

Skaitļu teorijas formulu lapa (NMS)			
Algebriski pārveidojumi.			
$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4.$	Binomiālie koeficienti: $(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \dots + \binom{n}{n-1}ab^{n-1} + b^n$, kur $\binom{n}{k} = C_n^k = \frac{n!}{k!(n-k)!}.$	$(a+b+c+d)^4 = \dots + 12a^2bc + \dots$, jo $\frac{4!}{2!1!1!} = 12.$	Polinomiālie koeficienti: $(a_1+a_2+\dots+a_m)^n$ izvirzījums satur $a_1^{k_1}a_2^{k_2}\dots a_m^{k_m}$ ar koeficientu $\frac{n!}{k_1!k_2!\dots k_m!}$, ja $k_1+k_2+\dots+k_m = n$.
$a^3+b^3 = (a+b)(a^2-ab+b^2).$	Nepāru pakāpju summa: $a^{2n+1}+b^{2n+1} = (a+b)(a^{2n}-a^{2n-1}b+\dots-ab^{2n-1}+b^{2n}).$	$a^3-b^3 = (a-b)(a^2+ab+b^2).$	Pakāpju starpība: $a^n-b^n = (a-b)(a^{n-1}+a^{n-2}b+\dots+ab^{n-2}+b^{n-1}).$
$ax^2+bx+c=0$ ir 3 saknes $\Rightarrow a=b=c=0$	Identiski polinomi: Ja $P(x)$ un $Q(x)$ ir n -tās pakāpes polinomi un to vērtības sakrīt $n+1$ dažādiem x_i , tad $P(x)=Q(x).$	$P(x)=4x^3-3x^2-25x-6$ dalās ar $(x-3).$	Polinoms $P(x)$ dalās ar $(x-a)$ tad un tikai tad, ja a ir $P(x)$ sakne.
$x^4+4=(x^2-2x+2)\cdot(x^2+2x+2)$	Sofijas-Žermēnas identitāte: $a^4+4b^4=((a+b)^2+b^2)\cdot((a-b)^2+b^2)$	3 kubu identitāte: $a^3+b^3+c^3-3abc=(a+b+c)(a^2+b^2+c^2-ab-bc-ca).$ Sekas: $(x-y)^3+(y-z)^3+(z-x)^3=3(x-y)(y-z)(z-x).$	
Dalāmība un pirmskaitļi: Veseliem a un d ($d \neq 0$) rakstām $d \mid a$, ja a dalās ar d . Atlikums, a dalot ar b : $(a \bmod b).$			
Pirmskaitļu 2, 3, 5, ... ir bezgalīgi daudz. (No pretejā: ja būtu galīgs skaits, tad $p_1p_2\cdots p_k+1$ nedalītos ne ar vienu no tiem.)		Eksistē cik patīk garas N apakšvirknes bez pirmskaitļiem. (Piemēram, $m!+2, m!+3, m!+m$ satur $m-1$ saliktu skaitli.)	
