February 2023. Limbe (Cameroun)

Number Theory
African Institute for Mathematical Sciences (AIMS)

Michel Waldschmidt, Sorbonne Université

Assignment 1

1.
(a) Show that
- two points in $\mathbb{R}^2$ lie on a line,
- five points lie on a conic,
- nine points lie on a cubic,
- 14 points lie on a **quartic**.
- How many points for a plane curve of degree d ?

`Hint`. *A plane curve of degree d is the set of points $(x, y) \in \mathbb{R}^2$ for which a polynomial*

$$P(x, y) = \sum_{i+j \le d} a_{ij} x^i y^j.$$

of degree d vanishes. A line is a curve of degree 1

$$a_{00} + a_{10}x + a_{01}y = 0,$$

a conic is a curve of degree 2

$$a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}y^2 = 0,$$

a cubic is a curve of degree 3

$$a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}y^2 + a_{30}x^3 + a_{21}x^2y + a_{12}xy^2 + a_{03}y^3 = 0,$$

a quartic is a curve of degree 4

$$a_{00} + a_{10}x + a_{01}y + a_{20}x^2 + a_{11}xy + a_{02}y^2 + a_{30}x^3 + a_{21}x^2y + a_{12}xy^2 + a_{03}y^3 + a_{40}x^4 + a_{31}x^3y + a_{22}x^2y^2 + a_{13}xy^3 + a_{04}y^4 = 0.$$

How many coefficients has a polynomial of degree d in two variables ?

(b) Let d and n be two positive integers.
Show that the number of $(i_1, i_2 \ldots, i_n)$ with $i_k \geq 0$ for $k = 1, 2, \ldots, n$ and $i_1 + i_2 + \cdots + i_n \leq d$ is the binomial coefficient

$$\binom{d+n}{n} = \frac{(d+n)!}{d!n!}.$$

Show that the number of $(i_1, i_2 \ldots, i_n)$ with $i_k \geq 0$ for $k = 1, 2, \ldots, n$ and $i_1 + i_2 + \cdots + i_n = d$ is the binomial coefficient

$$\binom{d+n-1}{n-1} = \frac{(d+n-1)!}{d!(n-1)!}.$$

`Hint`. *One can prove the result by induction using the fact that a polynomial of degree $\leq d$ is the sum of a polynomial of degree $\leq d-1$ and a homogeneous polynomial of degree d in a unique way.*

A different combinatorial proof rests on the fact that for $0 \leq k \leq m$, the number of subsets with k elements in a set with m elements is the binomial coefficient

$$\binom{m}{k} = \frac{m!}{k!(m-k)!}.$$

Select $n-1$ elements in a set with $d+n-1$ elements.

2. Check

$3 = 1+2, \quad 5 = 2+3, \quad 6 = 1+2+3, \quad 7 = 3+4, \quad 9 = 4+5, \quad 10 = 1+2+3+4.$

Prove that a positive integer m is the sum of two or more consecutive positive integers if and only if m is not a power of 2.

3. Compute the gcd of $10^{100} - 100$ and $10^{10} - 1000$. Give explicitly a common divisor to these two numbers between 500 and 1000.

February 2023. Limbe (Cameroun)

Number Theory
African Institute for Mathematical Sciences (AIMS)

Michel Waldschmidt, Sorbonne Université

Assignment 1 — Solution

1. We start with the second part of (b).

Denote by $f(n,d)$ the dimension of the vector space of polynomials in n variables of degree $\le d$ and by $\tilde{f}(n,d)$ the dimension of the vector space of homogeneous polynomials in n variables of degree d (including 0).

By sending one of the variables to 1, we obtain a biojective map between the vector space of homogeneous polynomials in n variables of degree d and the vector space of polynomials in $n-1$ variables of degree $\le d$; hence

$$\tilde{f}(n,d) = f(n-1,d).$$

• *First proof of (b)* by induction.

