

<b>NMS Izlases nodarbības: Skaitļu teorija.</b> Sk. <a href="http://www.dudajevagatve.lv/nt/index.html">http://www.dudajevagatve.lv/nt/index.html</a>	
<b>Definīcijas:</b> Veseliem $a$ un $d$ ( $d \neq 0$ ) rakstām $d \mid a$ , ja $a$ dalās ar $d$ . Atlikumu, $a$ dalot ar $b$ , apzīmē ar $a \bmod b$ . Ja veseli skaitļi $a$ un $b$ dod vienādus atlikumus, dalot ar $m$ , raksta $a \equiv b \pmod{m}$ : $a$ un $b$ ir <i>kongruenti</i> pēc moduļa $m$ .	
<b>Aritmētikas pamatteorēma:</b> Katru $n \in \mathbb{N}$ var tieši vienā veidā izteikt kā pirmskaitļu pakāpju reizinājumu: $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ .	$2016 = 2^5 \cdot 3^2 \cdot 7$ ; <b>2017</b> = 2017 <sup>1</sup> ; 2018 = 2 <sup>1</sup> · 1009 <sup>1</sup> ; 2019 = 3 <sup>1</sup> · 673 <sup>1</sup> ; 2020 = 2 <sup>2</sup> · 5 <sup>1</sup> · 101 <sup>1</sup>
<b>Dalītāju skaits:</b> Katram $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ pozitīvo dalītāju skaits, ieskaitot 1 un $n$ , ir $d(n) = (a_1 + 1) \cdots (a_k + 1)$ .	$60 = 2^2 \cdot 3^1 \cdot 5^1$ ir $(2 + 1) \cdot (1 + 1) \cdot (1 + 1) = 12$ dalītāji.
<b>Dalītāju skaits:</b> Skaitlis $n \in \mathbb{N}$ ir pilns kvadrāts tad un tikai tad, ja tam ir nepāru skaits pozitīvu dalītāju.	Piemēri: 100 ir pilns kvadrāts, tam ir 9 dalītāji. 1000 nav pilns kvadrāts, tam ir 16 dalītāji.
<b>BW.2016.11</b> Kopa $A$ sastāv no 2016 dažādiem skaitļiem, visi šo skaitļu pirmreizinātāji ir mazāki par 30. Pierādīt, ka kopā $A$ var atrast tādus 4 dažādus skaitļus $a, b, c$ un $d$ , ka $abcd$ ir naturāla skaitļa kvadrāts.	
<b>Pirmskaitļu pārbaudes algoritms (ļoti lēns lieliem <math>n</math>)</b> isPRIME( $n$ ) 1. <b>for</b> $d = 2$ <b>to</b> $\lfloor \sqrt{n} \rfloor$ 2. <b>if</b> $n \bmod d == 0$ // $n \bmod d$ apzīmē atlikumu, $n$ dalot ar $d$ 3. <b>return</b> FALSE 4. <b>return</b> TRUE	Ja $n = 2017$ , tad $\sqrt{2017} \approx 44.91$ . Apakšējā veselā daļa ir 44. 2017 nedalās ar $2, 3, \dots, 44 \Rightarrow 2017$ ir pirmskaitlis. (Varētu nedaudz uzlabot, izlaižot pāru dalītājus $d > 2$ vai dalot tikai ar pirmskaitļiem. Bet lieliem skaitļiem izmanto <i>Miller-Rabin</i> (1980.g.) vai <i>Agrawal-Kayal-Saxena</i> (2002.g.) algoritmus.)
<b>Eiklīda algoritms LKD atrašanai:</b> EUCLID( $a, b$ ) 1. <b>if</b> $b == 0$ 2. <b>return</b> $a$ 3. <b>else return</b> EUCLID( $b, a \bmod b$ )	Funkcijas, kuras izsauc pašas sevi, bet ar citiem argumentiem, sauc par <i>rekursīvām</i> . Eiklīda algoritms ir rekursīvs. Piemēram, EUCLID(30, 21) = EUCLID(21, 9) = EUCLID(9, 3) = EUCLID(3, 0) = 3.
<b>Bezū (Bézout) lemma:</b> Ja naturālu skaitļu $a$ un $b$ lielākais kopīgais dalītājs ir $d$ , tad eksistē veseli skaitļi $x$ un $y$ , kuriem $ax + by = d$ . Visi citi skaitļi, ko var izteikt formā $ax + by$ , dalās ar $d$ .	
