Chapitre

l'Arithmétique dans $\mathbb{Z}$.

I PGCD & PPCM .

1 Rappel et Complément .

D Définition

Soient a et b deux entiers relatifs non nuls.le plus grand commun diviseur de a et b, qu'on note $a \wedge b$ ou $PGCD(a,b)$, est le plus grand des diviseurs communs à a et b.
Le plus petit commun multiple de a et b, qu'on note $a \vee b$ ou $PPCM(a,b)$, est le plus petit des multiples strictement positifs communs à a et b.
On Convient que : $a \wedge 0 = |a|$ et $a \vee 0 = 0$.

Remarque

Soient a et b deux entiers relatifs non nuls. Si $d = a \wedge b$ et $m = a \vee b$ alors :

1. $d \geqslant 1$ et d/a et d/b
2. $m \geqslant 1$ et a/m et b/m
3. $\forall c \in \mathbb{N}^* : [(c/a \text{ et } c/b) \Longrightarrow c/d]$ et $[(a/c \text{ et } b/c) \Longrightarrow m/c]$.
4. $\forall c \in \mathbb{N}^* : [(c/a \text{ et } c/b) \Longrightarrow c \leqslant d]$ et $[(a/c \text{ et } b/c) \Longrightarrow m \leqslant c]$.
5. $|a| \wedge |b| = d$ et $a \wedge 1 = 1$ et $a \wedge aa \wedge 0 = |a|$.
6. $|a| \vee |b| = m$ et $a \vee 1 = |a|$ et $a \vee a = |a|$.

Propriété

Soient a , b et c trois entiers relatifs non nuls, soit $n \in \mathbb{N}$. Alors :

1. $a \wedge b = b \wedge a$. et $a \vee b = b \vee a$
2. $a/b \Longleftrightarrow a \wedge b = |a| \Longleftrightarrow a \vee b = |b|$
3. $(a \wedge b) \wedge c = a \wedge (b \wedge c)$.
4. $(ca \wedge cb) = |c|(a \wedge b)$.
5. $\left\{ \begin{matrix} c/a \\ c/b \end{matrix} \right. \Longrightarrow (\frac{a}{c}) \wedge (\frac{b}{c}) = \frac{a \wedge b}{|c|}$.
6. $(a \vee b) \vee c = a \vee (b \vee c)$.
7. $(ca \vee cb) = |c|(a \vee b)$.
8. $\left\{ \begin{matrix} c/a \\ c/b \end{matrix} \right. \Longrightarrow (\frac{a}{c}) \vee (\frac{b}{c}) = \frac{a \vee b}{|c|}$.
9. $a^n \wedge b^n = (a \wedge b)^n$ et $a^n \vee b^n = (a \vee b)^n$.
10. $(a \wedge b) \times (a \vee b) = |ab|$

2 Calcul du PGCD : Algorithme d'Euclide.

Propriété

Soit $a \in \mathbb{Z}^*$ et $b \in \mathbb{N}$
Lorsque b ne divise pas a, alors le $PGCD(a,b)$ est égale au dernier reste non nul obtenu grâce à l'algorithme d'Euclide

3 Nombres premiers entre eux .

D **Définition**

soient a et b deux entiers relatifs non nuls.
On dir que a et b sont premiers entre eux si leurs PGCD vaut 1 c'est à dire : $a \wedge b = 1$.

T **Théorème**

soient a et b deux entiers relatifs non nuls, et $d \in \mathbb{N}^*$, alors :

$$d = a \wedge b \Longleftrightarrow \left[(\exists(\alpha,\beta) \in \mathbb{Z}^2)/a = \alpha d \quad \text{et} \quad b = \beta b \quad \text{et} \quad \alpha \wedge \beta = 1\right]$$

T **Théorème**

soit $(a,b) \in \mathbb{Z}^2$:
On a l'implication suivante :
$d = a \wedge b \Longleftrightarrow \left[(\exists(u,v) \in \mathbb{Z}^2)/ \quad d = au + bv\right]$.

