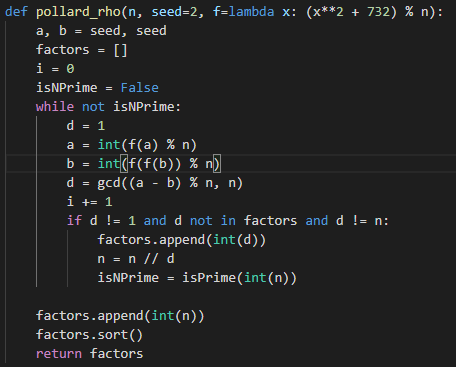
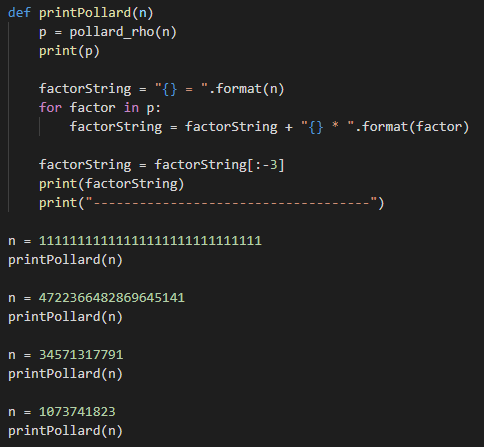
**Pollard rho algoritmas:**

Kodas:



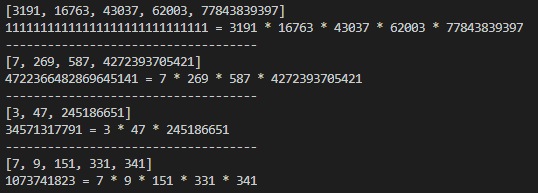
Naudoju daugianarį x2 + 732 mod(n) (n – faktorizuojamas skaičius, o daugianaris paimtas iš skaidrių) ir atlieku skaidrėse nurodytus veiksmus. Radus daliklį dalinu n iš jų tol, kol n nėra pirminis skaičius, o kai jis pasidaro pirminis pridedu jį prie daliklių. Seed – pradinės a ir b reikšmės.

Išvedimas:



Faktorizuojų jūsų duotą mažesnį skaičių (paskutinis) ir kelis savo variantus (vienas paimtas iš skaidrių), kad pademonstruoti daugiau panaudojimų.

Rezultatas:



Deja negalėjau faktorizuoti iš pradžių duoto skaičiaus, spėju, kad taip atsitiko, nes tas skaičius buvo dviejų didelių skaičių sandauga ir šis algoritmas arba nesugeba rasti tokių skaičių arba užtrunka daug ilgiau nei aš norėčiau laukti, taip pat jei ir randamas teisingas daliklis patikrinimas ar n yra pirminis padalinus iš šio daugiklio užtruktų labai ilgai su mano paprastu priminio skaičiaus tikrinimo algoritmu.