2016 = $2^53^27.$ 2017 = $2017^1.$ 2018 = $2\cdot 1009.$	Aritmētikas pamatteorēma: Katru $n \in \mathbb{N}$ var tieši vienā veidā izteikt kā pirmskaitļu pakāpju reizinājumu: $n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}.$	$60 = 2^2 \cdot 3^1 \cdot 5^1$ ir $3 \cdot 2 \cdot 2 = 12$ dalītāji.	Dalītāju skaits: Katram $n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ pozitīvo dalītāju skaits, ieskaitot 1 un n , ir $d(n) = (a_1+1)\cdots(a_k+1).$
$d(100)=9;$ $d(1000)=16.$	Dalītāju skaita teorēma: $n \in \mathbb{N}$ ir pilns kvadrāts t.t.t., ja tam ir nepāru skaits pozitīvu dalītāju (visi pirmreizinātāji ir pāru pakāpēs).	$n=12$: (1, 12), (2, 6) un (3, 4).	Dalītāju pāri: Visus n dalītājus (izņemot \sqrt{n}) var grupēt pāros: $d_1 < \sqrt{n} < d_2$, kur $d_2 = n/d_1.$
$\gcd(192, 78) = \gcd(78, 36) = \gcd(36, 6) = \gcd(6, 0) = 6.$	Eiklīda algoritms: function gcd(a, b) if (b == 0) { return a; } else { return gcd(b, a mod b); }	Piemērs polinomiem: $\gcd(n^2+3, n^2+2n+4) = \gcd(n^2+3, 2n+1) = \gcd(2n^2+6, 2n+1) = \gcd(-n+6, 2n+1) = \gcd(n-6, 13).$	
$a=8, b=13 \Rightarrow 5a-3b=1.$	Bezū lemma: Ja $a, b \in \mathbb{N}$ un $d = \gcd(a, b)$, tad eksistē $x, y \in \mathbb{Z}$, kam $ax+by=d.$ Eiklīda lemma: Dots pirmskaitlis p un $a, b \in \mathbb{Z}$. Ja $p \mid ab$, tad $p \mid a$ vai $p \mid b.$	$(n_1, n_2, n_3) = (2, 3, 5),$ $(x_1, x_2, x_3) = (1, 2, 3) \Rightarrow x \equiv 23 \pmod{30}.$	Ķīniešu atlikumu teorēma: Ja n_1, \dots, n_k ir naturāli skaitļi, $\gcd(n_i, n_j) = 1$ visiem $i \neq j$, tad visiem naturāliem x_1, \dots, x_k eksistē tieši viena kongruenču klase x pēc moduļa $n = n_1 \cdots n_k$, kam $x \equiv x_i \pmod{n_i}$ visiem $i.$
Kongruences: Veseliem a, b, m rakstām $a \equiv b \pmod{m}$, ja $a-b$ dalās ar $m.$			
Intuīcija: Ja skaitli a , kas nedalās ar p , pietiekami ilgi reizina pašu ar sevi, iegūst atlikumu 1 (mod p).	Intuīcija: Skaitli a , kam nav kopīgu dalītāju ar nepirmskaitli n , reizinot pašu ar sevi, arī kaut kad iegūst atlikumu 1 (mod n).		
$1^6 \equiv 2^6 \equiv 3^6 \equiv 4^6 \equiv 5^6 \equiv 6^6 \equiv 1 \pmod{7}.$	Mazā Fermā teorēma: Ja p ir pirmskaitlis un $\gcd(a, p) = 1$, tad $a^{p-1} \equiv 1 \pmod{p}.$	$1^4 \equiv 3^4 \equiv 7^4 \equiv 9^4 \equiv 1 \pmod{10}$	Eilera teorēma: Katram naturālam n un katram a , kam $\gcd(a, n) = 1$ izpildās $a^{\varphi(n)} \equiv 1 \pmod{n}.$
Valuācijas un pakāpes pacelšanas lemmas:			
Intuīcija: $x^n \pm y^n$ dalāmība ar nepāra pirmskaitļu pakāpēm ir precīzi atrodama (ar indukciju).	Intuīcija: $x^n \pm y^n$ dalāmība ar divnieka pakāpēm ir precīzi atrodama, bet citāda.		
$\nu_3(999999999) = \nu_3(10^9 - 1^9) = \nu_3(10 - 1) + \nu_3(9) = 2 + 2 = 4.$	Lemma 1: Ja x un y ir veseli skaitļi (ne obligāti pozitīvi), n ir naturāls skaitlis un p ir nepāru pirmskaitlis. Zināms, ka $x \not\equiv 0 \pmod{p}$, $y \not\equiv 0 \pmod{p}$, bet $x-y \equiv 0 \pmod{p}.$ Tad $\nu_p(x^n - y^n) = \nu_p(x-y) + \nu_p(n).$ Der arī negatīvi x vai $y.$ Piemēram, $\nu_{11}(10^{121} + 1) = \nu_{11}(10 + 1) + \nu_{11}(121) = 3.$	$\nu_2(5^{128} - 1) = \nu_2(5 - 1) + \nu_2(5 + 1) + \nu_2(128) - 1 = 9.$	Lemma 2: Ja x un y ir divi nepāru veseli skaitļi un n ir pāru naturāls skaitlis. Tādā gadījumā: $\nu_2(x^n - y^n) = \nu_2(x-y) + \nu_2(x+y) + \nu_2(n) - 1.$
Skaitļi ar neparastām īpašībām: Fermā skaitļi, Mersena skaitļi, Viferiha skaitļi, Karmaikla skaitļi.			
