

Soru 1) Her $a \in U_{23}$ için $\left(\frac{-a}{23}\right) = -\left(\frac{a}{23}\right)$ olduğunu gösteriniz.

$23 \equiv 3 \pmod{4}$ olduğundan $-1 \notin Q_{23}$ 'tür. Yani $-1, 23$ modunda bir tamkare değildir. $\left(\frac{-a}{23}\right) = \left(\frac{-1}{23}\right) \cdot \left(\frac{a}{23}\right)$ olduğundan $\left(\frac{-1}{23}\right) = -1$ olup $\left(\frac{-a}{23}\right) = -\left(\frac{a}{23}\right)$ elde edilir.

Soru 2) $x \equiv a \pmod{m}$
 $x \equiv a \pmod{n}$

sisteminin çözümünün $x \equiv a \pmod{[m,n]}$ olduğunu gösteriniz.

İlk kongrüanstan k bir tamsayı olmak üzere $x = a + mk$ yazabiliriz. Bu değer ikincide yerine konulduğunda

$$a + mk \equiv a \pmod{n}$$

veya denk olarak $mk \equiv 0 \pmod{n}$ kongrüansı elde edilir. Bu son kongrüansın çözümü ise

$$k \equiv 0 \pmod{\left(\frac{n}{(m,n)}\right)}$$

şeklindedir. Bu çözüm t bir tamsayı olmak üzere

$$k = \frac{n}{(m,n)} t$$

şeklinde düşünülebilir. Bu değer yukarıda x için bulunan ifadede yerine konulursa

$$x = a + m \frac{nt}{(m,n)} = a + t[m,n]$$

veya $x \equiv a \pmod{[m,n]}$ elde edilir.

Soru 3) $x^{16} + x^2 + x + 3 \equiv 0 \pmod{17}$ denkleminin tüm çözümlerini bulunuz.

Fermat'ın küçük teoremi gereği $x^{16} \equiv 1 \pmod{17}$ yazabiliriz. O halde verilen kongrüans $x^2 + x + 4 \equiv 0 \pmod{17}$ olarak düzenlenebilir. Bu denklemin diskriminantı $\Delta = -15 \equiv 36 \pmod{17}$ olduğundan ve 17 asal modunda 36 'nın 6 ve 11 gibi iki karekökü olduğundan denklemin kökleri ikinci derece denklemin köklerini veren formülden 5 ve 11 olarak hesaplanabilir.

Soru 4) a bir tek tamsayı ise a^2 'nin 8 ile bölümünden kalanının ne(ler) olabileceğini belirleyip sebeplerini açıklayınız.

k bir tamsayı olmak üzere $a = 2k+1$ olsun. $a^2 = (2k+1)^2 = 4k^2+4k+1 = 4k(k+1) + 1$ olur. Burada k ve $k+1$ ardışık iki tamsayı olduğundan çarpımları çift olacaktır. Yani q bir tamsayı olmak üzere $k(k+1) = 2q$ şeklinde yazılabilir. O halde $a^2 = 4 \cdot 2q + 1 = 8q + 1$ bulunur. Bu da herhangi bir tek a tamsayısının karesinin 8 ile bölümünden kalanın 1 olduğunu gösterir.

Soru 5) 11 modundaki ilkel kökleri bulunuz.

$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 5, 2^5 \equiv 10, 2^6 \equiv 9, 2^7 \equiv 7, 2^8 \equiv 3, 2^9 \equiv 6, 2^{10} \equiv 1$ olduğundan 2 bir ilkel köktür. Benzer işlemlerle $6, 7, 8$ sayılarının da birer ilkel kök oldukları görülür.