Remarque

le couple (u,v) n'est pas **unique**.En effet :
$9 \wedge 4 = 1 = 1 \times 9 - 2 \wedge 4 \quad (u = 1 \quad et \quad v = -2)$
$9 \wedge 4 = -43 \times 9 + 97 \times 4 \quad (u = -43 \quad et \quad v = 97)$.
La réciproque du dernier théorème n'est pas toujours vraie, ainsi $3 \times 5 + 7 \times (-1) = 8$ mais $3 \wedge 7 \neq 8$

4 Théorème de Bezout

Application

En utilisant le theoreme de Bezout, montrer que pour tout $n \in \mathbb{N}$:

1. $(5n+3) \wedge (2n+1) = 1$.
2. $(2n-1) \wedge (3-7n) = 1$

5 Détermination des coefficient du théorème de Bezout

l'inconvénient du théorème de Bezout, sous sa forme théorique, est qu'il fournit pas les coefficients u et v intervenant dans la relation $au+bv=1$.
l'algorithme d'Euclide fournit une telle réponse pratique à ce problème.

T **Théorème**

Soient a,b et c des entiers relatifs non nuls.On a l'implication suivante :
$(a/bc \quad \text{et} \quad a\wedge b=1) \Longrightarrow a/c$. ce résultat est connu sous le nom du ❝Théorème de Gauss❞

Remarque

dans le dernier théorème, la condition de primalité $a\wedge b=1$des deux relatifs a et b est nécessaire , en effet $8/48$ et $12/48$ mais 12×8 ne divise pas 48

Propriété

soient $a,b \quad \text{et} \quad c$ trois entiers relatifs non nuls.alors :

1. $(a\wedge b=1 \quad \text{et} \quad a\wedge c) \Longleftrightarrow a\wedge bc=1$.
2. $\forall (m,n)\in \mathbb{N}^{*2} : (a\wedge b=1 \Longleftrightarrow a\wedge b^n=1) \quad \text{et} \quad (a\wedge b=1 \Longleftrightarrow a^m\wedge b^n=1)$

6 L'équation diophantienne : $ax+by=c$

T **Théorème**

Si le couple (x_0,y_0) est une solution de l'équation $ax+by=c$, alors l'ensemble des solutions de cette équation est : $\mathscr{S}=\left\{\left(x_0+\dfrac{bk}{a\wedge b};y_0-\dfrac{ak}{a\wedge b}\right)/k\in\mathbb{Z}\right\}$

7 PGCD et PPCM d'un nombre fini d'entiers relatifs

D **Définition**

Soit n un entier naturel tel que $n\geqslant 2$, et soient $a_0,a_1,a_2\cdots\cdots a_n$ des entiers relatifs non nuls.
Le plus grand commun diviseur des ces entiers qu'on note $a_1\wedge a_2\wedge a_3\cdots\wedge a_n$ est le plus grand diviseur commun positif à $a_2,a_2,a_3\cdots a_n$.
Le plus petit commun multiple des ces entiers qu'on note $a_1\vee a_2\vee a_3\cdots\vee a_n$ est le plus petit multiple commun positif à $a_2,a_2,a_3\cdots a_n$.

T **Théorème**

Soit n un entier naturel tel que $n\geqslant 2$, et soient $a_0,a_1,a_2\cdots\cdots a_n$ des entiers relatifs non nuls.Il existe des entiers relatifs $u_1,u_2,\cdots u_n$ tel que : $\sum_{i=1}^{n} a_iu_i=\delta$ avec δ désigne le plus grand diviseur commun de $a_1,a_2\cdots a_n$

D **Définition**

Soit n un entier naturel tel que $n \geqslant 2$, et soient $a_0, a_1, a_2 \cdots\cdots a_n$ des entiers relatifs non nuls. On dit que les entiers $a_1, a_2, \cdots\cdots a_n$ sont premiers entre eux si 1 est le seul diviseur positif commun à tous ces entiers, c'est à dire que : $a_1 \wedge a_2 \wedge \cdots\cdots \wedge a_n = 1$.