Ja $a$ un $b$ ir savstarpēji pirmskaitļi, tad eksistē tādi veseli $x, y$ , kam $ax + by = 1$ ; citiem vārdiem, ar $a$ un $b$ centu monētām var nomaksāt jebkuru naudas summu. “Bezū koeficientus” $x, y$ var atrast ar pielāgotu Eiklīda algoritmu. Piemērs: $a = 99$ , $b = 78$ , LKD( $a, b$ ) = 3. Meklējām $x, y$ , kam $ax + by = 3$ . $\begin{cases} 1 \cdot a + 0 \cdot b = 99 & \text{no 1.rindas} \\ 0 \cdot a + 1 \cdot b = 78 & \text{atņem 2.rindu} \end{cases} \quad \begin{cases} 1 \cdot a - 1 \cdot b = 21 & \text{no 2.rindas} \\ 0 \cdot a + 1 \cdot b = 78 & \text{atņem } 3 \times 1.\text{rindu} \end{cases} \Rightarrow \begin{cases} 1 \cdot a - 1 \cdot b = 21 \\ -3 \cdot a + 4 \cdot b = 15 \end{cases} \Rightarrow \begin{cases} 4 \cdot a - 5 \cdot b = 6 \\ -3 \cdot a + 4 \cdot b = 15 \end{cases}$ $\Rightarrow \begin{cases} 4 \cdot a - 5 \cdot b = 6 \\ -11 \cdot a + 14 \cdot b = 3 \end{cases} \quad \text{Tātad } (-11) \cdot 99 + 14 \cdot 78 = 3 \text{ jeb } x = -11, y = 14.$	
<b>LV.VO.2014.10.2</b> Atrast visas tādas vesela skaitļa $n$ vērtības, kurām gan $\frac{n^3+3}{n+3}$ , gan $\frac{n^4+4}{n+4}$ ir veseli skaitļi.	
<b>Apgalvojums par polinomu dalīšanu ar atlikumu:</b> Jebkuriem polinomiem $A(x)$ un $B(x)$ eksistē to “dalījums” $Q(x)$ un “atlikums” $R(x)$ , t.i. tādi polinomi, kam $A(x) = Q(x) \cdot B(x) + R(x)$ un $R(x)$ pakāpe ir mazāka par $B(x)$ pakāpi.	
Polinomos $A(x), B(x)$ atrod vecākos locekļus un dala tos — iegūst $Q(x)$ kārtējo locekli. Pēc tam pārveido: $\frac{n^3+3}{n+3} = \frac{n^2(n+3)-3n^2+3}{n+3} = n^2 + \frac{-3n^2+3}{n+3} = n^2 + \frac{-3n(n+3)+9n+3}{n+3} = n^2 - 3n + \frac{9n+3}{n+3} = n^2 - 3n + \frac{9(n+3)-27+3}{n+3} = n^2 - 3n + 9 + \frac{-24}{n+3}$ . Iegūstam, ka $A(n) = n^3 + 3$ un $B(n) = n + 3$ dalījums ir $Q(n) = n^2 - 3n + 9$ , bet atlikums $R(n) = -24$ . (Tā kā $B(n) = n + 3$ ir 1.pakāpes polinoms, tad $R(n)$ ir 0.pakāpes polinoms: konstante $-24$ . Iegūstam, ka $\frac{-24}{n+3}$ ir vesels jeb $n + 3$ ir kāds no skaitļa 24 dalītājiem.	
<b>BW.TST.2016.16</b> Kāda ir izteiksmes LKD( $n^2 + 3, (n + 1)^2 + 3$ ) lielākā iespējamā vērtība naturāliem $n$ ?	
Eiklīda algoritmu lieto, dalot polinomus ar atlikumu: LKD( $n^2 + 3, n^2 + 2n + 4$ ) = LKD( $n^2 + 3, 2n + 1$ ) = LKD( $2n^2 + 6, 2n + 1$ ) = LKD( $-n + 6, 2n + 1$ ) = LKD( $n - 6, 13$ ). Ja $n - 6$ dalās ar 13, tad LKD( $n^2 + 3, (n + 1)^2 + 3$ ) = 13. Citos gadījumos LKD ir 1.	
