Préparation à l'agrégation interne de mathématiques - Année 2011
Arithmétique dans $\mathbb{Z}$ - Mercredi 08 juin 2011

1 Divisibilité dans $\mathbb{Z}$, congruences

Exercice 1.1. *En utilisant une combinaison linéaire adéquate, démontrer que :*

1. *deux entiers consécutifs sont premiers entre eux ;*
2. *deux entiers impairs consécutifs sont premiers entre eux ;*
3. *les entiers $3n+5$ et $2n+3$ sont premiers entre eux (n entier).*

Exercice 1.2. *Déterminer tous les entiers relatifs n tels que le réel $\frac{5n^2+3n+2}{n+3}$ soit un entier.*

Exercice 1.3. *L'ensemble $\{n^2-25 : n \in \mathbb{N}\}$ contient-il des nombres premiers ?*

Exercice 1.4.
1. *Résoudre dans $\mathbb{N}^2$, l'équation $a^2-b^2=12$.*
2. *Vérifier que 2011 est un nombre premier. Résoudre dans $\mathbb{N}^2$, l'équation $a^2-b^2=2011$.*
3. *Soient a et b deux entiers tels que a^2-b^2 soit pair. Montrer que a^2-b^2 est divisible par 4.*
4. *Résoudre dans $\mathbb{N}^2$, l'équation $a^2-b^2=162$.*

Exercice 1.5.
1. *Soient p et q deux entiers naturels non nuls. Démontrer (à l'aide d'une somme de termes d'une suite géométrique) que 2^p-1 divise $2^{pq}-1$.*
2. *En déduire une condition nécessaire simple pour que l'entier $M_n=2^n-1$ (nombre de Mersenne) soit premier. Contre-exemple au caractère suffisant ?*

Exercice 1.6 (utilisation du plus petit élément)**.** *Le nombre φ (environ $1,618$) est le réel positif vérifiant l'égalité $\varphi^{-1}=\varphi-1$. Démontrer qu'il est irrationnel.*
(Indication : par l'absurde, utiliser le plus petit numérateur positif permettant de représenter φ comme un rationnel.)

Exercice 1.7. *Calculs modulo 4.*

1. *Dresser la table de multiplication dans $\mathbb{Z}/4\mathbb{Z}$.*
2. *Montrer que, si un entier est la somme de deux carrés, il est congru à 0, 1 ou 2 modulo 4.*
3. *Résoudre dans $\mathbb{N}^2$ l'équation $a^2+b^2=2011$.*
4. *Retrouver le résultat de l'exercice 1.4 3).*

Exercice 1.8. *Calculs modulo 5.*

1. *Dresser la table de multiplication dans $\mathbb{Z}/5\mathbb{Z}$.*
2. *Résoudre dans $\mathbb{Z}$ l'équation $x^2+1 \equiv 0 \pmod 5$.*
3. *Déterminer selon l'entier naturel n, le reste de 13^n dans la divion euclidienne par 5.*

Exercice 1.9. *Quel est le chiffre des unités (en notation décimale) du nombre 7^{2011} ? Et le chiffre des dizaines ?*

2 Décomposition, $PGCD$, $PPCM$, Euclide, Bézout, Gauss

Exercice 2.1. *Soient a et b deux entiers non nuls et $\delta = PGCD(a;b)$. Montrer que $\frac{a}{\delta}$ et $\frac{b}{\delta}$ sont deux entiers premiers entre eux.*

Exercice 2.2.
1. *Décomposer 2600 en produit de facteurs premiers.*
2. *Combien 2600 admet-il de diviseurs positifs ?*
3. *Déterminer les deux (respectivement trois) plus petits entiers naturels admettant exactement 35 diviseurs positifs.*
4. *Démontrer qu'un entier non nul est un carré parfait si et seulement s'il admet un nombre impair de diviseurs positifs.*

Exercice 2.3. *1. Appliquer l'algorithme d'Euclide aux nombres* 1806 *et* 714.

2. En déduire le PGCD, le PPCM ainsi que tous les diviseurs communs positifs de 1806 *et* 714.

Exercice 2.4. *1. Appliquer l'algorithme d'Euclide à* $a = 90$ *et* $b = 77$ *et déterminer deux entiers* u *et* v *tels que* $au + bv = 1$.

