Reizināšana pēc p moduļa, kur p ir nepāru pirmskaitlis ("Multiplikatīvā teorija").

Rezultāti par skaitļu kāpināšanu pēc moduļa p ir saistīti: definīcijas un teorēmas labāk iegaumēt kā vienotu sistēmu.

Intuīcija: Ja skaitli a, kas nedalās ar p, pietiekami ilgi reizina pašu ar sevi, iegūst atlikumu $1 \pmod{p}$.	
Mazā Fermā teorēma: Ja p ir pirmskaitlis un $\gcd(a,p)=1$, tad $a^{p-1} \equiv 1 \pmod{p}$.	$1^6 \equiv 2^6 \equiv 3^6 \equiv 4^6 \equiv 5^6 \equiv 6^6 \equiv 1 \pmod{7}$.

```
# Izdrukā dažādu skaitļu 40.pakāpes, ko dala ar 41. Tā ir Mazā Fermā teorēma pie p=41.
list(map(lambda x: x**40 % 41, range(1,41)))
# (Aizstājot kāpinātāju 40 ar citu skaitli, var pārliecināties, ka nesanāk visi vieninieki.)
```

Intuīcija: Ir tādi skaitļi a, kuri izstaigā visas kongruenču klases (izņemot $0 \pmod{p}$), pirms atgriežas pie $1 \pmod{p}$.	
Teorēma par primitīvo sakni: Katram pirmskaitlim p eksistē tāds a, kuram kongruenču klases $a^1, a^2, \ldots, a^{p-1}$ pieņem visas vērtības $1, 2, \ldots, p-1$ (sajauktā secībā). *Piezīme* Primitīvās saknes ir definējamas arī dažiem saliktiem skaitļiem, piemēram, pirmskaitļu pakāpēm p^k; to pakāpes izstaigā kongruenču klases, kuras nedalās ar p. Primitīvo sakņu tabulu sk. `https://bit.ly/2NqEzuB`.	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 $k=1,\ldots,6$. Arī 5 ir primitīvā sakne (mod 7). Citu primitīvo sakņu pirmskaitlim $p=7$ nav.

```
# Pirmskaitlim p=41 viena no primitīvajām saknēm ir 6. Kāpina a=6 visās pakāpēs līdz 40.pakāpei.
a = 6
list(map(lambda x: a**x % 41, range(1,41)))
set(list(map(lambda x: a**x % 41, range(1,41))))
# (Aizstājot a=6 ar citām vērtībām: 2, 3, 4, vai 5, var pārliecināties, ka tie nav primitīvās saknes.)
```

Intuīcija: Katram atlikumam a (ja $a \not\equiv 0 \pmod{p}$) var atrast vismazāko kāpinātāju, kuram a^k atgriežas pie vērtības $1 \pmod{p}$.	
Definīcija: Par skaitļa a multiplikatīvo kārtu (*multiplicative order*) pēc p moduļa sauc mazāko kāpinātāju k, kuram $a^k \equiv 1 \pmod{p}$. Multiplikatīvo kārtu apzīmē $\mathrm{ord}_p(a)$. **Apgalvojums #1:** Ja $\mathrm{ord}_p(a) = p-1$, tad a ir primitīvā sakne (mod p). **Apgalvojums #2:** $\mathrm{ord}_p(a)$ vienmēr ir $p-1$ dalītājs. **Apgalvojums #3:** Jebkuram skaitlim k, ar kuru dalās $p-1$, atradīsies tāds a, kuram $\mathrm{ord}_p(a) = k$. Definīciju sk. `https://bit.ly/35ZlK7V`.	$\mathrm{ord}_7(1) = 1$, $\mathrm{ord}_7(3) = \mathrm{ord}_7(5) = 6$, $\mathrm{ord}_7(2) = \mathrm{ord}_7(4) = 3$, $\mathrm{ord}_7(6) = 2$.

```
# Dažādo atlikumu skaits starp "a" pakāpēm sakrīt ar "a" multiplikatīvo kārtu.
# Pie p=41, ord(2)=20, ord(3)=8, ord(4)=10, ord(5)=20, ord(6)=40, utt.
a = 3
len(set(list(map(lambda x: a**x % 41, range(1,41)))))
# Mēģiniet atrast tādus a, kuriem multiplikatīvā kārta (ja p=41) ir 1,2,4,5,8,10,20,40.
# Visi tie eksistē (Apgalvojums 3), jo skaitlim p-1=40 ir tieši šādi dalītāji.
# Visus tos var viegli atrast, kāpinot primitīvo sakni (piemēram a=6) piemērotā pakāpē.
```

