do loop p=", p
end do
!
do i= 1, n
if(vect(i).ne.0) then
print*, vect(i)
endif
end do
end program
```

Test run :

```
divisor=           2
end of do loop p=           2
```

```
divisor=           3
end of do loop p=          3
divisor=           5
end of do loop p=          5
divisor=           7
end of do loop p=          7
1
2
3
5
7
11
13
17
19
23
29
31
37
41
43
47
53
59
61
67
71
73
79
83
89
97
```

Number 1 is on this output list, but 1 is not a prime.

8. Basic Fermat's method for Factoring.

```
program factorf
```

```
! basic fermat's method to find a factor of integer n
! if n is an odd integer, it is difference of two squares
! n= a*a - b*b = (a=b)*(a-b)
! if n is even, it has a factor 2
use iso_fortran_env
implicit none
integer(kind=int32)  a,b,m,iflag,n,b2
integer(kind=int32)  c,d, n0
print *, selected_int_kind(32)
!
WRITE(*,*)  "Basic Fermat's method for factoring n  "
READ(*,*)   n
! open files (if needed)
open (unit=6, file='factorf.dat')
!
print*, " Basic Fermat's method for factoring n "
print*, "  * n =", n
if (mod(n,2).eq.0) then
print*, "  n is even  =", n
c=2
d=n/2
print*, "  *  c =", c
print*, "  *  d =", d
STOP
endif
!
call zeno(n,m,iflag)
print*, "  * m =", m , " * m*m=", m*m
print*, "  * iflag =", iflag
!
if( iflag ==1) then
c=m
d=m
print*, "  * perfect square n =", n
print*, "  *  c =", c
print*, "  *  d =", d
STOP
endif
```

```
! start search
a=m-1
do while (iflag==-1)
a=a+1
b2=a*a-n
call zeno(b2,b,iflag)
end do
! jump out when b2 is a perfect square
print*, "  * a  =", a
print*, "  * b  =", b
c=a+b
d=a-b
print*, "  * c  =", c
print*, "  * d  =", d
! check results
n0= a*a -b*b
print*, "  * a*a-b*b  =", n0
n0=c*d
print*, "  * c*d      =", n0
end program
!
!234567890
SUBROUTINE zeno(n,m,iflag)
use iso_fortran_env
implicit none
integer(kind=int32) n,m,iflag
iflag=-1
m=1
do while ( m*m < n )
m=m+1
end do
if( m*m == n) then
iflag=1
return
end if
if( m*m > n) then
iflag=-1
return
```

```
end if
end
```

Test run 1:

```
Basic Fermat's method for factoring n
* n =        3989
* m =          64  * m*m=        4096
* iflag =          -1
* a  =        1995
* b  =        1994
* c  =        3989
* d  =           1
* a*a-b*b  =        3989
* c*d      =        3989
```

3989 is prime.

```
Test run 2:
Basic Fermat's method for factoring n
* n =        3987
* m =          64  * m*m=        4096
* iflag =          -1
* a  =         226
* b  =         217
* c  =         443
* d  =           9
* a*a-b*b  =        3987
* c*d      =        3987
```

Found two factors, $c = 443$, and $d = 9$.

8. Brute Force (Fast) Factorizing

```
PROGRAM  Factorize
! Dr C-K Shene, Michigan Techn. Univ.
! Checked by Dr Melvin No, Privatdozent, July, 2019
IMPLICIT  NONE

INTEGER(kind=selected_int_kind(15)) :: Input
```

```
INTEGER(kind=selected_int_kind(15))  :: Divisor
INTEGER(kind=selected_int_kind(15))  :: Count

WRITE(*,*)  'This program factorizes any integer >= 2 --> '
READ(*,*)   Input
! open files (if needed)
open (unit=6, file='Brute.dat')
WRITE(*,*)  'This program factorizes any integer >= 2 --> '
WRITE(*,*)  'Input =', Input
Count = 0
DO                          ! here, we try to remove all factors of 2
IF (MOD(Input,2) /= 0 .OR. Input == 1)  EXIT
Count = Count + 1       ! increase count
WRITE(*,*)  'Factor # ', Count, ': ', 2
Input = Input / 2       ! remove this factor from Input
END DO

Divisor = 3                 ! now we only worry about odd factors
DO                          ! 3, 5, 7, .... will be tried
IF (Divisor > Input) EXIT    ! if a factor is too large, exit and done
DO                        ! try this factor repeatedly
IF (MOD(Input,Divisor) /= 0 .OR. Input == 1)  EXIT
Count = Count + 1
WRITE(*,*)  'Factor # ', Count, ': ', Divisor
Input = Input / Divisor   ! remove this factor from Input
END DO
Divisor = Divisor + 2   ! move to next odd number
END DO

END PROGRAM  Factorize
```

Test run 1:

```
This program factorizes any integer >= 2 -->
Input =                 3889
Factor #                     1 :                 3889
```

Test run 2:

```
This program factorizes any integer >= 2 -->
Input =                 4096
Factor #                     1 :            2
Factor #                     2 :            2
Factor #                     3 :            2
Factor #                     4 :            2
Factor #                     5 :            2
Factor #                     6 :            2
Factor #                     7 :            2
Factor #                     8 :            2
Factor #                     9 :            2
Factor #                    10 :            2
Factor #                    11 :            2
Factor #                    12 :            2
```

Test run 3:

```
This program factorizes any integer >= 2 -->
Input =                11111
Factor #                     1 :                   41
Factor #                     2 :                  271
```