Département de mathématiques et de statistique
Université de Montréal
Mathématiques discrètes. Mat 1500. Examen intra 2
Le 4 avril 2013. 13h30-15h20
Professeure: Matilde N. Lalín

1. Aucun document ni calculatrice ni autres instruments ne sont autorisés.
2. Les téléphones cellulaires doivent être éteints.
3. Lire attentivement les questions avant de commencer à travailler.
4. Répondre à toutes les questions en **justifiant** vos réponses.
5. Répondre à toutes les questions dans les cahiers d'examen.
6. Éviter de déchirer les cahiers d'examen.
7. Le total des points de cet examen vaut 25 (il y a 1 point additionnel).

---

1. (a) (2 points) Trouver un inverse de 7 modulo 20 en utilisant l'algorithme d'Euclide.

   (b) (1 point) Résoudre l'équation

$$7x \equiv 5 \pmod{20}.$$

Solution: (a) 7 a un inverse modulo 20 parce que $\text{pgcd}(7, 20) = 1$. Pour le trouver, on utilise l'algorithme d'Euclide

$$\begin{aligned} 20 &= 7 \cdot 2 + 6 \\ 7 &= 6 \cdot 1 + 1 \\ 6 &= 1 \cdot 6. \end{aligned}$$

Alors, on trouve

$$\begin{aligned} 1 &= 7 - 6 \\ &= 7 - (20 - 7 \cdot 2) = 3 \cdot 7 - 20 \end{aligned}$$

Par conséquent, un inverse de 7 modulo 20 est 3. C'est-à-dire,

$$3 \cdot 7 \equiv 1 \pmod{20}.$$

(b) En multipliant par 3, on trouve,

$$3 \cdot 7x \equiv 3 \cdot 5 \pmod{20}.$$

Alors,

$$x \equiv 15 \pmod{20}.$$

2. (4 points) Trouver (avec preuve) un entier $0 \leq k < 17$ tel que

$$4^{162} \equiv k \pmod{17}.$$

Solution: On trouve les congruences des premiers puissances de 4 modulo 17:

$$\begin{aligned} 4 &\equiv 4 \pmod{17} \\ 4^2 &\equiv 16 \pmod{17} \\ 4^3 &\equiv 64 \equiv 13 \pmod{17} \end{aligned}$$

$$\begin{aligned} 4^4 &\equiv 52 \equiv 1 \pmod{17} \\ 4^5 &\equiv 4 \pmod{17}. \end{aligned}$$

On voit donc que le cycle se repète avec longuer 4. On trouve de plus que $162 = 4 \cdot 40 + 2$. Alors,

$$4^{162} = 4^{4 \cdot 40 + 2} = (4^4)^{40} \cdot 4^2 \equiv 1 \cdot 16 \pmod{17}.$$

Par conséquent, $k = 16$.

Solution: Comme $\mathrm{pgcd}(4, 17) = 1$, et 17 est premier, on a, par le petit théorème de Fermat,

$$4^{16} \equiv 1 \pmod{17}.$$

On trouve que $162 = 16 \cdot 10 + 2$. Alors,

$$4^{162} = 4^{16 \cdot 10 + 2} = (4^{16})^{10} \cdot 4^2 \equiv 1 \cdot 16 \pmod{17}.$$

Par conséquent, $k = 16$.

Solution: Comme 17 est premier, on a, par le petit théorème de Fermat,

$$4^{17} \equiv 4 \pmod{17}.$$

On trouve que $162 = 17 \cdot 9 + 9$. Alors,

$$4^{162} = 4^{17 \cdot 9 + 9} = (4^{17})^9 4^9 \equiv 4^{9+9} \equiv 4^{17+1} \equiv 4^2 \equiv 16 \pmod{17}.$$

Par conséquent, $k = 16$.

Solution: On trouve les congruences des premiers puissances de 4 modulo 17:

$$\begin{aligned} 4 &\equiv 4 \pmod{17} \\ 4^2 &\equiv 16 \equiv -1 \pmod{17} \end{aligned}$$

Alors,
$$4^{162} = (4^2)^{81} \equiv (-1)^{81} \equiv -1 \equiv 16 (\operatorname{mod} 17).$$
Par conséquent, $k = 16$.

3. Rappelons que l'alphabet français contient 20 consonnes et 6 voyelles pour un total de 26 lettres. Combien de chaînes de lettres de longeur 5 est-il possible de former avec l'alphabet français si
   (a) (1 point) chaque chaîne doit contenir exactement 1 voyelle?
   (b) (1 point) chaque chaîne doit contenir au moins 2 voyelles?
   (c) (1 point) chaque chaîne doit contenir exactement deux lettres identiques?