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 $x_2 \equiv -x_2$); 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 (*quadratic residue*), 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.

```
# Atrodam visus kvadrātiskos atlikumus, ja p=41 (Iegūstam tieši 20 skaitļus no 40.)
set(map(lambda x: x**2 % 41, range(1,41)))
# Tālāk risinām vienādojumu x**2 = 2. ("Kvadrātsakne no 2 (mod 41)")
list(filter(lambda x: x**2 % 41 == 2, range(1,41)))
# Iegūstam divas saknes: [17,24]. Ievērojam, ka 24 = -17 (mod 41).
```

Intuīcija: No visiem atlikumiem (izņemot atlikumu 0) būs tieši puse tādu, kuri atgriežas pie $1 \pmod{p}$ jau divreiz ātrāk nekā pēc $p-1$ soļiem.	
Definīcija: Par skaitļa a Ležandra simbolu (*Legendre symbol*) 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`.	$\left(\frac{0}{7}\right) = 0$. $\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1$. $\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$.

Piemērs. Visu atlikumu (kongruenču klašu) $a = 1, \ldots, 6$ pakāpes pēc $p = 7$ moduļa.

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 kārta).
- 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 $p = 5, 13, 17, 29, \ldots$, bet nevar atrisināt pirmskaitļiem $p = 3, 7, 11, 19, 23, \ldots$, jo tiem $\left(\frac{-1}{p}\right) = -1$.

Baltic Way atlase, 2019.g. septembris. Dots naturāls skaitlis m un pirmskaitlis p, kas ir skaitļa $m^2 - 2$ dalītājs. Zināms, ka eksistē tāds naturāls skaitlis a, ka $a^2 + m - 2$ dalās ar p. Pierādīt, ka eksistē tāds naturāls skaitlis b, ka $b^2 - m - 2$ dalās ar p.

Pierādījums. Zināms, ka $\left(\frac{2-m}{p}\right) = 1$; pieņemsim no pretējā, ka $\left(\frac{2+m}{p}\right) = -1$ (t.i. kongruenci $b^2 - m - 2 \equiv 0$ nevar atrisināt). Iegūstam:

$$1 \cdot (-1) = \left(\frac{2-m}{p}\right) \cdot \left(\frac{2+m}{p}\right) = \left(\frac{4-m^2}{p}\right) = \left(\frac{(4-m^2) + (m^2-2)}{p}\right) = \left(\frac{2}{p}\right).$$

Esam ieguvuši, ka $\left(\frac{2}{p}\right) = -1$, bet tas nav iespējams, jo $m^2 - 2$ dalās ar p, t.i. kongruenci $m^2 \equiv 2$ var atrisināt un 2 ir kvadrātiskais atlikums pēc p moduļa. Pretruna. ■

Jautājums. (A) Izmantojot Python vai jebkādus matemātiskus spriedumus, atrast cik dažādu primitīvo sakņu ir pirmskaitlim $p = 41$? (Viena no tām ir $a = 6$, bet ir arī citas.)
(B) Vai var pamatot, ka patvaļīgam nepāra pirmskaitlim p, primitīvo sakņu skaits ir $\varphi(p-1)$, kas ir Eilera funkcijas vērtība?