2. Vérifier qu'il n'y a pas unicité du couple $(u; v)$.

3. Résoudre dans $\mathbb{Z}^2$ *l'équation* $90x + 77y = 1$.

4. Résoudre dans $\mathbb{Z}^2$ *l'équation* $90x + 77y = 5$.

Exercice 2.5. *1. Dans la division euclidienne d'un nombre par* 69*, le reste est* 35*. Dans la division euclidienne par* 75*, le quotient est le même et le reste est* 17*. Quel est ce nombre ?*

2. Lorsqu'on effectue la division euclidienne de 2011 *par l'entier naturel* b*, le quotient est* 29*. Déterminer les valeurs possibles du diviseur* b *et du reste* r.

Exercice 2.6. *Pour tout entier naturel* n*, on considère les nombres* $a = 2n^2-7n-4$ *et* $b = n^2-n-12$*. On souhaite déterminer* $PGCD(a; b)$.

1. *On pose* $\alpha = 2n + 1$ *et* $\beta = n + 3$ *et on note* $\delta = PGCD(\alpha; \beta)$.
   Justifier que $PGCD(a; b) = |n - 4|\delta$.
2. *À l'aide des combinaisons linéaires* $2\beta - \alpha = 5$ *et* $\alpha - \beta = n - 2$*, démontrer que* $\delta = 5$ *si* $n - 2$ *est un multiple de* 5 *et* $\delta = 1$ *sinon.*
3. *En utilisant les résultats précédents, exprimer le nombre* $PGCD(a; b)$.

Exercice 2.7. *Résoudre sur* $\mathbb{N}$ *le système* $\begin{cases} PGCD(x; y) = 5 \\ PPCM(x; y) = 450 \end{cases}$

Exercice 2.8. *Résoudre sur* $\mathbb{N}$ *le système* $\begin{cases} x + y = 180 \\ PGCD(x; y) = 12 \end{cases}$

Exercice 2.9. *Soit* P *un polynôme à coefficients entiers, unitaire et de degré* n *supérieur ou égal à* 1*. Démontrer que si une racine de* P *est un nombre rationnel, alors c'est un nombre entier.*

3 Primalité

Exercice 3.1. *Le «petit théorème» de Fermat est le suivant : si* p *est un nombre premier, alors pour tout entier* a *non divisible par* p *on a la congruence*

$$a^{p-1} \equiv 1 \pmod{p}.$$

1. *Montrer, à l'aide du théorème de Gauss, que* p *divise le coefficient binomial* $\binom{p}{k} = \frac{p!}{(p-k)!k!}$ *pour tout entier* $1 \leqslant k \leqslant p - 1$.
2. *En déduire, pour tout entier* a*, la congruence*

$$(1 + a)^p \equiv 1 + a^p \pmod{p}.$$

3. *Démontrer par récurrence que, pour tout entier* a *:*

$$a^p \equiv a \pmod{p}.$$

4. *En déduire le théorème.*

Exercice 3.2. *Le théorème de Wilson est le suivant : si* p *est un nombre premier, alors*

$$(p - 1)! \equiv -1 \pmod{p}.$$

1. *Démontrer que pour tout entier* $1 \leqslant x \leqslant p - 1$*, il existe un entier* y *tel que* $xy \equiv 1 \pmod{p}$.
2. *Justifier qu'un tel entier* y *est unique dans* $[1; p - 1]$*. Que représente* y *pour* x *dans* $\mathbb{Z}/p\mathbb{Z}$ *?*
3. *Résoudre* $x^2 \equiv 1 \pmod{p}$*. Que représentent les solutions dans* $\mathbb{Z}/p\mathbb{Z}$ *?*
4. *Démontrer le théorème de Wilson.*

Préparation à l'agrégation interne de mathématiques - Année 2011
Arithmétique dans $\mathbb{Z}$ - Résultats de base - Mercredi 08 juin 2011

Je renvoie aux livres [Mon06] et [WAC+02] pour plus de détails et de démonstrations.

1 Divisibilité dans $\mathbb{Z}$, congruences

Proposition 1.1.

