NMS Izlases nodarbības: Skaitļu teorija. Sk. `http://www.dudajevagatve.lv/nt/index.html`

Definīcijas: 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 *kongruenti* pēc moduļa m.

Aritmētikas pamatteorēma: Katru $n \in \mathbb{N}$ var tieši vienā veidā izteikt kā pirmskaitļu pakāpju reizinājumu: $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$.

$2016 = 2^5 \cdot 3^2 \cdot 7$; $\mathbf{2017} = 2017^1$; $2018 = 2^1 \cdot 1009^1$; $2019 = 3^1 \cdot 673^1$; $2020 = 2^2 \cdot 5^1 \cdot 101^1$

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 $d(n) = (a_1+1) \cdots (a_k+1)$.

$60 = 2^2 \cdot 3^1 \cdot 5^1$ ir $(2+1)\cdot(1+1)\cdot(1+1) = 12$ dalītāji.

Dalītāju skaits: 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.

BW.2016.11 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.

Pirmskaitļu pārbaudes algoritms (ļoti lēns lieliem n)

```
isPrime(n)
    for d = 2 to ⌊√n⌋
        if n mod d == 0    // n mod d apzīmē atlikumu, n dalot ar d
            return FALSE
    return TRUE
```

Ja $n = 2017$, tad $\sqrt{2017} \approx 44.91$. Apakšējā veselā daļa ir 44. 2017 nedalās ar $2, 3, \ldots, 44 \Rightarrow 2017$ ir pirmskaitlis. (Varētu nedaudz uzlabot, izlaižot pāru dalītājus $d > 2$ vai dalot tikai ar pirmskaitļiem. Bet lieliem skaitļiem izmanto *Miller-Rabin* (1980.g.) vai *Agrawal–Kayal–Saxena* (2002.g.) algoritmus.)

Eiklīda algoritms LKD atrašanai:

```
Euclid(a, b)
    if b == 0
        return a
    else return Euclid(b, a mod b)
```

Funkcijas, kuras izsauc pašas sevi, bet ar citiem argumentiem, sauc par *rekursīvām.* Eiklīda algoritms ir rekursīvs. Piemēram, $\text{Euclid}(30,21) = \text{Euclid}(21,9) = \text{Euclid}(9,3) = \text{Euclid}(3,0) = 3$.

Bezū (Bézout) lemma: 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: $a = 99$, $b = 78$, $\text{LKD}(a,b) = 3$. Meklējam x, y, kam $ax + by = 3$.

$$\begin{cases} 1\cdot a + 0 \cdot b = 99 & \textit{no 1.rindas} \\ 0 \cdot a + 1 \cdot b = 78 & \textit{atņem 2.rindu} \end{cases} \begin{cases} 1\cdot a - 1 \cdot b = 21 & \textit{no 2.rindas} \\ 0 \cdot a + 1 \cdot b = 78 & \textit{atņem } 3\times\textit{1.rindu} \end{cases} \begin{cases} 1\cdot a - 1 \cdot b = 21 \\ -3 \cdot a + 4 \cdot b = 15 \end{cases} \Rightarrow \begin{cases} 4\cdot a - 5 \cdot b = 6 \\ -3 \cdot a + 4 \cdot b = 15 \end{cases}$$

$$\Rightarrow \begin{cases} 4\cdot a - 5 \cdot b = 6 \\ -11 \cdot a + 14 \cdot b = 3 \end{cases}$$ Tātad $(-11)\cdot 99 + 14 \cdot 78 = 3$ jeb $x = -11$, $y = 14$.

LV.VO.2014.10.2 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.

Apgalvojums par polinomu dalīšanu ar atlikumu: 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.

BW.TST.2016.16 Kāda ir izteiksmes $\text{LKD}\left(n^2+3, (n+1)^2+3\right)$ lielākā iespējamā vērtība naturāliem n?

Eiklīda algoritmu lieto, dalot polinomus ar atlikumu: $\text{LKD}\left(n^2+3, n^2+2n+4\right) = \text{LKD}\left(n^2+3, 2n+1\right) = \text{LKD}\left(2n^2+6, 2n+1\right) = \text{LKD}\left(-n+6, 2n+1\right) = \text{LKD}\left(n-6, 13\right)$. Ja $n-6$ dalās ar 13, tad $\text{LKD}\left(n^2+3, (n+1)^2+3\right) = 13$. Citos gadījumos LKD ir 1.

