Skaitļu teorijas rezultāti, 2020-08-17

Ķīniešu atlikumu teorēma

Ja $m_1, m_2, \ldots, m_k$ ir pa pāriem savstarpēji pirmskaitļi, bet $a_1, a_2, \ldots, a_k$ ir jebkādi veseli skaitļi, tad eksistē vesels atrisinājums $x \in \mathbb{Z}$ šādai kongruenču sistēmai

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

Turklāt visi šīs sistēmas atrisinājumi ir savstarpēji kongruenti pēc moduļa $M = m_1 \cdot m_2 \cdot \ldots \cdot m_k$.

Kāpinātāja pacelšanas lemma (Lifting the Exponent Lemma)

Dots p ir pirmskaitlis, x un y ir veseli skaitļi, kuri ar p nedalās ($p \nmid x$ un $p \nmid y$), bet to starpība $x - y$ ar p dalās ($p \mid x - y$).

(A) ja p ir nepāru, tad

$$\nu_p(x^n - y^n) = \nu_p(x - y) + \nu_p(n).$$

(B) ja $p = 2$ un n ir pāru skaitlis, tad

$$\nu_2(x^n - y^n) = \nu_2(x - y) + \nu_2(n) + \nu_2(x + y) - 1.$$