Poglavlje 2

Kongruencije

Henselova lema

Teorem (**Lagrange**)**:** *Neka je $f \in \mathbb{Z}[x]$ polinom stupnja n. Ako vodeći koeficijent polinoma f nije djeljiv prostim brojem p, tada kongruencija $f(x) \equiv 0 \pmod{p}$ ima najviše n rješenja mod p.*

Teorem (**Henselova lema**)**:** *Neka je $f \in \mathbb{Z}[x]$. Ako je $f(a) \equiv 0 \pmod{p^j}$ i $f'(a) \neq 0 \pmod{p}$, tada postoji jedinstveni $t \in \{0, 1, \ldots, p-1\}$ takav da je $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$.*

Zadatak 2.22. Riješite kongruenciju $x^3 + 2x^2 - 21 \equiv 0 \pmod{7^3}$.

Rješenje. Neka je $f(x) = x^3 + 2x^2 - 21$. Rješenja kongruencije $f(x) \equiv 0 \pmod{7}$ su $x_0 = 0, -2$. Nultočka $x_0 = 0$ je dvostruka pa za nju ne možemo koristiti Henselovu lemu. 0 se ne može proširiti do rješenja $x_1 \bmod 7^2$ jer bi moralo vrijediti $x_1^3 + 2x_1^2 - 21 \equiv -21 \neq 0 \pmod{7^2}$.

Neka je sada $x_0 = -2$. Vrijedi $f(-2) = -21$ i $f'(-2) = 4$. Stoga je rješenje kongruencije mod 7^2 jednako $x_1 = -2 + 21 \cdot 4^{-1} = 40 \equiv -9 \pmod{7^2}$ (koristili smo da je $4^{-1} = 2 \bmod 7$).

Sada vrijedi $f(-9) = -588$. Stoga je rješenje kongruencije mod 7^3 jednako $x_2 = -9 + 588 \cdot 4^{-1} = 138 \pmod{7^3}$.

Dakle, jedino rješenje je $x \equiv 138 \pmod{7^3}$.

Zadatak 2.23. Riješite kongruenciju $x^5 + 4x^3 + 4x \equiv 0 \pmod{11^3}$.

Rješenje. Neka je $f(x) = x^5 + 4x^3 + 4x = x(x^2 + 2)^2$. Rješenja kongruencije $f(x) \equiv 0 \pmod{11}$ su $x_0 = 0, \pm 3$. Nultočke ± 3 su dvostruke pa za njih ne možemo koristiti Henselovu lemu.

Neka je x_1 rješenje kongruencije $x^2 + 2 \equiv 0 \pmod{11^2}$ koje dolazi od ± 3. Primijetimo da je tada $f(x_1) = x_1(x_1^2 + 2)^2$ djeljivo s 11^4. Polinom $x^2 + 2$ ima dvije jednostruke nultočke ± 3 pa ih možemo proširiti do rješenja $x_1 \equiv \pm 19 \pmod{11^2}$ preko Henselove leme.

Nultočka 0 je jednostruka pa ju možemo standardno proširiti do rješenja $x_2 \equiv 0 \pmod{11^3}$, preko Henselove leme ili samo tako da primijetimo da je $f(x)$ djeljiv s

x. Stoga su sva rješenja kongruencije

$$x \equiv 0 \pmod{11^3},\ x \equiv \pm 19 \pmod{11^2}.$$

Zadatak 2.24. Riješite kongruenciju $x^{112} + x \equiv 0 \pmod{11^2}$.

Rješenje. Vrijedi $\varphi(11^2) = 110$. Stoga je po Eulerovom teoremu $x^{112} \equiv x^2 \pmod{11^2}$. Rješenja kongruencije $x^2 + x \equiv 0 \pmod{11^2}$ su $x \equiv 0, -1 \pmod{11^2}$.

Napomena: Henselova lema zapravo daje jaču tvrdnju. Ako je $f \in \mathbb{Z}[x]$ i $a \in \mathbb{Z}$ nultočka polinoma f takva da je $f'(a) \neq 0$, tada se ona može proširiti do nultočke polinoma f u prstenu p-adskih cijelih brojeva $\mathbb{Z}_p$ (koji je proširenje prstena $\mathbb{Z}$). Prsten $\mathbb{Z}_p$ i njegovo polje razlomaka $\mathbb{Q}_p$ su vrlo važni u teoriji brojeva zbog svojih svojstava.