   Pour cette question, les produits et les coefficients binomiaux peuvent être laissés tel quels. Il n'est pas nécessaire de les simplifier.

Solution: (a) On choisit les places pour la voyelle de 5 façons. On choisit la voyelle de 6 façons et les consonnes de 20^4 façons. Alors, la réponse est donné par
$$5 \cdot 6 \cdot 20^4.$$

(b) Il y a un total de 26^5 chaînes dont 20^5 avec aucune voyelle et $5 \cdot 6 \cdot 20^4$ avec exactement une voyelle. Par conséquent, il y a
$$26^5 - 20^5 - 5 \cdot 6 \cdot 20^4$$
chaînes avec au moins deux voyelles.

Autre possibilité est de compter les chaînes avec deux voyelles, trois voyelles, quatre voyelles, et cinq voyelles.
$$\binom{5}{2} 6^2 \cdot 20^3 + \binom{5}{3} 6^3 \cdot 20^2 + \binom{5}{4} 6^4 \cdot 20 + 6^5.$$

(c) On choisit la lettre qui va se répeter de 26 façons et les places pour cette lettre de $\binom{5}{2}$ façons. Après, on choisit les lettres pour les autres places de $25 \cdot 24 \cdot 23$ façons, car elles ne peuvent se répeter et elles doivent être différentes de la lettre répetée. Le total est
$$\binom{5}{2} \cdot 26 \cdot 25 \cdot 24 \cdot 23 = \binom{5}{2} P(26, 4).$$

4. Soit n un entier plus grand ou égal à 1.

(a) (1 point) Combien y a-t-il de fonctions $f : \{1, \ldots, n\} \to \{1, 2, 3\}$?

(b) (1 point) Combien y a-t-il de fonctions injectives $f : \{1, \ldots, n\} \to \{1, 2, 3\}$?

(c) (1 point) Combien y a-t-il de fonctions surjectives $f : \{1, \ldots, n\} \to \{1, 2\}$?

Solution: (a) Comme à chaque entier entre 1 et n il faut lui corresponder un nombre entre 1 et 3, il y a 3^n fonctions.

(b) Si $n > 3$, il n'y a pas de fonctions injectives. Si $n = 3$, il y a $3! = 6$ fonctions injectives. Si $n = 2$ il y a $3 \cdot 2 = 6$ fonctions injectives Si $n = 1$ il y a 3 fonctions injectives.

(c) Supposons d'abord que $n \geq 2$. Il y a une fonction $f : \{1, \ldots, n\} \to \{1\}$ et une fonction $f : \{1, \ldots, n\} \to \{2\}$. Les autres fonctions sont surjectives. Le total de fontions $f : \{1, \ldots, n\} \to \{1, 2\}$ est 2^n. Alors, on trouve $2^n - 2$ fonctions surjectives. Si $n = 1$, il n'y a pas de fonctions surjectives.

5. (4 points) Prouver que si n est un entier plus grand ou égal à 1, alors,

$$\sum_{k=0}^{n} C(n, k)2^k = 3^n$$

Solution: On peut écrire

$$\sum_{k=0}^{n} C(n, k)2^k = \sum_{k=0}^{n} C(n, k)2^k 1^{n-k} = (2 + 1)^n = 3^n$$

par le théorème du binôme.

Solution: Soit $P(n) : \sum_{k=0}^{n} C(n, k)2^k = 3^n$.

1) On a $\sum_{k=0}^{1} C(1, k)2^k = C(1, 0)2^0 + C(1, 1)2^1 = 1 + 2 = 3 = 3^1$, donc $P(1)$ est V.

2) Supposons que $P(n)$ est V. Alors,

$$\sum_{k=0}^{n+1} C(n + 1, k)2^k = C(n + 1, 0)2^0 + \sum_{k=1}^{n} C(n + 1, k)2^k + C(n + 1, n + 1)2^{n+1}.$$

Par l'identité de Pascal,

$$= \quad 1 + \sum_{k=1}^{n} (C(n, k) + C(n, k - 1)2^k + 2^{n+1}$$

$$\begin{aligned}
&= 1+\sum_{k=1}^{n} C(n,k)2^k + \sum_{k=1}^{n} C(n,k-1)2^k + 2^{n+1} \\
&= \sum_{k=0}^{n} C(n,k)2^k + \sum_{k=0}^{n-1} C(n,k)2^{k+1} + 2^{n+1} \\
&= 3^n + 2\left(\sum_{k=0}^{n-1} C(n,k)2^k + 2^n\right) \\
&= 3^n + 2\cdot 3^n \\
&= 3^{n+1}.
\end{aligned}$$

Donc, $P(n) \Rightarrow P(n+1)$. Par le principe de l'induction, $P(n)$ est V pour $n \geq 1$.