<b>Teorēma par inverso elementu:</b> Ja $p$ ir pirmskaitlis, tad katram $a \not\equiv 0 \pmod{p}$ eksistē tāds $a^{-1}$ , ka $a^{-1} \cdot a \equiv 1 \pmod{p}$	Ja $p = 7$ , tad $1^{-1} = 1, 2^{-1} = 4, 3^{-1} = 5, 4^{-1} = 2, 5^{-1} = 3, 6^{-1} = 6$ .
<b>Ķīniešu atlikumu teorēma:</b> Ja $n_1, \dots, n_k$ ir pa pāriem savstarpēji pirmskaitļi, tad jebkuriem atlikumiem $x_1, \dots, x_k$ eksistē atrisinājums $x$ , kurš dod vajadzīgos atlikumus $x_i$ , dalot ar $n_i$ . T.i. $0 \leq x < n_1 n_2 \cdots n_k$ un $x \equiv x_i \pmod{n_i}$ katram $i = 1, \dots, n$ .	Aplūkojam savstarpējus pirmskaitļus 2, 3, 5: $\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases} \Leftrightarrow x \equiv 23 \pmod{30}.$
<b>Apgalvojums par pirmskaitļu bezgalīgo skaitu.</b> Pirmskaitļu 2, 3, 5, ... ir bezgalīgi daudz. (Pierādījums no pretejā: ja būtu galīgs skaits, tad $p_1 p_2 \cdots p_k + 1$ nedalītos ne ar vienu no tiem.)	Eksistē cik patīk garas $\mathbb{N}$ apakšvirsknes bez pirmskaitļiem. (Piemēram, $m! + 2, m! + 3, m! + m$ satur $m - 1$ saliktu skaitli.)
Ir bezgalīgi daudzi tādi pirmskaitļi $p$ , kam $p \equiv 3 \pmod{4}$ . (Līdzīgi, ir bezgalīgi daudzi pirmskaitļi $p$ , kam $p \equiv 5 \pmod{6}$ )	
Pierādījums no pretejā: Ja to ir galīgs skaits, tad apzīmē visu to reizinājumu ar $P$ un aplūko $4P - 1$ . $4P - 1$ dod atlikumu 3, dalot ar 4 — tātad nevar sastāvēt tikai no pirmreizinātājiem, kas visi dod atlikumu 1, dalot ar 4.	
<b>USA.MO.2008.1</b> Pierādīt, ka jebkuram naturālam $n$ eksistē $n + 1$ savstarpēji pirmskaitļi $k_0, k_1, \dots, k_n$ , kas visi lielāki par 1 un kuriem $k_0 k_1 \cdots k_n - 1$ ir divu pēc kārtas sekojošu naturālu skaitļu reizinājums.	Ja sekojoši naturāli skaitļi ir $t, t + 1$ , vai starp $P(t) = t(t + 1) + 1$ vērtībām var būt tādas, kurām ir patvaļīgi daudz dažādu pirmreizinātāju?
<b>Definīcija:</b> Skaitļus formā $M_n = 2^n - 1$ sauc par <i>Mersena (Mersenne) skaitļiem</i> . Ja turklāt $M_n$ ir pirmskaitlis, tad to sauc par <i>Mersena pirmskaitli</i> .	
<b>Apgalvojums par Mersena pirmskaitļiem:</b> Lai $M_n = 2^n - 1$ būtu pirmskaitlis, ir nepieciešami, lai pats $n$ būtu pirmskaitlis. (Pavisam zināmi 51 Mersena pirmskaitļi. Lielākais ir $2^{82,589,933} - 1$ , ko atrada 2018.g. decembrī. Tas ir arī lielākais šobrīd zināmais pirmskaitlis.)	Ja $n$ dalās reizinātājos, tad arī pakāpju starpība $2^n - 1$ dalās reizinātājos. Piemēram, $2^{15} - 1 = (2^5)^3 - 1^3 = (2^5 - 1)((2^5)^2 + 2^5 + 1)$ . Arī, piemēram, $2^{11} - 1 = 2047 = 23 \cdot 89$ .