1. *Un sous-ensemble non-vide de $\mathbb{N}$ possède un plus petit élément.*
2. *Un sous-ensemble non-vide et minoré de $\mathbb{Z}$ possède un plus petit élément.*
3. *Quels que soient l'entier naturel b non nul et l'entier naturel a, il existe un entier naturel n tel que $a < nb$. ($\mathbb{N}$ est* archimédien*).*

Une liste de définitions/vocabulaires :

1. Un entier b divise un entier a (on note $b|a$) s'il existe un nombre entier k tel que $a = b \times k$.
2. L'ensemble $\mathcal{D}_a$ des diviseurs positifs d'un entier a est non vide (et fini si a est non nul).
3. L'entier a est *premier* si $\mathcal{D}_a$ contient exactement deux éléments (qui sont alors 1 et $|a|$).
4. L'ensemble des multiples de a est $a\mathbb{Z}$.
5. La notion de diviseur commun, de multiple commun à deux (ou plus) nombres est naturelle.
6. Deux entiers a et b (ou plus...) sont *premiers entre eux* si $\mathcal{D}_a \cap \mathcal{D}_b = \{1\}$.

Propriété 1.1. *Si c divise a et b, alors c divise toutes les combinaisons linéaires $\alpha a + \beta b$ avec α et β entiers relatifs.*

Propriété 1.2 (Sur l'existence des nombres premiers).

1. *Tout nombre entier naturel $n \geqslant 2$ admet pour diviseur un nombre premier.*
2. *Tout nombre entier naturel $n \geqslant 2$ non premier admet un diviseur premier p vérifiant $p^2 \leqslant n$.*
3. *L'ensemble des nombres premiers est infini.*

Théorème 1.1 (Division euclidienne). *Soient a et b deux entiers avec $b \neq 0$.*
Il existe un unique couple $(q; r)$ (quotient ; reste) d'entiers vérifiant :

$$a = bq + r \ \textbf{\textit{et}}\ 0 \leqslant r < |b|.$$

Définition 1.1. *Deux entiers relatifs a et b sont dits* congrus modulo l'entier n *si n divise $b - a$.*
On note $a \equiv b \pmod{n}$.

Remarque 1.1. *Il est équivalent de dire que a et b ont même reste dans la division euclidienne par n (si $n \neq 0$).*

Propriété 1.3. *La congruence est compatible avec les opérations usuelles ($+$; $-$; $\times$; exponentiation).*

La congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$ constituée de n classes (si $n > 0$). L'ensemble quotient est (l'anneau) $\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}; \overline{1}; \ldots; \overline{n-1}\right\}$.

2 Décomposition, $PGCD$, $PPCM$, Euclide, Bézout, Gauss

Théorème 2.1 (**Décomposition en produit de facteurs premiers**). *Tout entier naturel $n \geqslant 2$ peut s'écrire de façon unique comme un produit :*

$$n = \prod_{i=1}^{i=m} p_i^{\alpha_i} = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$$

où $p_1, p_2, \dots, p_m$ sont des nombres premiers vérifiant $2 \leqslant p_1 < p_2 < \dots < p_m$
et $\alpha_1, \alpha_2, \dots, \alpha_m$ sont des nombres entiers naturels non nuls.

Les deux définitions suivantes ne sont pas les plus habituelles mais ont l'avantage de ne pas nécessiter d'hypothèses de non-nullité sur a et b.

Propriété et définition 2.1 (**Plus Grand Commun Diviseur**). *Soient a et b deux entiers relatifs. Il existe un unique entier naturel $\delta = PGCD(a;b) = PGCD(b;a)$ vérifiant :*

- *δ est un diviseur commun à a et b ;*
- *tout autre diviseur commun à a et b divise δ.*

Si a et b sont non nuls, le nombre $PGCD(a;b)$ est le dernier reste non nul obtenu en appliquant l'algorithme d'Euclide aux entiers a et b.

Propriété et définition 2.2 (**Plus Petit Commun Multiple**). *Soient a et b deux entiers relatifs. Il existe un unique entier naturel $\mu = PPCM(a;b) = PPCM(b;a)$ vérifiant :*

- *μ est un multiple commun à a et b ;*
- *tout autre multiple commun à a et b est un multiple de μ.*

Remarque 2.1. *Le nombre $\mu = PPCM(a;b)$ vérifie $a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}$.*

Théorème 2.2 (**Bézout**). *Soient a et b deux entiers relatifs.*

1. *il existe des entiers relatifs u et v tels que $au + bv = PGCD(a;b)$.*
2. *(Corollaire) Les entiers a et b sont premiers entre eux si et seulement s'il existe des entiers relatifs u et v tels que $au + bv = 1$.*

