שאריות ריבועיות

יהי p ראשוני אי-זוגי. שארית $a \neq 0$ תקרא שארית ריבועית מודולו p אם קיים x כך ש-$x^2 \equiv a \; mod \; p$.

1. הראו כי מספר השאריות הריבועיות מודולו p הוא $\frac{p-1}{2}$.

2. מצאו את סכום השאריות הריבועיות מודולו p.

3. מצאו את מכפלת השאריות הריבועיות מודולו p.

הגדרה: סימן לז'אנגר:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \exists x \neq 0, x^2 \equiv a \; mod \; p \\ 0, & if \; a = 0 \\ -1, & else \end{cases}$$

4. הוכיחו את קריטריון אוילר:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \; mod \; p.$$

5. הראו כי למשוואה $x^2 + y^2 + 1 \equiv 0 \; mod \; p$ יש פתרון.

6. הראו כי יש אינסוף ראשוניים מהצורה $4k + 1$.

7. הראו כי קיימת שארית לא ריבועית $0 < a < \sqrt{p} + 1$.

8. חשבו את הסכום

$$\left\lfloor\frac{1}{2027}\right\rfloor + \left\lfloor\frac{2}{2027}\right\rfloor + \left\lfloor\frac{2^2}{2027}\right\rfloor + \cdots + \left\lfloor\frac{2^{2025}}{2027}\right\rfloor$$

9. הוכיחו כי 2 הוא שארית ריבועית מוד p אם ורק אם $p \equiv \pm 1 \; mod \; 8$.

10. יהי $n \geq 3$ שלם. הראו כי שלם אי-זוגי a הוא שארית ריבועית מודולו 2^n אם ורק אם $a \equiv 1 \; mod \; 8$.

11. הראו כי ל-$2^n + 1$ אין מחלקים ראשוניים שהם 7 מוד 8.

12. אם $p \geq 7$, הוכיחו שכל שארית מודולו p מתקבלת כהפרש של שתי שאריות ריבועיות שונות מ-0.

13. פתרו בשלמים: $y^2 = x^3 + 7$.

14. מצאו את מספר הפתרונות של המשוואה $x^2 + y^2 \equiv 1 \; mod \; p$.

בתיאבון!