Teorēma par inverso elementu: 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 $1^{-1} = 1$, $2^{-1} = 4$, $3^{-1} = 5$, $4^{-1} = 2$, $5^{-1} = 3$, $6^{-1} = 6$.

Ķīniešu atlikumu teorēma: Ja $n_1, \ldots, n_k$ ir pa pāriem savstarpēji pirmskaitļi, tad jebkuriem atlikumiem $x_1, \ldots, x_k$ 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 $i = 1, \ldots, n$.

Aplūkojam savstarpējus pirmskaitļus $2, 3, 5$:

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases} \Leftrightarrow x \equiv 23 \pmod{30}.$$

Apgalvojums par pirmskaitļu bezgalīgo skaitu. Pirmskaitļu $2, 3, 5, \ldots$ ir bezgalīgi daudz. (Pierādījums no pretējā: ja būtu galīgs skaits, tad $p_1 p_2 \cdots p_k + 1$ nedalītos ne ar vienu no tiem.)

Eksistē cik patīk garas $\mathbb{N}$ apakšvirknes 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 pretējā: 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.

USA.MO.2008.1 Pierādīt, ka jebkuram naturālam n eksistē $n + 1$ savstarpēji pirmskaitļi $k_0, k_1, \ldots, k_n$, kas visi lielāli 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?

Definīcija: Skaitļus formā $M_n = 2^n - 1$ sauc par *Mersena (Mersenne) skaitļiem.* Ja turklāt M_n ir pirmskaitlis, tad to sauc par *Mersena pirmskaitli.*

Apgalvojums par Mersena pirmskaitļiem: 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, $2^{11} - 1 = 2047 = 23 \cdot 89$.