Propriété 2.1. *Soient a, b, c, d et k des entiers relatifs.*

1. *Si $a|c$ et $b|d$, alors $PGCD(a;b)|PGCD(c;d)$ et $PPCM(a;b)|PPCM(c;d)$.*
2. *$PGCD(ka;kb) = |k| \times PGCD(a;b)$ et $PPCM(ka;kb) = |k| \times PPCM(a;b)$*
3. *$PGCD(a;b) \times PPCM(a;b) = |ab|$*

Théorème 2.3 (**Gauss**). *Soient a, b et c trois entiers relatifs.*

1. $\left.\begin{array}{r} a \mid bc \\ PGCD(a;c) = 1 \end{array}\right\} \Longleftrightarrow a \mid b$
2. *Plus généralement : si $PGCD(a;c) = 1$ alors $PGCD(a;bc) = PGCD(a;b)$.*
3. *(Corollaire) Un nombre premier p divise ab si et seulement si p divise a ou p divise b.*

Références

[Mon06] Jean-Marie Monier. *Algèbre MPSI, Cours, méthodes et exercices corrigés, 4^{e}édition.* J'intègre. Dunod, Paris, 2006.

[WAC+02] André Warusfel, Paul Attali, Michel Collet, Christian Gautier, and Serge Nicolas. *Arithmétique.* Mathématiques, Cours et exercices TS. Vuibert, Paris, 2002.

Préparation à l'agrégation interne de mathématiques - Année 2011
Arithmétique dans $\mathbb{Z}$ - Éléments de correction

1 Divisibilité dans $\mathbb{Z}$, congruences

Exercice 1.1.
1. *Deux entiers consécutifs sont premiers entre eux car tout diviseur commun divise* $(n+1)-n=1$.
2. *Deux entiers impairs consécutifs sont premiers entre eux car tout diviseur commun divise* $(2n+1)-(2n-1)=2$ *sans pouvoir être pair.*
3. *Les entiers* $3n+5$ *et* $2n+3$ *sont premiers entre eux car tout diviseur commun divise* $2(3n+5)-3(2n+3)=1$.

Exercice 1.2. $\frac{5n^2+3n+2}{n+3}$ *est un entier si et seulement si* $n+3$ *divise* $(5n^2+3n+2)-(5n-12)(n+3)=38$ *donc si et seulement si* $n+3\in\{\pm1;\pm2;\pm19;\pm38\}$. *On trouve ainsi les valeurs possibles de* n.

Exercice 1.3. $n^2-25=(n+5)(n-5)$ *est premier seulement si* $n+5=-1$ *ou* $n+5=1$ *(impossible car* $n\geqslant 0$*) ou* $n-5=-1$ *(mais alors* $n^2-25=-9$ *n'est pas premier) ou* $n-5=1$ *(et alors* $n^2-25=11$ *est premier).*
Donc 11 *est le seul nombre premier de la liste.*

Exercice 1.4.
1. $a^2-b^2=12\Leftrightarrow(a+b)(a-b)=12$. *On liste les diviseurs positifs* $(a,b\in\mathbb{N})$ *de 12 et on teste. Seul* $(4;2)$ *est solution.*
2. $a^2-b^2=2011\Leftrightarrow\left\{\begin{array}{l}a+b=2011\\a-b=1\end{array}\right.\Leftrightarrow(a;b)=(1006;1005)$.
3. *Si* $a^2-b^2=(a+b)(a-b)$ *est pair, alors l'un des deux facteurs l'est donc l'autre également car* $a+b=(a-b)+2b$.
4. *L'entier* 162 *est pair mais n'est pas divisible par 4 donc l'équation n'admet pas de solutions entières.*

Exercice 1.5.
1. $\dfrac{2^{pq}-1}{2^p-1}=\displaystyle\sum_{k=0}^{q-1}(2^p)^k\in\mathbb{N}$
2. *Si* $n=pq$ *est composé* $(p,q\neq1)$, *alors* $M_n=2^{pq}-1$ *est divisible par* $M_p=2^p-1>1$ *donc n'est pas premier. Il faut donc que* n *soit premier. Mais* $M_{11}=2047=23\times89$.