<p><b>Definīcija:</b> Skaitļus formā <math>F_n = 2^{2^n} + 1</math> sauc par <i>Fermā skaitļiem</i>. Ja turklāt <math>F_n</math> ir pirmskaitlis, tad to sauc par <i>Fermā pirmskaitli</i>. (Ja <math>m</math> ir kāds nepāru dalītājs <math>d &gt; 1</math>, tad <math>2^m + 1</math> nevar būt pirmskaitlis. Teiksim, <math>2^{24} + 1 = (2^8)^3 + 1^3</math> dalās reizinātajos pēc <math>a^3 + b^3 = (a+b)(a^2 - ab + b^2)</math> identitātes.)</p>	<p>Šobrīd zināmi pieci Fermā pirmskaitļi: <math>F_0 = 2^1 + 1 = 3</math>, <math>F_1 = 2^2 + 1 = 5</math>, <math>F_2 = 2^4 + 1 = 17</math>, <math>F_3 = 2^8 + 1 = 257</math>, <math>F_4 = 2^{16} + 1 = 65537</math>. Bet <math>F_5 = 2^{32} + 1 = 4,294,967,297 = 641 \cdot 6,700,417</math></p>
<p><b>Andreescu.2006.1.78</b> Dažādiem naturāliem <math>m</math> un <math>n</math>, Fermā skaitļi <math>F_m</math> un <math>F_n</math> ir savstarpēji pirmskaitļi. (Piemēram, tā kā <math>F_5</math> dalās ar 641, tad neviens cits Fermā skaitlis ar 641 nedalās.)</p>	<p>Atkārtoti lietojot kvadrātu starpības formulu <math>a^2 - b^2</math>, var pamatot, ka <math>F_m - 2</math> dalās ar <math>F_n</math>, ja <math>m &gt; n</math>. Tādēļ pēc Eiklīda algoritma. <math>\text{LKD}(F_m, F_n) = \text{LKD}((F_m - 2) + 2, F_n) = \text{LKD}(2, F_n) = 1</math>.</p>
<p><b>Mazā Fermā teorēma:</b> Ja <math>p</math> ir pirmskaitlis un <math>\text{gcd}(a, p) = 1</math>, tad <math>a^{p-1} \equiv 1 \pmod{p}</math>.</p>	<p><math>1^6 \equiv 2^6 \equiv 3^6 \equiv 4^6 \equiv 5^6 \equiv 6^6 \equiv 1 \pmod{7}</math>.</p>
<p><b>BW2016.3</b> Kuriem naturāliem <math>n = 1, \dots, 6</math> vienādojumam <math>a^n + b^n = c^n + n</math> eksistē atrisinājums veselos skaitļos?</p>	
<p><b>Teorēma par primitīvo sakni:</b> Katram pirmskaitlim <math>p</math> eksistē tāds <math>a</math>, kuram kongruenču klases <math>a^1, a^2, \dots, a^{p-1}</math> pieņem visas vērtības <math>1, 2, \dots, p-1</math>.</p>	<p>Ja <math>p = 7</math>, tad <math>3^k</math> pieņem visus iespējamus atlikumus, dalot ar 7 (izņemot pašu 7): <math>3^k \equiv 3, 2, 6, 4, 5, 1 \pmod{7}</math> ja <math>k = 1, \dots, 6</math>.</p>
<p><b>BW.2016.5</b> Dots pirmskaitlis <math>p &gt; 3</math>, kuram <math>p \equiv 3 \pmod{4}</math>. Dotam naturālam skaitlim <math>a_0</math> virkni <math>a_0, a_1, \dots</math> definē kā <math>a_n = a_{n-1}^{2^n}</math> visiem <math>n = 1, 2, \dots</math>. Pierādīt, ka <math>a_0</math> var izvēlēties tā, ka apakšvirknē <math>a_N, a_{N+1}, a_{N+2}, \dots</math> nav konstanta pēc moduļa <math>p</math> nevienam naturālam <math>N</math>.</p>	
<p><b>Definīcija:</b> Eilera funkcija <math>\varphi(n)</math> apzīmē, cik ir veselu skaitļu <math>x \in [1, n]</math>, kas ir savstarpēji pirmskaitļi ar <math>n</math>.</p>	<p>Pirmskaitļiem <math>\varphi(p) = p - 1</math>. Pirmskaitļu pakāpēm <math>\varphi(p^k) = p^k - p^{k-1}</math>.</p>
<p><b>Definīcija:</b> Funkciju <math>f(n)</math>, kas definēta naturāliem skaitļiem sauc par <i>multiplikatīvu</i>, ja jebkuriem diviem savstarpējiem pirmskaitļiem <math>a, b</math>: <math>f(ab) = f(a)f(b)</math>.</p>	<p>Eilera funkcija ir multiplikatīva. Piemēram <math>\varphi(100) = \varphi(4)\varphi(25) = (4-2)(25-5) = 2 \cdot 20 = 40</math>.</p>