Definīcija: Skaitļus formā $F_n = 2^{2^n} + 1$ sauc par *Fermā skaitļiem.* Ja turklāt F_n ir pirmskaitlis, tad to sauc par *Fermā pirmskaitli.* (*Ja m ir kāds nepāru dalītājs $d > 1$, tad $2^m + 1$ nevar būt pirmskaitlis. Teiksim, $2^{24} + 1 = (2^8)^3 + 1^3$ dalās reizinātājos pēc $a^3 + b^3 = (a+b)(a^2 - ab + b^2)$ identitātes.*)	Šobrīd zināmi pieci Fermā pirmskaitļi: $F_0 = 2^1 + 1 = 3$, $F_1 = 2^2 + 1 = 5$, $F_2 = 2^4 + 1 = 17$, $F_3 = 2^8 + 1 = 257$, $F_4 = 2^{16} + 1 = 65537$. Bet $F_5 = 2^{32} + 1 = 4,294,967,297 = 641 \cdot 6,700,417$
Andreescu.2006.1.78 Dažādiem naturāliem m un n, Fermā skaitļi F_m un F_n ir savstarpēji pirsmkaitļi. (*Piemēram, tā kā F_5 dalās ar 641, tad neviens cits Fermā skaitlis ar 641 nedalās.*)	Atkārtoti lietojot kvadrātu starpības formulu $a^2 - b^2$, var pamatot, ka $F_m - 2$ dalās ar F_n, ja $m > n$. Tādēļ pēc Eiklīda algoritma. $\text{LKD}(F_m, F_n) = \text{LKD}((F_m - 2) + 2, F_n) = \text{LKD}(2, F_n) = 1$.
Mazā Fermā teorēma: Ja p ir pirmskaitlis un $\gcd(a,p) = 1$, tad $a^{p-1} \equiv 1 \pmod{p}$.	$1^6 \equiv 2^6 \equiv 3^6 \equiv 4^6 \equiv 5^6 \equiv 6^6 \equiv 1 \pmod{7}$.
BW2016.3 Kuriem naturāliem $n = 1, \ldots 6$ vienādojumam $a^n + b^n = c^n + n$ eksistē atrisinājums veselos skaitļos?	
Teorēma par primitīvo sakni: Katram pirmskaitlim p eksistē tāds a, kuram kongruenču klases $a^1, a^2, \ldots, a^{p-1}$ pieņem visas vērtības $1, 2, \ldots, p-1$.	Ja $p = 7$, tad 3^k pieņem visus iespējamos atlikumus, dalot ar 7 (izņemot pašu 7): $3^k \equiv 3,\ 2,\ 6,\ 4,\ 5,\ 1 \pmod{7}$ ja $k = 1, \ldots, 6$.
BW.2016.5 Dots pirmskaitlis $p > 3$, kuram $p \equiv 3 \pmod{4}$. Dotam naturālam skaitlim a_0 virkni $a_0, a_1, \ldots$ definē kā $a_n = a_{n-1}^{2^n}$ visiem $n = 1, 2, \ldots$. Pierādīt, ka a_0 var izvēlēties tā, ka apakšvirkne $a_N, a_{N+1}, a_{N+2}, \ldots$ nav konstanta pēc moduļa p nevienam naturālam N.	
Definīcija: *Eilera funkcija* $\varphi(n)$ apzīmē, cik ir veselu skaitļu $x \in [1, n]$, kas ir savstarpēji pirmskaitļi ar n.	Pirmskaitļiem $\varphi(p) = p - 1$. Pirmskaitļu pakāpēm $\varphi(p^k) = p^k - p^{k-1}$.
Definīcija: Funkciju $f(n)$, kas definēta naturāliem skaitļiem sauc par *multiplikatīvu*, ja jebkuriem diviem savstarpējiem pirmskaitļiem a, b: $f(ab) = f(a)f(b)$.	Eilera funkcija ir multiplikatīva. Piemēram $\varphi(100) = \varphi(4)\varphi(25) = (4-2)(25-5) = 2 \cdot 20 = 40$.
Eilera teorēma: Ja a un n ir savstarpēji pirmskaitļi, tad $a^{\varphi(n)} \equiv 1 \pmod{n}$.	Ja a nedalās ar 2 un 5, tad a^k decimālpieraksta pēdējie divi cipari ir tādi paši kā $a^{k+\varphi(100)} = a^{k+40}$.
Apgalvojums: Ja q nedalās ar 2 un 5, tad racionāla skaitļa p/q ir tīri periodiska decimāldaļa (bez priekšperioda). Eilera funkcija $\varphi(q)$ dalās ar ciparu skaitu periodā.	$1/41 = 0.(02439)$. $\varphi(41) = 40$ dalās ar 5. $1/13 = 0.(076923)$. $\varphi(13) = 12$ dalās ar 6. Bet $1/12 = 0.08(3)$ satur priekšperiodu.
Definīcija: Naturāla skaitļa n pozitīvo dalītāju skaitu apzīmē ar $d(n)$, pozitīvo dalītāju summu - ar $\sigma(n)$, pozitīvo dalītāju kvadrātu summu - ar $\sigma_2(n)$. $d(n)$, $\sigma(n)$, $\sigma_2(n)$ ir multiplikatīvas funkcijas.	Ja $n = p_1^{a_1} p_2^{a_2}$, tad $d(n) = (a_1 + 1)(a_2 + 1)$, $\sigma(n) = \left(1 + p_1^1 + \cdots + p_1^{a_1}\right)\left(1 + p_2^1 + \cdots + p_2^{a_2}\right)$.