Exercice 1.6. *Supposons* $\varphi=\frac{p}{q}$ *avec* $0<q<p$ *entiers et* p *minimal vérifiant cette égalité. Alors* $\varphi=\frac{1}{\varphi-1}=\frac{q}{p-q}$. *Donc* q *est un numérateur strictement inférieur à* p. *Contradiction.*

Exercice 1.7. *Calculs modulo* 4.

1. *La table de multiplication dans* $\mathbb{Z}/4\mathbb{Z}$.

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

2. *Sur la diagonale (les carrés), on ne lit que* 0 *ou* 1 *d'où les valeurs possibles pour la somme.*
3. *Puisque* $2011\equiv3\pmod4$, *l'équation* $a^2+b^2=2011$ *n'admet pas de solutions entières. (Attention, la congruence à* 0, 1 *ou* 2 *n'est pas suffisante pour l'existence de solutions. Voir le théorème des deux carrés.)*
4. *Puisque* $x^2\equiv0$ *ou* $1\pmod4$, *alors* $a^2-b^2\equiv0$ *ou* 1 *ou* $3\pmod4$ *ne peut être congru à* 2 *modulo* 4.

Exercice 1.8. *Calculs modulo* 5.

1. *La table de multiplication dans* $\mathbb{Z}/5\mathbb{Z}$.
2. *D'après la diagonale (les carrés) l'équation* $x^2+1\equiv 0 \pmod 5$ *admet pour solutions tous les entiers de la forme* $2+5k$ *ou* $3+5k$, k *entier.*
3. *Puisque* $13\equiv 3 \pmod 5$ *et* $3^0\equiv 1 \pmod 5$, $3^1\equiv 3 \pmod 5$, $3^2\equiv 4 \pmod 5$, $3^3\equiv 2 \pmod 5$ *et* $3^4\equiv 1 \pmod 5$ *(voir exercice 3.1), on note* r *le reste de* n *modulo* 4 *et on a :*

$$13^n\equiv 3^n\equiv 3^{4q+r}\equiv \left(3^4\right)^q\times 3^r\equiv 3^r \pmod 5$$

donc le reste de 13^n *dans la divion euclidienne par* 5 *est* $1,3,4,2$ *selon que* r *est respectivement égal à* $0,1,2,3$.

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Exercice 1.9. *On a* $7^4\equiv 1 \pmod{10}$ *donc* $7^{2011}\equiv 7^{4\times 502+3}\equiv 7^3\equiv 3 \pmod{10}$ *donc le chiffre des unités de* 7^{2011} *est un* 3. *Et le chiffre des dizaines est un* 4 *(car* $7^4\equiv 1 \pmod{100}$, *même principe).*

2 Décomposition, $PGCD$, $PPCM$, Euclide, Bézout, Gauss

Exercice 2.1. *Les réels* $\frac{a}{\delta}$ *et* $\frac{b}{\delta}$ *sont deux entiers car* δ *est un diviseur commun de* a *et* b. *Si* d *est un diviseur positif commun de* $\frac{a}{\delta}$ *et* $\frac{b}{\delta}$ *alors* $a=d\delta\alpha$ *et* $b=d\delta\beta$ *(*α,β *entiers). Donc* a *et* b *sont divisibles par* $d\delta$ *ce qui implique que* $d\delta|\delta$ *d'où* $d=1$.

Exercice 2.2.

1. $2600=2^3\times 5^2\times 13$
2. *Les diviseurs positifs de* $2600=2^3\times 5^2\times 13$ *sont les entiers de la forme* $2^{\alpha_2}\times 5^{\alpha_5}\times 13^{\alpha_{13}}$ *avec* $0\leqslant\alpha_2\leqslant 3$, $0\leqslant\alpha_5\leqslant 2$ *et* $0\leqslant\alpha_{13}\leqslant 1$. *Il y en a donc* $(3+1)(2+1)(1+1)=24$.
3. *D'après le raisonnement précédent un entier naturel admet exactement* $35=34+1=5\times 7=(4+1)(6+1)$ *diviseurs positifs si et seulement si sa décomposition est de la forme* p^{34} *ou* p^4q^6 *avec* p *et* q *deux nombres premiers distincts. Les plus petits sont* $2^6.3^4=5184$, $2^4.3^6=11664$, $2^6.5^4=40000$.
4. *Un entier non nul admet un nombre impair de diviseurs positifs si et seulement si tous les exposants de sa décomposition sont pairs.*

Exercice 2.3.