Remarque

1. Dire que les entiers sont premiers entre eux, signifie pas qu'il sont premiers entre eux deux à deux, en effet $a =, b = 7$ et $c = 12$ sont premiers entre eux, par contre $a \wedge c = 4 \geq 1$.
2. La relation $(a \wedge b)(a \vee b) = |ab|$ n'est pas valable pour plus de deux entiers relatifs. c'est à dire en général : $(a \wedge b \wedge c)(a \vee b \vee c) \neq |abc|$.
3. Le résultat de ce théorème reste valable pour plus de deux entiers relatifs , plus précisément : $(n \geqslant 2), \delta = a_1 \wedge a_2 \wedge \cdots \wedge a_n$ signifie qu'il existe $(a_1, a_2, \cdots\cdots a_n) \in \mathbb{Z}^n : \sum_{i=1}^{n} a_i u_i = 1$. autrement dit :

$$(a_1 \wedge a_2 \wedge \cdots \wedge a_n = 1) \Longleftrightarrow \left[\exists (u_1, u_2 \cdots u_n) \in \mathbb{Z}^n : \sum_{i=1}^{n} a_i u_i = 1\right]$$

8 Congruence modulo n (Rappel et complément)

D **Définition**

soit $n \in \mathbb{N}^*$. On dit que deux entiers a et b sont congrus modulo n si l'entier n divise $b - a$, c'est à dire $\exists k \in \mathbb{Z}$ tel que : $b = a + kn$, et on écrit : $a \equiv b[n]$

Propriété

soit $n \in \mathbb{N}^*$. La relation de ❝ Congruence modulo n ❞ est une relation d'équivalence sur $\mathbb{Z}$, c'est à dire :

1. Réflexive : $(\forall a \in \mathbb{Z}) : a \equiv a[n]$.
2. Symétrique : $\left(\forall (a,b) \in \mathbb{Z}^2\right) : a \equiv b[n] \Longrightarrow b \equiv a[n]$.
3. Transitive : $\left(\forall (a,b,c) \in \mathbb{Z}^3\right) : a \equiv b[n] \quad \text{et} \quad b \equiv c[n] \Longrightarrow a = c \equiv [n]$.

Propriété

Soit $n \in \mathbb{N}$ et soit $(a,b,c,d) \in \mathbb{Z}^4$ .Alors :

1. $a \equiv b[n] \Longleftrightarrow$ (les restes de la division euclidienne de a t et b par n sont égaux)
2. Si $a \equiv b[n]$ et $c \equiv d[n]$ alors $a + c \equiv b + d[n]$ et $ac \equiv bd[n]$
3. Si $a \equiv b[n]$ et $k \in \mathbb{Z}^*$ alors $ka \equiv kb[n]$
4. Si $a \equiv b[n]$ et $p \in \mathbb{N}$ alors $a^p \equiv b^p[n]$

T **Théorème**

Soient $a,b,c \in \mathbb{Z}^*$ et $n \in \mathbb{N}^*$.
Si $d = c \wedge n$ alors : $ac \equiv bc[n] \Longleftrightarrow a \equiv b\left[\frac{n}{d}\right]$

Propriété

Soit $(a,b,c) \in \mathbb{Z}^{*,3}$ et soit $(n,p) \in \mathbb{N}^{*,2}$ tel que : $c \wedge n = 1$, Alors :

1. $ac \equiv bc[n] \Longleftrightarrow a \equiv b[n]$
2. $\begin{cases} a \equiv b[n] \\ p/n \end{cases} \Longrightarrow a \equiv b[p]$
3. $\begin{cases} ac \equiv bc[p] \\ n \text{ne divise pas} \end{cases} \Longrightarrow a \equiv b[p]$

II Les Nombres Premiers

1 Rappel et complément

D **Définition**

Un entier relatif p est dite **Premier** s'il admet exactement quatre diviseurs.

Remarque

Si p est un entier premier dans $\mathbb{N}$, alors $-p$ est premier dans $\mathbb{Z}$, c'est pourquoi dans cette section nous nous limitons à l'ensemble $\mathbb{N}$.L'ensemble des nombres premiers positifs et noté $\mathbb{P}$, et un entier $n \geqslant 2$ non premier est dit Composé.

T **Théorème**

Soit n un entier composé supérieur ou égale à 2, Alors :

1. Le plus petit diviseur positif de n différent de 1 est un nombre premier.
2. n est un produit de nombres premiers, en particulier n possède au moins un diviseur premier.
3. n possède un facteur premier p tel que : $p^2 \leqslant n$

T **Théorème**

L'ensemble $\mathbb{P}$ est un ensemble **Infini**

T **Théorème**

1. Si p et q sont deux nombres premiers positifs distincts, alors ils sont premiers entre eux. en d'autre terme : $p,q \in \mathbb{P}$ et $p \neq q \Longleftrightarrow p \wedge q = 1$.
2. si $p \in \mathbb{P}$ alors p est premier avec tous les entiers qu'il ne divise pas, c'est à dire : $(\forall a \in \mathbb{Z})(\forall p \in \mathbb{P}) : [(\ p \quad \text{ne divise pas}\ ) \Longrightarrow p \wedge a = 1]$

