Master of Science in Mathematics *Michel Waldschmidt* Master Training Program
Royal University of Phnom Penh RUPP URPP - Université Royale de Phnom Penh
Centre International de Mathématiques Pures et Appliquées CIMPA
Coopération Mathématique Interuniversitaire Cambodge France

MMA105: Discrete Mathematics

Main Assignment, June 4, 2009
3 hours

Exercise 1.
Let $f : E \longrightarrow F$ and $g : F \longrightarrow G$ be two maps. Assume that $g \circ f : E \longrightarrow G$ is a bijective map. For each of the four questions below, answer yes or no. If the answer is yes, give an example. If the answer is no, prove it.
a) Is-it possible to give an example where f is not injective?
b) Is-it possible to give an example where f is not surjective?
c) Is-it possible to give an example where g is not injective?
d) Is-it possible to give an example where g is not surjective?

Exercise 2.
What is the remainder of the Euclidean division of 123^{801} by each of the following numbers: 2, 3, 5, 6, 8, 9, 50, 125, 1000?

Exercise 3.
Compute, for $n \geq 0$,

$$\sum_{k=0}^{n} \binom{n}{k} 2^k \quad \text{and} \quad \sum_{k=0}^{n} \binom{n}{k} (-2)^k.$$

Exercise 4.
Find all $N \in \mathbf{Z}$ which satisfy

$$N \equiv 3 \pmod{26} \quad \text{and} \quad N \equiv 1 \pmod{57}.$$

What is the smallest such positive N?

Exercise 5.
Define u_n for $n \geq 0$ by $u_0 = 0$, $u_1 = 1$ and

$$u_{n+1} = 2u_n + u_{n-1} \qquad (n \geq 2).$$

a) Give the numerical values of u_2, u_3, u_4 and u_5. Next write a formula for u_n valid for all $n \geq 1$ and prove it.

b) Show that the limit u_{n+1}/u_n exists and compute it.
c) Write the rational fraction $f(z)$ whose Taylor expansion at the origin is

$$\sum_{n\geq 0} u_n z^n.$$

What is the radius of convergence of this series?
d) Compute, for $n \geq 1$,

$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u_n \\ u_{n-1} \end{pmatrix}, \qquad \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}^n \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}^n.$$

What is the product of the two last matrices?
Deduce, for all $n \geq 1$,

$$u_{n+1}u_{n-1} - u_n^2 = (-1)^n.$$

Exercise 6. Let K be a field and n, d two positive integers. Recall that a homogeneous polynomial of degree d in n variables is a polynomial

$$P(X_1, \ldots, X_n) = \sum c_{k_1,\ldots,k_n} X_1^{k_1} \cdots X_n^{k_n}$$

where the sum is over the set of $(k_1, \ldots, k_n) \in \mathbf{Z}^n$ with $k_j \geq 0$ for $1 \leq j \leq n$ and $k_1 + \cdots + k_n = d$.
What is the dimension of the K–vector space of homogeneous polynomial of degree d in n variable?

Exercise 7.
a) Draw a graph with nodes representing the numbers $11, 12, 13, 14, 15, 16$, in which two nodes are connected by an edge if and only if they have no common divisor larger than 1.
b) Draw a graph with nodes representing the numbers $1, 2, \ldots, 8$, in which two nodes are connected by an edge if and only if their sum is a prime number.
c) Find the number of edges and the degrees in these graphs.

Exercise 8. Let n be a positive integer. Denote by G_n the graph with nodes the divisors d of n, with $1 \leq d \leq n$, and where two nodes d_1 and d_2 are connected by an edge if and only if either
(i) d_1 divides d_2 and d_2/d_1 is a prime number,
or symmetrically
(ii) d_2 divides d_1 and d_1/d_2 is a prime number.
a) Draw G_n for $n = 1, 2, \ldots, 12$.
b) For which values of $n \geq 1$ is G_n a tree?
c) For which values of $n \geq 1$ is G_n a cycle?