1. *Algorithme d'Euclide appliqué aux nombres* 1806 *et* 714 *:*

$$\begin{aligned} 1806 &= 2\times 714 + 378\\ 714 &= 1\times 378 + 336\\ 378 &= 1\times 336 + 42\\ 336 &= 8\times 42 + 0 \end{aligned}$$

2. *On a* $PGCD(1806;714)=42$, $PPCM(1806;714)=\frac{1806\times 714}{42}=30702$. *Les diviseurs communs de* 1806 *et* 714 *sont les diviseurs de* $PGCD(1806;714)=42$ *:* $\mathcal{D}_{1806}\cap\mathcal{D}_{714}=\mathcal{D}_{42}=\{1;2;3;6;7;14;21;42\}$.

Exercice 2.4.

1. *Algorithme d'Euclide appliqué aux nombres* 90 *et* 77 *:*

$$\begin{aligned} 90 &= 1\times 77 + 13\\ 77 &= 5\times 13 + 12\\ 13 &= 1\times 12 + 1\\ 12 &= 12\times 1 + 0 \end{aligned}$$

Donc $PGCD(90;77)=1=13-1\times 12=13-1\times(77-5\times 13)=6\times 13-1\times 77=6(90-77)-77=6\times 90-7\times 77$. *Le couple* $(6;-7)$ *convient.*

2. *Le couple* $(6+77;-7-90)$ *est aussi solution.*
3. *Soit* $(x;y)$ *une solution de* $77x+13y=1$, *on a alors :*

$$\begin{aligned} 90x+77y &= 1\\ 90x+77y &= 6\times 90-7\times 77\\ 90(x-6) &= -77(y+7) \end{aligned}$$

Les nombres x et y sont entiers donc 77 divise $90(x-6)$. Puisque 77 et 90 sont premiers entre eux, le théorème de Gauss affirme que 77 divise $x-6$: il existe un entier k tel que $x=6+77k$. On en déduit que $y=-7+90k$.
Réciproquement, pour tout entier k, le couple $(6+77k;-790k)$ est solution.
Donc l'ensemble des solutions est $\mathcal{S}=\{(6+77k;-7-90k)\ :\ k\in\mathbb{Z}\}$

4. *Même méthode : $\mathcal{S}'=\{(30+77k;-35-90k)\ :\ k\in\mathbb{Z}\}$.*

Exercice 2.5. 1. *Si a est le nombre recherché, alors $a=69q+35$ et $a=75q+17$. On en déduit la valeur $q=\frac{35-17}{75-69}=3$ puis la valeur $a=69\times 3+35=242$.*

2. *On peut écrire $2009=b\times 29+r$ avec $0\leqslant r<b$. On en déduit l'encadrement $29b+0\leqslant 2009<29b+b$ qui permet d'obtenir $29b\leqslant 2009<30b$. Le diviseur b étant entier, il est égal à 67, 68 ou 69. Le reste est alors égal à, respectivement 66, 37 ou 8.*

Exercice 2.6. 1. *On a $a=\alpha(n-4)$ et $b=\beta(n-4)$ donc $\delta=PGCD(a;b)=|n-4|PGCD(\alpha;\beta)$.*

2. *L'entier δ est le PGCD de α et β donc il divise $2\beta-\alpha=5$ et $\alpha-\beta=n-2$.*
   - *Si 5 ne divise pas $n-2$, alors $\delta=1$.*
   - *Si 5 divise $n-2$, alors 5 divise $2(n-2)+5=\alpha$ et $(n-2)+5=\beta$. Donc $\delta=5$.*

3. *On obtient donc* $PGCD(2n^2-7n-4;n^2-n-12)=\begin{cases}5|n-4| & \text{si } n\equiv 2 \pmod 5\\ |n-4| & \text{sinon}\end{cases}$.