Propriété

Soit $(a,b) \in \mathbb{Z}^2$ et p un nombre premier, alors :

$$p/ab \quad \Longleftrightarrow \quad (p/a \quad ou \quad p/b)$$

COROLAIRE

⁕ Soient $a_1, a_2, \cdots a_n$ des entiers relatifs et soit p un nombre premier, alors :

$$p/\ a_1.a_2.....a_n \quad \Longleftrightarrow \quad (\exists i \in \{1,2,\cdots\cdots n\} :\ p/a_i)$$

⁕ Soit $a \in \mathbb{Z}$ et p un nombre premier, alors :

$$(\forall n \in \mathbb{N}) \quad p/a^n \quad \Longleftrightarrow \quad p/a.$$

⁕ Soient $p_1, p_2, \cdots p_n$ et p des nombres premiers, alors :

$$p/p_1.p_2 \cdots p_n \quad \Longleftrightarrow \quad (\exists i \in \{1,2,\cdots,n\} : \quad p = p_i)$$

2 Petit théorème de FERMAT

T **Théorème**

1. Si p est un nombre premier positif, alors pour tout $a \in \mathbb{Z}$, alors p divise $a^p - a$, autrement : $(\forall a \in \mathbb{Z}) : a^p \equiv a[p]$
2. Si p est un nombre premier positif, alors pour tout $a \in \mathbb{Z}$: $p \wedge a = 1 \Longleftrightarrow a^{p-1} \equiv 1[p]$

Remarque

La réciproque du théorème de FERMAT n,est pas vraie, en effet si $a^{p-1} \equiv 1[p]$ alors l'entier p n'est pas forcement un nombre premier.A titre d'exemple soit $p = 341 = 31 * 11$ n'est pas premier, pourtant il divise $2^3 41 - 2$ car :
$2^{341} - 2 = 2(2^{340} - 1) = 2((2^{10})^{34} - 1) = 2(2^{10} - 1)\sum_{k=0}^{3} 32^{10k} = 2 * 3 * 341 * \sum_{k=0}^{3} 32^{10k}$
Le petit théorème de FERMAT permet de calculer le reste de n'importe quel entier assez grand modulo un nombre premier positif p.

3 Décomposition en produit de facteurs premiers

Théorème

Tout élément de $\mathbb{Z}^* - \{-1,1\}$admet une décomposition en produit de nombre premiers, unique à l'ordre prés des facteurs. Autrement dit, si $n \in \mathbb{Z}^* - \{-1,1\}$, il existe $N \in \mathbb{N}^*, \varepsilon \in \{-1,1\}$ des nombres premiers deux à deux distincts $p_1, p_2, \cdots p_N$, et des entiers $\alpha_1, \alpha_2, \alpha_N$ tels que : $n = \varepsilon.p_1^{\alpha_1}.p_2^{\alpha_2} \cdots\cdots p_N^{\alpha_N}$.
Ce théorème est connu sous le nom du ❄Théorème fondamental de l'Arithmétique❄

4 Application de la décomposition en produit de facteurs premiers

Théorème

Soit $n \in \mathbb{Z}^* - \{-1,1\}$et sa décomposition $n = \varepsilon.p_1^{\alpha_1}.p_2^{\alpha_2} \cdots\cdots p_N^{\alpha_N}$ en produit de facteurs premier .
Les diviseurs de n sont les entiers relatifs : $d = \varepsilon'.p_1^{\gamma_1}.p_2^{\gamma_2} \cdots\cdots p_N^{\gamma_N}$ avec $0 \leqslant \gamma_k \leqslant \alpha_k, \forall k \in \{1,2,....N\}$ et $\varepsilon' \in \{-1,1\}$.
le nombre des diviseurs positifs de n vaut : $(1+\alpha_1)(1+\alpha_2)\cdots(1+\alpha_N)$

III L'Ensemble $\mathbb{Z}/n\mathbb{Z}$

1 Classe d'équivalence

Définition

Soit $n \in \mathbb{N}^*$.
L'ensemble des entiers relatifs qui ont le même reste r de la division euclidienne par n est appelé la classe d'équivalence de r, qu'on note $\bar{r}$.
C'est la classe d'équivalence de r modulo n dans $\mathbb{Z}$.
Généralisation : soit $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$, la classe d'équivalence de a modulo n est définie par :

$$\bar{a} = \{x \in \mathbb{Z} \,/\, x \equiv a[n]\} = \{a + kn \,/\, k \in \mathbb{Z}\}$$

Application

Déterminer la classe d'équivalences modulo 12 de chacun des nombres suivants :

116 1979 2018.

