2 Congruences and Euler's theorem

Recall that $a \equiv b \pmod m$ whenever $m \mid (a-b)$.

2.1. Solve the following congruences in $\mathbb{Z}$:

(a) $x \equiv 2 \pmod 8$,

(b) $3x \equiv 2 \pmod 5$,

(c) $27x \equiv 16 \pmod{41}$,

(d) $6x \equiv 2 \pmod 8$,

(e)* $ax \equiv b \pmod m$ for $a, b \in Z$, $m \in \mathbb{N}$.

2.2. Solve the following congruences in $\mathbb{Z}$:

(a) $x^2 + 5x \equiv 0 \pmod{19}$,

(b) $x^2 \equiv 1 \pmod p$ for p prime,

(c)* $x^2 + 10x + 6 \equiv 0 \pmod{17}$.

2.3. Divide polynomials using an analogue of the division with remainder you know from $\mathbb{Z}$:

(a) $x^4 + 3x^3 + 4x^2 + x + 3$ a $x^2 + 2$ in $\mathbb{Q}[x]$,

(b) $x^{10} + x^9 + x^7 + x^5 + x^3 + x^2 + x$ a $x + 1$ in $\mathbb{Z}_2[x]$ (here we deal with coefficients in the field $\mathbb{Z}_2$)

2.4. Calculate the greatest common divisor and the corresponding Bézout coefficients using analogue of Euclid's algorithm:

(a) $\gcd(x^3 - 1, x^2 - 1)$ in $\mathbb{R}[x]$,

(b) $\gcd(2x^2 + x - 1, x^2 + 1)$ in $\mathbb{R}[x]$,

(c) $\gcd(x^4 + x + 1, x^3 + x + 1)$ in $\mathbb{Z}_2[x]$

2.5. Show that $n^2 \equiv 1 \pmod 8$ for every odd $n \in \mathbb{N}$.

2.6. Determine the value

(a) $\varphi(600)$,

(b) $\varphi(7425)$ (it might be useful to know that $7425 = 27 \cdot 25 \cdot 11$),

(c)* of all natural n such that $\phi(n) = 18$.

2.7. Calculate

(a) $3^{5^7} \bmod 28$,

(b) $100^{99^{98}} \bmod 39$,

(c)* $100^{99^{98}} \bmod 40$.

2.8. Find the last

(a) one digits of 1357^{246},

(b) two digits of $999^{888^{777}}$,

(c)* three digits of 249^{19}.

2.9. Prove that $13 \mid 16^{20} + 29^{21} + 42^{22}$.

2.10. Find all $x \in \mathbb{Z}$ satisfying

(a) $x \equiv 2 \pmod{3}$, $\;x \equiv 4 \pmod{7}$, $\;x \equiv 3 \pmod{8}$.

(b) $2x + 1 \equiv 2 \pmod{3}$, $\;3x + 2 \equiv 3 \pmod{4}$, $\;4x + 3 \equiv 2 \pmod{5}$.

(c) $10x \equiv 6 \pmod{32}$, $\;3x \equiv 1 \pmod{5}$.

2.11. Find all $x \in \mathbb{Z}$ such that

(a) $x^2 \equiv 1 \pmod{3}$, $\;x^2 \equiv 1 \pmod{7}$.

(b) $x^2 \equiv -1 \pmod{66}$.

(c) $x^2 \equiv -1 \pmod{65}$.