<p><b>Eilera teorēma:</b> Ja <math>a</math> un <math>n</math> ir savstarpēji pirmskaitļi, tad <math>a^{\varphi(n)} \equiv 1 \pmod{n}</math>.</p>	<p>Ja <math>a</math> nedalās ar 2 un 5, tad <math>a^k</math> decimālpieraksta pēdējie divi cipari ir tādi paši kā <math>a^{k+\varphi(100)} = a^{k+40}</math>.</p>
<p><b>Apgalvojums:</b> Ja <math>q</math> nedalās ar 2 un 5, tad racionāla skaitļa <math>p/q</math> ir tīri periodiska decimāldaļa (bez priekšperioda). Eilera funkcija <math>\varphi(q)</math> dalās ar ciparu skaitu periodā.</p>	<p><math>1/41 = 0.(02439)</math>. <math>\varphi(41) = 40</math> dalās ar 5. <math>1/13 = 0.(076923)</math>. <math>\varphi(13) = 12</math> dalās ar 6. Bet <math>1/12 = 0.08(3)</math> satur priekšperiodu.</p>
<p><b>Definīcija:</b> Naturāla skaitļa <math>n</math> pozitīvo dalītāju skaitu apzīmē ar <math>d(n)</math>, pozitīvo dalītāju summu - ar <math>\sigma(n)</math>, pozitīvo dalītāju kvadrātu summu - ar <math>\sigma_2(n)</math>. <math>d(n)</math>, <math>\sigma(n)</math>, <math>\sigma_2(n)</math> ir multiplikatīvas funkcijas.</p>	<p>Ja <math>n = p_1^{a_1} p_2^{a_2}</math>, tad <math>d(n) = (a_1 + 1)(a_2 + 1)</math>, <math>\sigma(n) = (1 + p_1^1 + \dots + p_1^{a_1})(1 + p_2^1 + \dots + p_2^{a_2})</math>.</p>
<p><b>Apgalvojums:</b> <math>d(1) + d(2) + \dots + d(n) = \left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + \dots + \left\lfloor \frac{n}{n} \right\rfloor</math>. <math>\sigma(1) + \sigma(2) + \dots + \sigma(n) = 1 \cdot \left\lfloor \frac{n}{1} \right\rfloor + 2 \cdot \left\lfloor \frac{n}{2} \right\rfloor + \dots + n \cdot \left\lfloor \frac{n}{n} \right\rfloor</math>.</p>	
<p><b>Definīcija:</b> Ja <math>p</math> ir pirmskaitlis, tad par naturāla skaitļa <math>n</math> <math>p</math>-valuāciju sauc lielāko pakāpi <math>p^a</math>, ar kuru dalās <math>n</math>. Apzīmē <math>\nu_p(n) = a</math>. Skaitlim 0 valuācijas nedefinētas, tas dalās ar jebko. Grieķu burtu <math>\nu</math> lasa "nī" (angl. "nu" [nju:]).</p>	
<p><b>Ležandra (Legendre) formula:</b> Ja <math>p</math> ir pirmskaitlis, tad jebkuram naturālam <math>n</math> <math>\nu(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots</math>.</p>	<p>Augstākā pakāpe <math>5^k</math>, ar ko dalās <math>100!</math> ir <math>\lfloor 100/5 \rfloor + \lfloor 100/25 \rfloor = 24</math>. Tādēļ <math>100!</math> decimālpieraksts beidzas ar 24 nullēm.</p>
<p><b>Kummera (Ernst Kummer) teorēma:</b> Ja <math>p</math> ir pirmskaitlis un <math>n \geq m \geq 0</math>, tad <math>\nu_p(C_n^m) = \nu_p\left(\frac{n!}{m!(n-m)!}\right)</math> vienāds ar pārnese summu skaitu, stabiņā saskaitot <math>m</math> un <math>n-m</math>, pierakstīti skaitīšanas sistēmā ar bāzi <math>p</math>.</p>	<p><math>C_8^2</math> dalās ar <math>2^2</math>, bet ne ar <math>2^3</math>, jo <math>2 = 10_2</math> un <math>6 = 110_2</math> saskaitīšanā <math>10_2 + 110_2 = 1000_2</math> ir divi pārneseumi.</p>