Proposition

Soit $n \in \mathbb{N}^*$.pour tout $x \in \mathbb{Z}$, on désigne par $\bar{x}$ la classe d'équivalence de x modulo n.Alors :

1. $(\forall a \in \mathbb{Z})\,(\exists! r \in \{0,1,2,\cdots,n-1\})$: $\quad \bar{a} = \bar{r}$.
2. Si $0 \leqslant r < n$ et $0 \leqslant r' < n$ alors : $\bar{r} = \bar{r'} \Longleftrightarrow r = r'$ et $r \neq r' \Longleftrightarrow \bar{r} \bigcap \bar{r'} = \emptyset$.

3 $(\forall x \in \mathbb{Z})\,(\exists! r \in \{0,1,2,\cdots,n-1\}) : x \in \bar{r}$ (avec r est le reste de la division euclidienne de x par n).

4 $\mathbb{Z} = \bar{0} \cup \bar{1} \cup \bar{2} \cup \cdots\cdots \cup \overline{(n-1)}$.

5 $\mathbb{Z}/n\mathbb{Z} = \left\{\bar{0};\ \bar{1};\ \bar{2};\ \cdots\cdots \overline{(n-1)}\right\}$

2 Opérations dans l'ensemble $\mathbb{Z}/n\mathbb{Z}$

D **Définition**

Soit $n \in \mathbb{N}^*$.
On définit l'addition dans $\mathbb{Z}/n\mathbb{Z}$ comme suit : $\bar{x}+\bar{y} = \overline{x+y} \quad \forall \bar{x},\bar{y} \in \mathbb{Z}/n\mathbb{Z}$.
On définit la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ comme suit : $\bar{x} \times \bar{y} = \overline{x \times y} \quad \forall \bar{x},\bar{y} \in \mathbb{Z}/n\mathbb{Z}$.

Application

Résoudre dans $\mathbb{Z}/6\mathbb{Z}$ les equations suivantes :

1 $\bar{4}x = \bar{2}$

2 $\bar{3}x^2 + x + \bar{1} = \bar{0}$

T **Théorème**

Soit p un nombre premier positif. Alors :

1 $(\forall \bar{x} \in \mathbb{Z}/p\mathbb{Z} - \{\bar{0}\})\ (\exists \bar{y} \in \mathbb{Z}/p\mathbb{Z} - \{\bar{0}\}) : \bar{x} \times \bar{y} = \bar{1}$.

2 $(\forall (\bar{x};\bar{y}) \in (\mathbb{Z}/p\mathbb{Z})^2)\ [\bar{x} \times \bar{y} = \bar{0} \iff (\bar{x} = \bar{0} \quad \text{ou} \quad \bar{y} = \bar{0})]$

IV Système de Numération

1 Représentation d'un entier naturel dans un système de numération

D **Définition**

la base b d'un système de numération représente le nombre d'unités d'un certain rang, nécessaire pour former une unité de rang immédiatement supérieur.
L'ensemble $\mathscr{B}_b = \{0,1,2,\cdots\cdots,(b-1)\}$, soit b caractères (chiffre en base 10) quantifie le nombre d'unités d'un rang quelconque.