$F_{0,\dots,4} = 3, 5, 17, 257, 65537.$	Ja 2^n+1 ir pirmskaitlis, tad n jābūt $2^k.$ Skaitļus $F_n = 2^{2^k}+1$ sauc par Fermā (<i>Fermat</i>) skaitļiem; pirmie pieci no tiem ir pirmskaitļi (nav zināms, vai ir vēl kāds pirmskaitlis $F_k, k > 4$).	$W_1 = 1093,$ $W_2 = 3511.$	Par Viferiha (<i>Wieferich</i>) pirmskaitļiem sauc pirmskaitļus p , kam 2^{p-1} dalās ne vien ar p (Mazā Fermā teorēma), bet uzreiz ar $p^2.$ Šobrīd zināmi tikai divi Viferiha pirmskaitļi.
$M_{2,3,5,7,13} = 3, 7, 31, 127, 8191$	Ja $M_p = 2^p - 1$ ir pirmskaitlis, tad p jābūt pirmskaitlim. Pirmskaitļus šajā formā sauc par Mersena pirmskaitļiem. Bet $2^{11} = 2047 = 23 \cdot 89$, t.i. visi M_p nav pirmskaitļi.	$561 = 3 \cdot 11 \cdot 17$	Par Karmaikla (<i>Carmichael</i>) skaitļiem sauc saliktus skaitļus n , kas apmierina Fermā teorēmai līdzīgu apgalvojumu: Visiem b , kam nav kopīgu dalītāju ar n : $b^{n-1} \equiv 1 \pmod{n}.$ 561 der, jo $(3-1) \mid 560, (10-1) \mid 560$, and $16 \mid 560$ (Korselta kritērijs).
Multiplikatīvā kārtā un primitīvās saknes: Var vienošķinīgi pateikt, kuriem kāpinātājiem k izpildās $a^k \equiv 1 \pmod{p}.$			
Intuīcija: Katram atlikumam a (ja $a \not\equiv 0 \pmod{p}$) var atrast vismazāko kāpinātāju, kuram a^k "ieciņklojas" un atgriežas pie vērtības 1 (mod p).	Intuīcija: Eksistē skaitļi a , kuri izstaigā visas kongruenču klases (izņemot 0 (mod p)), pirms atgriežas pie 1 (mod p).		
$\text{ord}_7(1) = 1,$ $\text{ord}_7(3) = \text{ord}_7(5) = 6,$ $\text{ord}_7(2) = \text{ord}_7(4) = 3,$ $\text{ord}_7(6) = 2.$	Definīcija: Par skaitļa a multiplikatīvo kārtu (<i>multiplicative order</i>) pēc p moduļa sauc mazāko kāpinātāju k , kuram $a^k \equiv 1 \pmod{p}.$ Multiplikatīvo kārtu apzīmē $\text{ord}_p(a).$	$3^k \equiv 3, 2, 6, 4, 5, 1 \pmod{7}$ ja $k = 1, \dots, 6.$ Arī 5 ir primitīvā sakne (mod 7).	Primitīvā sakne: Katram pirmskaitlim p eksistē tāds a , kuram kongruenču klases a^1, a^2, \dots, a^{p-1} pieņem visas vērtības $1, 2, \dots, p-1$ (sajauktā secībā).

Intuīcija: Dažām $a \not\equiv 0$ vērtībām vienādojumu $x^2 \equiv a \pmod{p}$ var atrisināt (un tad tam ir tieši divas saknes x_1, x_2 , kam $x_2 \equiv -x_1$); citām a vērtībām šim “kongruenču kvadrātvienādojumam” nav nevienas saknes. (Ja $a \equiv 0$, tad ir tieši viena sakne $x \equiv 0$.)	