Master of Science in Mathematics *Michel Waldschmidt* Master Training Program
Royal University of Phnom Penh RUPP URPP - Université Royale de Phnom Penh
Centre International de Mathématiques Pures et Appliquées CIMPA
Coopération Mathématique Interuniversitaire Cambodge France

MMA105: Discrete Mathematics

Main Assignment, June 4, 2009 — solutions

Solution exercise 1
If $h = g \circ f$ is bijective, then g is surjective and f is injective. Indeed if $f(x) = f(x')$ then $g \circ f(x) = g \circ f(x')$, and since h is injective this implies $x = x'$, which shows that f is injective. Similarly any $z \in g$ can be written $h(x)$ for some $x \in E$, hence $z = g(y)$ with $y = f(x)$, and this shows that g is surjective.

An example where f is not surjective and g is not injective is obtained with $E = \{x\}$, $F = \{y_1, y_2\}$ and $G = \{z\}$, $f(z) = y_1$, $g(y_1) = g(y_2) = z$.

Therefore the answer is no for a) and d), it is yes for b) and c).

Solution exercise 2
The remainder of the Euclidean division of 123^{801} by 1000 is 123, since $123^{400} \equiv 1 \pmod{1000}$.

As a consequence the remainder of the Euclidean division of 123^{801} by any divisor d of 1000 is the same as the remainder of the Euclidean division of 123 by d.

Hence the remainder of the division of 123^{801} by 2 is 1, by 5 is 3, by 8 is 3, by 50 is 23, by 125 is 123.

Also the number 123^{801} is divisible by 3^{801}, hence by 3 and by 9. So the remainder of the division by 3 and by 9 is 0.

Finally 123^{801} is an odd multiple of 3, hence it is congruent to 3 modulo 6. So the remainder the remainder of the division by 6 is 3.

Solution exercise 3
For $n \geq 0$,

$$\sum_{k=0}^{n} \binom{n}{k} 2^k = (1+2)^n = 3^n \quad \text{and} \quad \sum_{k=0}^{n} \binom{n}{k} (-2)^k = (1-2)^n = (-1)^n.$$

Solution exercise 4
The set of solutions is the set of integers of the form $-569 + 1482k$ with $k \in \mathbf{Z}$, the smallest positive solution is 913. Here is the proof.

The Euclidean algorithm for computing the gcd of 57 and 26 yields

$$57 = 26 \times 2 + 5, \quad 26 = 5 \times 5 + 1,$$

hence the gcd is 1 and a Bézout relation is

$$1 = 26 - 5 \times 5 = 26 - 5 \times (57 - 2 \times 26) = 11 \times 26 - 5 \times 57 = 286 - 285.$$

Write the unknown integer N as

$$N = 3 + 26u = 1 + 57v, .$$

This yields the equation $2 = 57v - 26u$. From Euclidean algorithms is follows that one solution to this equation is $u = -22$, $v = -10$ with $2 = 26 \times 22 - 57 \times 10$. This gives one solution N

$$-569 = 1 - 57 \times 10 = 3 - 22 \times 26.$$

To get all possible values of N one needs to add a multiple of $57 \times 26 = 1482$, which meanss that the set of solutions is the set of integers of the form $-569 + 1482k$. One deduces the smallest positive solution is $913 = 1482 - 569$, which satisfies

$$913 \equiv 3 \pmod{26} \qquad \text{and} \quad 913 \equiv 1 \pmod{57}.$$

Solution exercise 5
The first values are

$$u_0 = 0, u_1 = 1, u_2 = 2, u_3 = 5, u_4 = 12, u_5 = 29.$$

The associated polynomial is $X^2 - 2X - 1 = (X - 1 - \sqrt{2})(X - 1 + \sqrt{2})$, hence

$$u_n = \frac{1}{2\sqrt{2}}\left((\sqrt{2}+1)^n - (1-\sqrt{2})^n\right)$$

with

$$\lim u_{n+1}/u_n = 1 + \sqrt{2}$$

and

$$f(z) = \frac{z}{1 - 2z - z^2}.$$

The radius of convergence is $1/(1 + \sqrt{2}) = \sqrt{2} - 1$. One checks

$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u_n \\ u_{n-1} \end{pmatrix} = \begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix}, \qquad \text{hence} \quad \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{pmatrix}$$

and

$$\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}^n = (-1)^n \begin{pmatrix} u_{n-1} & -u_n \\ -u_n & u_{n+1} \end{pmatrix}$$

Since

$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

it follows that

$$\begin{pmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{pmatrix} \begin{pmatrix} u_{n-1} & -u_n \\ -u_n & u_{n+1} \end{pmatrix} = (-1)^n \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