(On fait, c'est V pour $n \in \mathbb{N}$.)

6. Demontrer que
   (a) (1 point) $1+2+\ldots+n = \frac{n(n+1)}{2}$ pour tout n entier plus grand ou égal à 1.
   (b) (3 points) $2^n < n!$ pour tout n entier plus grand ou égal à 4.

Solution: (a) Soit $P(n) : 1+2+\ldots+n = \frac{n(n+1)}{2}$.

1) On a: $1 = \frac{1(1+1)}{2}$, donc $P(1)$ est V.

2) Supposons que $P(n)$ est V. Alors,

$$1+2+\ldots+n+(n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2},$$

donc, $P(n) \Rightarrow P(n+1)$. Pas conséquent, $P(n)$ est V pour $n \geq 1$ par le principe de l'induction.

(b) Soit $P(n) : 2^n < n!$.

1) On a $2^4 = 16 < 24 = 4!$, donc $P(4)$ est V.

2) Supposons que $P(n)$ est V. Notons que $2 < n+1$ si $n \geq 4$. Alors,

$$2^{n+1} = 2\cdot 2^n < 2\cdot n! \leq (n+1)n! = (n+1)!$$

donc, $P(n) \Rightarrow P(n+1)$. Pas conséquent, $P(n)$ est V pour $n \geq 4$ par le principe de l'induction.

Solution: (a) Soit n pair, alors $n = 2k$ avec $k \geq 1$. On met les nombres en des couples $\{1, 2k\}, \{2, 2k-1\}, \ldots, \{k-1, k+2\}, \{k, k+1\}$. Observe que $1 + 2k = 2 + (2k-1) = \ldots = (k-1) + (k+2) = k + (k+1) = 2k+1$. Alors, la somme $1 + 2 + \ldots + n$ est égale à

$$k(2k+1) = \frac{n(n+1)}{2}.$$

Maintenant supposons que n impair et on écrit $n = 2k-1$ avec $k \geq 1$. On met les nombres en des couples $\{1, 2k-1\}, \{2, 2k-2\}, \ldots, \{k-1, k+1\}$, et $\{k\}$ qui reste seul. On a que $1 + (2k-1) = 2 + (2k-2) = \ldots = (k-1) + (k+1) = 2k$. Alors, la somme $1 + 2 + \ldots + n$ est égale à

$$(k-1)2k + k = (2(k-1)+1)k = (2k-1)k = \frac{n(n+1)}{2}.$$

Comment on a consideré les deux cas, on a prouvé l'identité pour $n \geq 1$.

Autre forme es de trouver la somme de $2(1 + \ldots + n) = (1+n) + (2+n-1) + \ldots + (n-1+2) + (n+1)$. Il y a n termes et chaqun est égale à $n+1$. Par conséquent le total est $n(n+1)$. On divise par 2 dans les deux côtés pour obtenir l'égalité.

(b) On a que $2^4 = 16 < 24 = 4!$. Si $n > 4$, on écrit

$$2^n = 2^4 \cdot 2^{n-4} = 16 \cdot \underbrace{2 \cdot 2 \cdots 2}_{n-4} < 24 \cdot 5 \cdot 6 \cdots (5 + n - 5) = n!$$

On a prouvé l'inégalité pour $n \geq 4$.

7. On suppose que l'ensemble de tous les étudiants en mathématiques de l'UdeM proviennent de 20 pays différents. On suppose également qu'un étudiant ne peut provenir que d'un seul pays.
   (a) (3 points) Quel est le nombre minimal d'étudiants qui doivent s'inscrire au cours de mathématiques discrètes pour être certain qu'il y ait au moins 8 étudiants qui proviennent du même pays?
   (b) (2 points) On suppose qu'il y a 209 étudiants inscrits au cours et qu'au moins un étudiant de chacun des 20 pays est inscrit au cours. Montrer qu'il y a au moins deux pays avec le même nombre d'étudiants inscrits au cours.

Solution: (a) S'il y a k étudiants dans le cours, par le théorème généralisé des nids de pigeons, on peut être certain qu'il y a au moins $\lceil \frac{k}{20} \rceil$ étudiants d'un même pays. On veut k minimal tel que $\lceil \frac{k}{20} \rceil = 8$. Alors, il faut avoir $k = 7 \cdot 20 + 1 = 141$ étudiants.

(b) Supposons qu'il y a un nombre différent d'étudiants pour chaque pays. Donc, il y a au moins $1 + 2 + \ldots + 20$ étudiants. Par le probléme 6 (a), cela donne $\frac{20 \cdot 21}{2} = 210$

étudiants au minimum. Comme il y a 209 étudiants, il faut que deux pays aient le même nombre d'étudiants.