Théorème

Soit b un entier naturel supérieur ou égale à 2.
Tout entier naturel non nul $n$peut de manière unique sous la forme :

$$n = a_m b^m + a_{m-1} b^{m-1} + \cdots\cdots + a_2 b^2 + a_1 b + a_0$$

où $a_0, a_1, \cdots, a_m$ sont des entiers tels que : $a_m \neq 0$ et $0 \leqslant a_i \leqslant b-1 \quad \forall i \in \{0,1,2,\cdots\cdots,m\}$
On écrit : $n = \overline{a_m a_{m-1} \cdots\cdots a_1 a_0}_{(b)}$.et On dit qu'on a représenter le nombre n dans le système de numération de base b

Application

1 Convertir en binaire les nombres suivants :

$$97; \quad 397; \quad 133$$

2 Convertir en numération décimale les nombres dont l'écriture en binaire est :

$$\overline{101}_{(2)} \qquad \overline{1101110}_{(2)}$$

2 Comparaison de deux nombre présentés dans le même système de numération

Théorème

Soient x et y deux entiers naturels représentés dans le même système de numération par :

$$x = \overline{a_n a_{n-1} \cdots\cdots a_1 a_0}_{(b)} \text{ et } y = \overline{c_m c_{m-1} \cdots\cdots c_1 c_0}_{(b)}$$

1 Si $m > n$ alors $y > x$

2 Si $m = n$ et $c_n = a_n$ et $c_{n-1} = a_{n-1}$ et $\cdots\cdots$ et $c_{i+1} = a_{i+1}$ et $c_i \neq a_i$, alors l'ordre de x et y est celui de c_i et a_i, En particulier si $c_i > a_i$ alors $y > x$

3 Addition et multiplication de deux nombre représentés dans le même système de numér

1 On considère les deux nombres suivants : $x = \overline{5312}_{(6)}$ et $y = \overline{214}_{(6)}$.
On veut représenter le nombre $x+y$ en base 6.
On a : $x = 5\times 6^3 + 3\times 6^2 + 6 + 2$ et $y = 2\times 6^2 + 6 + 4$
Par conséquent : $x+y = 5\times 6^3 + 5\times 6^2 + 3\times 6 + 2 = \overline{5530}_{(6)}$.
On peut représenter le nombre $x+y$ directement en base 6 en utilisant la méthode vue en primaire ❝l'addition par retenue❞ comme suit :

$$\begin{array}{r} {\scriptstyle 1} \\ \overline{5312}_{(6)} \\ + \\ \overline{214}_{(6)} \\ \hline = \overline{5530}_{(6)} \end{array}$$

2 On considère les deux nombres suivants : $a = \overline{432}_{(5)}$ et $b = \overline{134}_{(5)}$

On veut représenter le nombre $a \times b$ en base 5.
On a $a = 4 \times 5^2 + 3 \times 5 + 2$ et $b = 5^2 + 3 \times 5 + 4$._ Par conséquent :

$$\begin{aligned} a \times b &= (4 \times 5^2 + 3 \times 5 + 2)(5^2 + 3 \times 5 + 4) \\ a \times b &= 5^5 + 3 \times 5^4 + 5^3 + 4 \times 5 + 3 \\ a \times b &= \overline{131043}_{(5)} \end{aligned}$$

Tout comme l'addition , on peut representer le nombre $a \times b$ directement dans la base 5 en utilisant la méthode de ❝la multiplication par retenue❞ comme suit :

$$\begin{array}{r} \overset{1}{\overline{432}_{(5)}} \\ \times \\ \overline{134}_{(5)} \\ \hline 333 \\ + \\ 2401\bullet \\ + \\ 432\bullet\bullet \\ \hline = \overline{131043}_{(5)} \end{array}$$

4 Critère de divisibilité sur les nombres : 3; 4; 5; 9; 11; 25

Proposition

Soit $x \in \mathbb{N}$ tel que $x = \overline{a_n a_{n-1} \cdots\cdots a_1 a_0}_{(10)} = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots\cdots + a_1 \times 10 + a_0$ avec $a_n \neq 0$ et $0 \leqslant a_i \leqslant 10 \quad \forall i \in \{0, 1, 2, \ldots\ldots, n\}$.
On a les conséquences suivantes :

1. $x \equiv 0[5] \iff (a_0 = 0 \quad \text{ou} \quad a_0 = 5)$
2. $x \equiv 0[25] \iff \overline{a_1 a_0}_{(10)} \equiv 0[25]$
3. $x \equiv 0[4] \iff \overline{a_1 a_0}_{(10)} \equiv 0[4]$
4. $x \equiv 0[3] \iff \sum_{i=0}^{n} a_i \equiv 0[3]$
5. $x \equiv 0[9] \iff \sum_{i=0}^{n} a_i \equiv 0[9]$
6. $x \equiv 0[11] \iff \sum_{i=0}^{n} (-1)^i a_i \equiv 0[11]$