On the other hand a direct computation gives

$$\begin{pmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{pmatrix} \begin{pmatrix} u_{n-1} & -u_n \\ -u_n & u_{n+1} \end{pmatrix} = \begin{pmatrix} u_{n-1}u_{n+1} - u_n^2 & 0 \\ 0 & u_{n-1}u_{n+1} - u_n^2 \end{pmatrix}.$$

Hence for $n \geq 1$,

$$u_{n-1}u_{n+1} - u_n^2 = (-1)^n.$$

Solution exercise 6

The dimension of the K–vector space of homogeneous polynomial of degree d in n variable is the number of $(k_1, \ldots, k_n) \in \mathbf{Z}^n$ with $k_j \geq 0$ for $1 \leq j \leq n$ and $k_1 + \cdots + k_n = d$. This is

$$\binom{d+n-1}{n-1}.$$

Let us recall the proof. Write $k_1 + \cdots + k_n = d$. Replace each k_i by $11 \ldots 11$ where the number of 1's is k_i. Then $k_1 + \cdots + k_n$ becomes a sequence of $n+k-1$ symbols, n of which are $+$'s, and the other $d-1$ are 1's. The number of sequences $(k_1, \ldots, k_n)$ of integers ≥ 0 with sum d is therefore the number of sequences of $n+k-1$ symbols, n of which are $+$, and the other $d-1$ are 1.

Solution exercise 7

a) The degrees of the nodes are respectively $5, 2, 5, 3, 4, 3$, the sum of which is 22, the number of edges is 11.

b) The degrees of the nodes are respectively $3, 3, 3, 3, 3, 3, 2, 2$, the sum of which is also 22, the number of edges is 11.

Solution exercise 8

For $n = 1$ the graph G_1 is the empty graph with one node (and no edge).

a) For $n = 2, 3, 5, 7, 11$, and more generally for n a prime p, the graph is

$$G_p \qquad\qquad p \text{ —— } 1.$$

For $n = 4, 9$, and more generally for $n = p^2$ the square of a prime number p, the graph is

$$G_{p^2} \qquad\qquad p^2 \text{ —— } p \text{ —— } 1.$$

For $n = 8$, and more generally for $n = p^s$ a power of a prime p, the graph G_{p^s} is a path with $s+1$ nodes and s edges

$$G_{p^s} \qquad p^s \text{ --- } p^{s-1} \text{ --- } \cdots \text{ --- } p^2 \text{ --- } p \text{ --- } 1.$$

Hence the graph G_{p^s} is a tree.

For $n = 6, 10$, and more generally for $n = p_1p_2$ product of two distinct prime numbers, the graph is a cycle

$$G_{p_1p_2} \qquad \begin{array}{ccc} p_1p_2 & — & p_1 \\ | & & | \\ p_2 & — & 1 \end{array}$$

The nodes of G_{12} are 1, 2, 3, 4, 6 and 12. There are 7 edges. More generally for $n = p_1^{a_1}p_2^{a_2}$ where p_1 and p_2 are two distinct prime numbers and a_1, a_2 two positive integers, the graph G_n is

$$G_{p_1^{a_1}p_2^{a_2}} \qquad \begin{array}{ccccccccc} p_1^{a_1}p_2^{a_2} & — & p_1^{a_1}p_2^{a_2-1} & — & \cdots & — & p_1^{a_1}p_2 & — & p_1^{a_1} \\ | & & | & & & & | & & | \\ p_1^{a_1-1}p_2^{a_2} & — & p_1^{a_1-1}p_2^{a_2-1} & — & \cdots & — & p_1^{a_1-1}p_2 & — & p_1^{a_1-1} \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ p_1p_2^{a_2} & — & p_1p_2^{a_2-1} & — & \cdots & — & p_1p_2 & — & p_1 \\ | & & | & & & & | & & | \\ p_2^{a_2} & — & p_2^{a_2-1} & — & \cdots & — & p_2 & — & 1 \end{array}$$

If n is not a power of a prime, it has at least two prime divisors p_1 and p_2, hence G_n contains the cycle $G_{p_1p_2}$.

b) It follows from this discussion that G_n is a tree if and only if n is a power of a prime, and G_n is a cycle if and only if n is the product p_1p_2 of two different primes.