$$[2x]_5 = [3]_5 \;\Rightarrow\; [2]_5 \cdot [x]_5 = [3]_5 \;\Rightarrow\; ([3]_5 \cdot [2]_5) \cdot [x]_5 = [3]_5 \cdot [3]_5 \;\Rightarrow$$
$$\Rightarrow\; [x]_5 = [4]_5$$

Cioè le soluzioni sono della forma $x = 4 + 5k$ al variare di $k \in \mathbb{Z}$.

Esercizio 3.32 *Scrivere codice in* MAGMA *in grado di determinare il giorno della settimana di una certa data. Attenzione alle regole per il calcolo degli anni bisestili. Cercare in rete la presenza di algoritmi all'uopo ideati.*

3.4.1 Criteri di Divisibilità

Mostriamo come le nozioni di congruenza introdotte sugli interi consentono di ottenere dei criteri di divisibilità ossia stabilire se un dato intero b ne divide un altro a. In particolare sono interessanti i casi in cui b non risulta molto grande. Nel seguito a verrà denotato in **forma decimale**

$$a = \sum_{i=0}^{d} a_i \cdot 10^i,$$

ove gli a_i sono cifre, i.e. $0 \leq a_i \leq 9$.

- $b = 2$: 2 divide a sse 2 divide a_0;
- $b = 3$: 3 divide a sse 3 divide $\sum_{i=0}^{d} a_i$. Infatti siccome $10 \equiv_3 1$ si ha
$$a \equiv_3 \sum_{i=0}^{d} a_i;$$
- $b = 5$: 5 divide a sse 5 divide a_0;
- $b = 9$: 9 divide a sse 9 divide $\sum_{i=0}^{d} a_i$. Segue come nel caso $b = 3$;
- $b = 11$: 11 divide a sse 11 divide $\sum_{i=0}^{d} (-1)^i a_i$. Segue come nel caso $b = 3$ osservando che $10 \equiv_{11} -1$;

Un'analisi più intrigante è richiesta per trattare il caso $b = 7$. Si noti che $10 \equiv_7 3$ e che $3^{-1} \equiv_7 -2$. Da cui $a \mod 7 = 0$ sse $-2a \mod 7 = 0$. Ora

$$-2a = -2 \cdot 10 \sum_{i=1}^{d} a_i 10^{i-1} - 2a_0 \equiv_7 \sum_{i=1}^{d} a_i 10^{i-1} - 2a_0.$$

Posto $H(a) = \sum_{i=1}^{d} a_i 10^{i-1}$ ne segue che 7 divide a sse 7 divide $H(a) - 2a_0$.

Esempio 3.33 *Sia $a = 123416526$ e $b = 7$. Un facile calcolo su carta o, per chi è pigro, un facile codice in* MAGMA *fornisce la seguente lista:*

$$[123416526, 12341640, 1234164, 123408, 12324, 1224, 114, 3].$$

Essendo il suo ultimo termine non nullo 7 non divide a.

La mappa $L : \mathbb{Z} \to \mathbb{Z}$ sembra ridurre in valore assoluto il suo argomento, ossia $|L(a)| < |a|$ ma questo non è sempre vero.

Esercizio 3.34 *Provate ad indagare quando questo non avviene e enunciare delle opportune richieste di arresto per il test di divisibilità per 7 sopra descritto.*

3.4.2 Primi Esempi di Codici Correttori

Il Criterio di divisibilità per 9 consente di descrivere un esempio molto semplice di codice rilevatore di errori noto con il nome di **prova del nove**. Supponiamo di voler sommare o moltiplicare due interi a, b tra loro. Posta $S(c)$ la somma delle cifre di un qualsiasi intero si ha che

$$S(a \cdot b) \equiv_9 S(a)S(b).$$

Se questo eguaglianza fallisce significa che abbiamo commesso errori nel calcolo di $a \cdot b$.

Esempio 3.35 *Sia* $a := 245142$, $b := 265127$. *I nostri calcoli ci forniscono* $m = a \cdot b = 64983763034$. *Valutiamo* $S(c)$ *per* $c = a, b, m$ *e otteniamo (questa volta correttamente)* $18, 23, 53$. *Riducendo modulo* 9 *otteniamo* $0 \cdot 5 \equiv_9 1$, *falsa.*

Putroppo questo codice è in grado di rilevare la presenza di errori ma non di correggerli.