Definīcija: Skaitli $a \not\equiv 0$ sauc par kvadrātisko atlikumu (<i>quadratic residue</i>), ja kongruenču vienādojumu $x^2 \equiv a \pmod{p}$ var atrisināt. Definīciju sk. https://bit.ly/3sFNqsh	Pirmskaitlim $p = 7$ skaitļi $a = 1, 2, 4$ ir kvadrātiskie atlikumi, bet $a = 3, 5, 6$ nav kvadrātiskie atlikumi.

Intuīcija: No visiem atlikumiem (izņemot atlikumu 0) būs tieši puse tādu, kuri atgriežas pie 1 (mod p) jau divreiz ātrāk nekā pēc $p - 1$ soļiem.	
Definīcija: Par skaitļa a Ležandra simbolu (<i>Legendre symbol</i>) pēc p moduļa sauc lielumu $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$. Teorēma (Eilera kritērijs): Skaitlis a ir kvadrātisks atlikums tad un tikai tad, ja $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Secinājums: Ja $\left(\frac{a}{p}\right) = 1$, tad vienādojumu $x^2 \equiv a \pmod{p}$ var atrisināt, bet ja $\left(\frac{a}{p}\right) = -1$, tad nevar atrisināt. Definīciju un vērtību tabulu sk. https://bit.ly/3qFKH0m .	$\left(\frac{0}{7}\right) = 0.$ $\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1.$ $\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1.$

a	1	2	3	4	5	6
$a^2 \pmod{7}$	1	4	2	2	4	1
$a^3 \pmod{7}$	1	1	6	1	6	6
$a^4 \pmod{7}$	1	2	4	4	2	1
$a^5 \pmod{7}$	1	4	5	2	3	6
$a^6 \pmod{7}$	1	1	1	1	1	1
$\text{ord}_7(a)$	1	3	6	3	6	2
$\left(\frac{a}{7}\right)$	1	1	-1	1	-1	-1

- Ležandra simbols $\left(\frac{a}{7}\right)$ ir atkarīgs no šīs pakāpju tabulas vidējās jeb 3.rindas (sarkana), kas atbilst kāpinātājam $\frac{p-1}{2} = 3$.
- Pēdējā, 6.rindā visas pakāpes a^6 atgriežas pie vērtības 1 (Mazā Fermā teorēma (zila)).
- Katrā vertikālē var noskaidrot mazāko k , kuram a^k ir kongruents 1 (tā ir multiplikatīvā kārtā).
- Pirmskaitļa $p = 7$ primitīvās saknes $a = 3$ un $a = 5$ nevar būt kvadrātiskie atlikumi. Arī $a = 6$ nevar būt kvadrātiskais atlikums, jo šī skaitļa pakāpes veic nepāra skaitu ciklu (tieši trīs ciklus) līdzkamēr tiek līdz a^6 . Bet kvadrātiskajam atlikumam (piemēram $a = 1, a = 2$, vai $a = 4$) savā stabiņā jāveic pāra skaits ciklu: $(p-1)/\text{ord}_p(a)$ jābūt pāru skaitlim.

Intuīcija: No Ležandra simbola definīcijas (tā ir skaitļa a pakāpe) seko vairākas vienkāršas īpašības:	
Apgalvojums #3: Ja $a \equiv b \pmod{p}$, tad $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, jeb Ležandra simbols ir periodisks ar periodu p (vienāds kongruentiem a, b). Apgalvojums #4: $\left(\frac{-1}{p}\right) = 1$ tad un tikai tad, ja $p = 4k + 1$. Apgalvojums #5: $\left(\frac{2}{p}\right) = 1$ tad un tikai tad, ja $p = 8k + 1$ vai $p = 8k + 7$. Apgalvojums #6: $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.	Kongruenci $x^2 + 1 \equiv 0 \pmod{p}$ var atrisināt pirmskaitļiem $p = 5, 13, 17, 29, \dots$, bet nevar atrisināt pirmskaitļiem $p = 3, 7, 11, 19, 23, \dots$, jo tiem $\left(\frac{-1}{p}\right) = -1$.