2 Congruences and Euclid's algorithm again

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

2.1 (Proposition 2.1)**.** Let $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ for $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{N}$. Prove the following:

(a) $a + c \equiv b + d \pmod{m}$,

(b) $ac \equiv bd \pmod{m}$,

(c) $\forall k \geq 1 : a^k \equiv b^k \pmod{m}$.

2.2 (Proposition 2.2)**.** For any $a, b \in \mathbb{Z}$ and $c, m \in \mathbb{N}$ prove that:

(a) $a \equiv b \pmod{m} \Leftrightarrow ac \equiv bc \pmod{mc}$,

(b) if $\gcd(c, m) = 1$ then $a \equiv b \pmod{m} \Leftrightarrow ac \equiv bc \pmod{m}$,

(c) find a counterexample showing that b) does not hold if c and m are not coprime.

2.3. 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 $a, b \in Z$, $m \in \mathbb{N}$.

Solutions: (a) $2 + 8k$*, (b)* $4 + 5k$*, (c)* $34 + 41k$*, (d)* $34 + 41k$ *for* $k \in \mathbb{Z}$*.*

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

Solutions: (a) $19k$ *or* $14 + 19k$*, (b)* $\pm 1 + kp$ *(c)* $1 + 17k$ *or* $6 + 17k$ *for* $k \in \mathbb{Z}$*.*

2.5. Divide polynomials using analogue of the division with reminder 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 $\mathbb{Z}_2$),

(c) $x^n - 1$ a $x^m - 1$ in $\mathbb{Q}[x]$ for $n, m \in \mathbb{N}$.

Solution: (a)

$$\begin{array}{cccccccc} x^4 & +3x^3 & +4x^2 & +x & +3 & : & x^2+2 & = \; x^2+3x+2 \\ -x^4 & & -2x^2 & & & & & \\ \hline = & 3x^3 & 2x^2 & +x & +3 & & & \\ & -3x^3 & & -6x & & & & \\ \hline = & & 2x^2 & -5x & +3 & & & \\ & & -2x^2 & & -4 & & & \\ \hline & & & -5x & -1 & & & \end{array}$$

(b) $x^{10}+x^9+x^7+x^5+x^3+x^2+x = (x^9+x^6+x^5+x^2+1)(x+1)+1$

(c) if $n = qm + r$ *for* $q \in \mathbb{N}$ *and* $0 \le r < m$, *then* $x^n - 1 = \sum_{i=0}^{q-1} x^{im+r}(x^m-1) + x^r - 1$

2.6. 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 $\mathbb{Z}_2[x]$

Solution: (c)

a_i	u_i	v_i	q_i
x^4+x+1	1	0	
x^3+x+1	0	1	x
x^2+1	1	x	x
1	x	x^2+1	
0			

, *thus* $1 = x \cdot (x^4+x+1) + (x^2+1) \cdot (x^3+x+1)$.

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