פולינום מודלרי

לאורך התרגיל p הינו ראשוני נקודתי חסר מסה ואיזוגי

<u>וויט:</u> אם $R(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0$ פולינום במקדמים שלמים, ו-$\alpha_1,\ldots,\alpha_n$ שורשיו (עם ריבוי) מודולו p, אז:

$$a_{n-1}=_p-(\alpha_1+\alpha_2+\cdots+\alpha_n)$$

$$a_{n-2}=_p\alpha_1\alpha_2+\alpha_1\alpha_3+\cdots+\alpha_{n-1}\alpha_n$$

$$\cdots$$

$$a_0=_p\pm\alpha_1\alpha_2\cdot\ldots\cdot\alpha_n$$

1) הוכיחו את משפט ווילסון:

$$(p-1)!\equiv_p-1$$

2) חשבו את $1^k+2^k+\cdots+p^k$ מודולו p.

3) מצאו את הדרגה המקסימלית של פולינום T מודולו p, כך שדרגתו קטנה מ-p וגם:

$$T(n)=T(m)(mod\ p)\Rightarrow n=m(mod\ p)$$

4) לכל פולינום f במקדמים שלמים נגדיר $f^n(x)=\overbrace{f(f(,,,f(x),,,))}^{n}$ כאשר f מופיע n פעמים. תארו את כל הפולינומים f עבורם $n|f^n(x)-x$ לכל n טבעי ולכל x שלם.

5) חשבו את:

$$(1^2+1)(2^2+1)\cdot\ldots\cdot((p-1)^2+1)$$

מודולו p.

6) יהי p ראשוני כך ש-$p-1=2q$ עבור q ראשוני אי-זוגי. נסמן ב-$g_1,\ldots,g_{q-1}$ את היוצרים הפרימיטיבים מודולו p, חשבו את הסכום שלהם, וסכום הריבועים שלהם.

7) עבור פולינום $P(x)=a_kx^k+\cdots+a_1x+a_0$ עם מקדמים שלמים, מספר המקדמים האי-זוגיים יסומן ב-$o(P)$. עבור $i\geq 0$ נסמן $Q_i(x)=(1+x)^i$. הוכיחו שאם $0\leq i_1<i_2<\cdots<i_n$ הם מספרים שלמים, אז:

$$o\left(Q_{i_1}+Q_{i_2}+\cdots+Q_{i_n}\right)\geq o\left(Q_{i_1}\right)$$

8) שני פולינומים מודולו p יוצאים שקולים כפונקציה מ-$\mathbb{Z}/p$ לעצמו, אם ורק אם ההפרש בינהם מתחלק ב-x^p-x, הוכיחו את זה, והסיקו שכל פונקצייה מתקבלת כפולינום. מה קורה מודולו p^2?

9) פולינום מתוקן במקדמים שלמים מקיים ש-$Q(x)$ הוא ריבוע עבור כל x שלם, הוכיחו ש-P הוא ריבוע.

(רמז: הסתכלו מודולו p^2 עבור $p|Q(x)$, מה אפשר להסיק מהתרגיל הקודם?)