<p><b>Kāpinātāja pacelšanas (Lifting the exponent, LTE) lemma 1:</b> Ja <math>x</math> un <math>y</math> ir veseli skaitļi (ne obligāti pozitīvi), <math>n</math> ir naturāls skaitlis un <math>p</math> ir nepāru pirmskaitlis, kuram <math>x - y</math> dalās ar <math>p</math>, bet ne <math>x</math>, ne <math>y</math> nedalās ar <math>p</math>, tad <math>\nu_p(x^n - y^n) = \nu_p(x - y) + \nu_p(n)</math>.</p>	<p><math>\nu_3(10^9 - 1^9) = \nu_3(10 - 1) + \nu_3(9) = 2 + 2 = 4</math>. Pārbaudām: <math>999999999 = 1001001 \cdot 111 \cdot 9</math>. Skaitlis <math>999999999</math> dalās ar <math>3^4</math>, bet ne ar <math>3^5</math>.</p>
<p><b>BW.2015.16</b> Ar <math>P(n)</math> apzīmējam lielāko pirmskaitli, ar ko dalās <math>n</math>. Atrast visus naturālos skaitļus <math>n \geq 2</math>, kam <math>P(n) + \lfloor \sqrt{n} \rfloor = P(n+1) + \lfloor \sqrt{n+1} \rfloor</math>.</p>	
<p><b>LTE lemma 2:</b> Ja <math>x</math> un <math>y</math> ir veseli skaitļi (ne obligāti pozitīvi), <math>n</math> ir nepāru naturāls skaitlis un <math>p</math> ir nepāru pirmskaitlis tāds, ka <math>p \mid x+y</math>, bet ne <math>x</math> ne <math>y</math> nedalās ar <math>p</math>, tad <math>\nu_p(x^n + y^n) = \nu_p(x + y) + \nu_p(n)</math>.</p>	<p><math>\nu_{11}(10^{121} + 1) = \nu_{11}(10 + 1) + \nu_{11}(121) = 1 + 2 = 3</math>. Skaitlis <math>1 \underbrace{0 \dots 0}_{120} 1</math> dalās ar <math>11^3</math>, bet ne ar <math>11^4</math>.</p>
<p><b>LTE lemma 3:</b> Ja <math>x</math> un <math>y</math> ir nepāru skaitļi, kam <math>x - y</math> dalās ar 4, tad <math>\nu_2(x^n - y^n) = \nu_2(x - y) + \nu_2(n)</math>.</p>	<p><math>\nu_2(5^{128} - 1) = 2 + 7 = 9</math></p>
<p><b>LV.TST.1993.2</b> Dots naturāls skaitlis <math>a &gt; 2</math>. Pierādīt, ka eksistē tikai galīgs skaits tādu naturālu <math>n</math>, ka <math>a^n - 1</math> dalās ar <math>2^n</math>.</p>	
<p><b>BW2015.17</b> Atrast visus naturālos skaitļus <math>n</math>, kuriem <math>n^{n-1} - 1</math> dalās ar <math>2^{2015}</math>, bet nedalās ar <math>2^{2016}</math>.</p>	
<p><b>LTE lemma 4:</b> Ja <math>x</math> un <math>y</math> ir divi nepāru veseli skaitļi un <math>m</math> ir pāru naturāls skaitlis. Tādā gadījumā: <math>\nu_2(x^m - y^m) = \nu_2(x - y) + \nu_2(x + y) + \nu_2(m) - 1</math>.</p>	<p><math>\nu_2(3^{16} - 1) = 1 + 2 + 4 - 1 = 6</math>.</p>
<p><b>LV.TST.1979.10.2</b> Pierādīt, ka eksistē tāds naturāls skaitlis <math>n</math>, ka <math>n^2 + 1</math> dalās ar <math>5^{1979}</math>.</p>	
<p><b>Henzela (Hensel) lemma:</b> Ja polinomam <math>P(x)</math> ir vienkārša sakne pēc kāda pirmskaitļa moduļa <math>p</math>, tad <math>P(x)</math> būs vienkārša sakne arī pēc jebkuras šī pirmskaitļa pakāpes <math>p^k</math>, kuru var iegūt, pakāpeniski "paceļot" pakāpi. (<math>P(x)</math> ir vienkārša sakne <math>x_0</math> pēc moduļa <math>p</math>, ja <math>P(x_0) \equiv 0 \pmod{p}</math>, bet polinoma atvasinājuma vērtība <math>P'(x_0)</math> ar <math>p</math> vairs nedalās.)</p>	