Exercice 2.7. *On a $PPCM(x;y)=2^1\times 3^2\times 5^2$ et $PGCD(x;y)=2^0\times 3^0\times 5^1$ donc $x=2^0\times 3^0\times 5^1=5$ et $y=450$ ou $x=2^1\times 3^0\times 5^1=10$ et $y=225$ ou $x=2^0\times 3^2\times 5^1=45$ et $y=50$ ou $x=2^1\times 3^2\times 5^1=90$ et $y=25$ ou ...*

Exercice 2.8. *En posant $x'=x/12$ et $y'=y/12$, on obtient le système* $\begin{cases}x'+y'=15\\ PGCD(x';y')=1\end{cases}$ *dont les solutions sont (pour x') : $1,2,4,7,8,11,13,14$. On obtient ensuite $(x;y)$.*

Exercice 2.9. *Notons $P(X)=X^n+a_{n-1}X^{n-1}+\ldots+a_0$ le polynôme. Si $\frac{p}{q}$ (que l'on supposera écrite sous forme irréductible : $PGCD(p;q)=1$) est une racine rationnelle de P, alors*

$$\begin{aligned}\left(\frac{p}{q}\right)^n+a_{n-1}\left(\frac{p}{q}\right)^{n-1}+\ldots+a_1\left(\frac{p}{q}\right)+a_0 &= 0\\ p^n+a_{n-1}p^{n-1}q+\ldots+a_1pq^{n-1}+a_0q^n &= 0\\ q\left(a_{n-1}p^{n-1}+\ldots+a_1pq^{n-2}+a_0q^{n-1}\right) &= -p^n\end{aligned}$$

Donc p^n est divisible par q. Ce qui implique (Gauss et récurrence) que $q=1$. Donc $\alpha=p$ est entier.

3 Primalité

Exercice 3.1. 1. *Le nombre p divise $(p-k)!k!\binom{p}{k}=p!$ et est premier avec $(p-k)!k!$ si $1\leqslant k\leqslant p-1$. Donc (Gauss) p divise $\binom{p}{k}$.*

2. *Formule du binôme :*

$$(1+a)^p\equiv\sum_{k=0}^{k=p}\binom{p}{k}a^k\equiv 1+\underbrace{\sum_{k=1}^{k=p-1}\binom{p}{k}a^k}_{\equiv 0 \pmod p}+a^p\equiv 1+a^p \pmod p.$$

3. *Si $a=0$, alors $0^p\equiv 0 \pmod p$. Si $a^p\equiv a \pmod p$, alors $(a+1)^p\equiv a^p+1\equiv a+1 \pmod p$.*

4. *La congruence $a\left(a^{p-1}-a\right)\equiv a^p-a\equiv 0 \pmod p$ montre que p divise $a\left(a^{p-1}-a\right)$. Si p ne divise pas a, p est premier avec a donc divise $a^{p-1}-a$.*

Exercice 3.2. *Le théorème de Wilson est le suivant : si p est un nombre premier, alors*

$$(p-1)! \equiv -1 \pmod{p}.$$

1. *Si $1 \leqslant x \leqslant p-1$, alors x est premier avec p donc (Bézout), il existe y et z entiers tels que $xy + zp = 1$ ce qui s'écrit aussi $xy \equiv 1 \pmod{p}$.*
2. *Quitte à remplacer y par son résidu modulo p, on peut supposer que $1 \leqslant y \leqslant p-1$. Pour l'unicité : si y_1 et y_2 sont deux candidats, alors $x(y_1 - y_2) \equiv 1 - 1 \equiv 0 \pmod{p}$ donc p divise $y_1 - y_2$ (Gauss). Mais $-p + 2 \leqslant y_1 - y_2 \leqslant p - 2$ donc $y_1 = y_2$.*
   L'entier y (ou plutôt sa classe) est l'inverse de (la classe de) x dans le corps $\mathbb{Z}/p\mathbb{Z}$.
3. *$x^2 \equiv 1 \pmod{p} \Leftrightarrow (x+1)(x-1) \equiv 0 \pmod{p} \Leftrightarrow x \equiv -1 \pmod{p}$ ou $x \equiv 1 \pmod{p}$.*
   Les solutions sont les éléments de $\mathbb{Z}/p\mathbb{Z}$ égaux à leur inverse (les éléments d'ordre 2).
4. *Dans le produit $(p-1)!$, distinguons 1 et $p-1$ (qui sont leur propre inverse modulo p) et les autres facteurs $2, \ldots, p-2$. Pour chacun des nombres de cette dernière liste, son inverse est également présent. Donc*

$$(p-1)! \equiv 1 \times \left(\prod_{x=2}^{p-2} x \right) \times (p-1) \equiv 1 \times 1^{\frac{p-1}{2}} \times (p-1) \equiv p - 1 \equiv -1 \pmod{p}.$$