Un altro esempio è il codice di Luhn utilizzato per la creazione dei numeri carta di credito. Queste sono codificate da un numero di 12 cifre diciamo $a = a_n \dots a_0$, dove $n = 11$. Sia L la funzione da $C = \{0, ldots, 9\}$ in sé definita da $L(c) = c$ se $c = 0, 9$, altrimenti $L(c) = 2cmod9$. Si calcola ora

$$v = a_0 + L(a_1) + a_2 + \dots + L(a_n).$$

Si ha che a è un numero di carta di credito valido solo se $v \mod 10 = 0$.

3.5 Congruenze sui polinomi

In modo analogo si possono definire congruenze in $A = K[x]$.

Definizione 3.36 *Dati* n, a *in* A *si dice che* n *divide* a *se esiste* $b \in A$ *tale che* $a = nb$ *e scriveremo* $n|a$.

Si fissi $n = n(x) \in A$ e si definisca aE_nb sse $n|a - b$.

Esercizio 3.37 *Dimostrare che* E_n *definisce una relazione di equivalenza su* A.

Esempio 3.38 *Se* $n = 0_A$, *il polinomio nullo, allora* $n|a - b$ *sse esiste* $c \in A$ *tale che* $a - b = 0_A c = 0_A$, *cioè* $a = b$.

Sia $a \in K$, allora possiamo pensare ad a come il polinomio costante

$$a \cdot 1_A + 0 \cdot x + \cdots .$$

Notate che scrivo $0_A, 1_A$ per sottolineare che si tratta del polinomio nullo e identicamente uguale a 1 (questo senza indice A perché trattasi di 1_K).

Esempio 3.39 *Sia $0_K \neq n \in K$ e $a \in A$, allora $a = n \cdot n^{-1}a$, ossia n divide qualsiasi polinomio. Quindi $aE_n 0_a$ per ogni $a \in A$.*

Analizziamo cosa accade quando n è un polinomio di grado positivo $d > 0$. Dato $a \in A$, l'algoritmo di divisione lunga afferma che esistono $q, r \in A$ tali che $a = nq + r$, $\deg(n) < d$, ossia $n|a - r$. Quindi $aE_n r$. Sia $r' \in A$ con $\deg(r') < d$ e $aE_n r'$. Allora $rE_n r'$ e n divide $r' - r$. Avendo grado minore di d, si ha $r = r'$. Abbiamo quindi

Teorema 3.40 *Dato $n \in A$ di grado $d > 0$, si ponga $E = E_n$, allora ogni classe di equivalenza $[a]_E$ contiene uno ed un solo polinomio di grado minore di d.*

Replicando la dimostrazione nel caso degli interi si verifica che E_n è una congruenza sia rispetto alla somma che al prodotto di polinomi. Come abbiamo fatto con gli interi scriveremo $[a]_n$ per la classe di a e $a \equiv_n b$ invece di $aE_n b$.

Esempio 3.41 *Sia $K = \mathbb{R}$, $n = x^2 + 1$ e $E = E_n$. Allora $d = 2$ e ogni classe è rappresentata da $a + bx$, $a, b \in \mathbb{R}$. La Proposizione 3.19 consente di definire una somma e un prodotto tra classi. Definiamo un prodotto tra reali e classi nel modo più naturale, ossia $b \cdot [c]_n := [bc]_n$. Si ponga $i := [x]_n$. Allora*

$$[a + bx]_n = [a]_n + [bx]_n = a[1]_n + b[x]_n = a \cdot 1 + bi = a + bi,$$

dove, con abuso di notazione, abbiamo posto $1 = [1]_n$. Abbiamo $(a + bi) + (c + di) = (a + c) + (b + d)i$ e

$$(a + bi)(c + di) = (ac + bdi^2) + (ad + bc)i = (ac - bd) + (ad + bc)i.$$

Va giustificata la seconda uguaglianza. Ora

$$i^2 = [x]_n^2 = [x^2]_n = [-1 + x^2 + 1]_n = [-1]_n = -1.$$

Il precedente esempio fornisce formalmente i numeri complessi. Segnalo che termini come unità immaginaria fanno pensare che la loro esistenza non sia stata accettata facilmente dai Matematici e in seguito da Fisici, Ingegneri e Informatici.

Ricordo che anche nel caso delle algebre Booleane definite per studiare la Logica Proposizionale abbiamo usato due volte insieme quozienti. La prima volta per introdurre il campo delle classi resto modulo due, la seconda per identificare x^2 con x per ogni variabile, ossia introducendo E_n per $n = x^2 - x$.

Esercizio 3.42 *Mostrare che $K = \mathbb{Z}/3$ è un campo. Sia $x^2 + 1 \in A = K[x]$ ed $E = E_n$. Provare che A/E contiene 9 classi e costruire le tabelle additiva e moltiplicativa di A/E. Quali classi ammettono inverso?*