Apgalvojums: $d(1) + d(2) + \cdots + d(n) = \left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + \cdots + \left\lfloor \frac{n}{n} \right\rfloor$. $\sigma(1) + \sigma(2) + \cdots + \sigma(n) = 1 \cdot \left\lfloor \frac{n}{1} \right\rfloor + 2 \cdot \left\lfloor \frac{n}{2} \right\rfloor + \cdots + n \cdot \left\lfloor \frac{n}{n} \right\rfloor$.	
Definīcija: Ja p ir pirmskaitlis, tad par naturāla skaitļa n p-valuāciju sauc lielāko pakāpi p^a, ar kuru dalās n. Apzīmē $\nu_p(n) = a$. Skaitlim 0 valuācijas nedefinētas, tas dalās ar jebko. Grieķu burtu ν lasa "nī" (angl. "nu" [nju:]).	
Ležandra (Legendre) formula: Ja p ir pirmskaitlis, tad jebkuram naturālam n $\nu(n!) = \left\lfloor \frac{n}{p^1} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$.	Augstākā pakāpe 5^k, ar ko dalās 100! ir $\lfloor 100/5 \rfloor + \lfloor 100/25 \rfloor = 24$. Tādēļ 100! decimālpieraksts beidzas ar 24 nullēm.
Kummera (Ernst Kummer) teorēma: Ja p ir pirmskaitlis un $n \geq m \geq 0$, tad $\nu_p\left(C_n^m\right) = \nu_p\left(\frac{n!}{m!(n-m)!}\right)$ vienāds ar pārnesumu skaitu, stabiņā saskaitot m un $n - m$, pierakstīti skaitīšanas sistēmā ar bāzi p.	C_8^2 dalās ar 2^2, bet ne ar 2^3, jo $2 = 10_2$ un $6 = 110_2$ saskaitīšanā $10_2 + 110_2 = 1000_2$ ir divi pārnesumi.
Kāpinātāja pacelšanas (Lifting the exponent, LTE) lemma 1: Ja x un y ir veseli skaitļi (ne obligāti pozitīvi), n ir naturāls skaitlis un p ir nepāru pirmskaitlis, kuram $x - y$ dalās ar p, bet ne x, ne y nedalās ar p, tad $\nu_p\left(x^n - y^n\right) = \nu_p(x - y) + \nu_p(n)$.	$\nu_3(10^9 - 1^9) = \nu_3(10 - 1) + \nu_3(9) = 2 + 2 = 4$. Pārbaudām: $999999999 = 1001001 \cdot 111 \cdot 9$. Skaitlis 999999999 dalās ar 3^4, bet ne ar 3^5.
BW.2015.16 Ar $P(n)$ apzīmējam lielāko pirmskaitli, ar ko dalās n. Atrast visus naturālos skaitļus $n \geq 2$, kam $P(n) + \lfloor \sqrt{n} \rfloor = P(n+1) + \lfloor \sqrt{n+1} \rfloor$.	
LTE lemma 2: Ja x un y ir veseli skaitļi (ne obligāti pozitīvi), n ir nepāru naturāls skaitlis un p ir nepāru pirmskaitlis tāds, ka $p \mid x + y$, bet ne x ne y nedalās ar p, tad $\nu_p\left(x^n + y^n\right) = \nu_p(x + y) + \nu_p(n)$.	$\nu_{11}(10^{121} + 1) = \nu_{11}(10 + 1) + \nu_{11}(121) = 1 + 2 = 3$. Skaitlis $1\underbrace{0\ldots0}_{120}1$ dalās ar 11^3, bet ne ar 11^4.
LTE lemma 3: Ja x un y ir nepāru skaitļi, kam $x - y$ dalās ar 4, tad $\nu_2(x^n - y^n) = \nu(x-y) + \nu_2(n)$.	$\nu_2(5^{128} - 1) = 2 + 7 = 9$
LV.TST.1993.2 Dots naturāls skaitlis $a > 2$. Pierādīt, ka eksistē tikai galīgs skaits tādu naturālu n, ka $a^n - 1$ dalās ar 2^n.	
BW2015.17 Atrast visus naturālos skaitļus n, kuriem $n^{n-1} - 1$ dalās ar 2^{2015}, bet nedalās ar 2^{2016}.	
LTE lemma 4: Ja x un y ir divi nepāru veseli skaitļi un m ir pāru naturāls skaitlis. Tādā gadījumā: $\nu_2(x^m - y^m) = \nu_2(x - y) + \nu_2(x + y) + \nu_2(m) - 1$.	$\nu_2(3^{16} - 1) = 1 + 2 + 4 - 1 = 6$.
LV.TST.1979.10.2 Pierādīt, ka eksistē tāds naturāls skaitlis n, ka $n^2 + 1$ dalās ar 5^{1979}.	
Henzela (Hensel) lemma: Ja polinomam $P(x)$ ir vienkārša sakne pēc kāda pirmskaitļa moduļa p, tad $P(x)$ būs vienkārša sakne arī pēc jebkuras šī pirmskaitļa pakāpes p^k, kuru var iegūt, pakāpeniski "paceļot" pakāpi. ($P(x)$ ir vienkārša sakne x_0 pēc moduļa p, ja $P(x_0) \equiv 0 \pmod{p}$, bet polinoma atvasinājuma vērtība $P'(x_0)$ ar p vairs nedalās.)	