A polynomial of degree $\le d$ is the sum of a polynomial of degree $\le d-1$ and a homogeneous polynomial of degree d in a unique way

$$\sum_{j_1+\cdots+j_n\le d} a_{j_1\dots j_n} X_1^{j_1}\cdots X_n^{j_n} = \sum_{j_1+\cdots+j_n< d} a_{j_1\dots j_n} X_1^{j_1}\cdots X_n^{j_n} + \sum_{j_1+\cdots+j_n= d} a_{j_1\dots j_n} X_1^{j_1}\cdots X_n^{j_n}.$$

Hence

$$f(n,d) = f(n,d-1) + \tilde{f}(n,d).$$

Since $\tilde{f}(n,d) = f(n-1,d)$ we deduce

$$f(n,d) = f(n,d-1) + f(n-1,d).$$

Since

$$\binom{n+d-1}{d-1} = \frac{(n+d-1)!}{n!(d-1)!} = d\frac{(n+d-1)!}{n!d!}$$

and

$$\binom{n-1+d}{d} = \frac{(n-1+d)!}{(n-1)!d!} = n\frac{(n+d-1)!}{n!d!},$$

the binomial coefficient $\binom{n+d}{d}$ satisfies the same relation

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

By induction on $n+d$, starting with $f(1,1)=1$, we deduce

$$f(n,d) = \binom{n+d}{d}.$$

• *Second proof of (b)* (combinatoric).

Given n and d, consider $d+n-1$ dots on a straight line; paint $n-1$ of them in blue and the other ones in red. Let i_1 be the number of dots on the left of the first blue dot, i_k the number of dots between the $(k-1)$–th and the k–th blue dots, and i_n the number of dots on the right of the $(n-1)$–th blue dot. We have $i_k \geq 0$ and $i_1 + \cdots + i_k = d$ (this is the number of red dots).

Conversely, given $(i_1, i_2 \ldots, i_n)$ with $i_k \geq 0$ for $k = 1, 2, \ldots, n$ and $i_1 + i_2 + \cdots + i_n = d$, paint d dots in red and insert $n-1$ blue dots, one between the $i_1 + i_2 + \cdots + i_k$–th red dot and the $i_1 + i_2 + \cdots + i_{k+1}$–th red dot for $1 \leq k \leq n-1$. This produces a subset with $n-1$ elements in a set with $d+n-1$ elements, and the number of such subsets is the binomial coefficient.

This shows that the dimension of the vector space of polynomials in n variables of degree $\leq d-1$ is the same as the dimension of the vector space of homogeneous polynomials in n variables of degree $\leq d$, namely

$$\binom{d+n-1}{n-1} = \frac{(d+n-1)!}{d!(n-1)!}.$$

We deduce the first part of (b) : if $i_1, i_2, \ldots, i_{n-1}$ satisfy $i_k \geq 0$ for $k = 1, 2, \ldots, n-1$ and $i_1 + i_2 + \cdots + i_{n-1} \leq d$, then set $i_n = d - (i_1 + i_2 + \cdots + i_{n-1})$ to get $i_1 + i_2 + \cdots + i_n = d$.

Since

$$\binom{d+2}{2} = \frac{(d+1)(d+2)}{2},$$

a polynomial in two variables of degree d has $(d+1)(d+2)/2$ coefficients. Any subset of $\mathbb{R}^2$ with at most

$$\frac{(d+1)(d+2)}{2} - 1 = \frac{d^2+3d}{2}$$

elements is contained in a plane curve of degree d : a system of homogeneous linear equation where the number of unknowns is larger than the number of equations has a non trivial solution. We have

$$\frac{d^2+3d}{2} = \begin{cases} 2 & \text{for } d=1, \\ 5 & \text{for } d=2, \\ 9 & \text{for } d=3, \\ 14 & \text{for } d=4. \end{cases}$$

The sequence

$$2, 5, 9, 14, 20, 27, 35, 44, 54, 65, 77, 90, 104, 119, 135, \dots$$

is `A000096` in Sloane's Online Encyclopedia of Integer Sequences `https://oeis.org/A000096`.

2. Write $m = 2^a b$ with $a \geq 0$ and b odd ≥ 1 and

$$\begin{aligned} m &= x + (x+1) + \cdots + (x+y) \\ &= 1 + 2 + \cdots + (x+y) - (1 + 2 + \cdots + (x-1)) \\ &= \frac{(x+y)(x+y+1)}{2} - \frac{x(x-1)}{2} \\ &= \frac{1}{2} y(2x+y+1) \\ &= 2^a b \end{aligned}$$

with $x \geq 0$ and $y \geq 1$. If y is odd and ≥ 3 then m has an odd factor, y. If $y = 1$ then $m = x(x+1)/2$ is not a power of 2. If y is even then $2x + y + 1$ is odd and ≥ 3, hence again m has an odd factor ≥ 3.

Therefore a power of 2 is not the sum of consecutive positive integers. If we drop the assumption that the integers are positive we have the trivial solution

$$m = -(m-1) - (m-2) - \cdots + (-1) + 0 + 1 + 2 + \cdots + (m-2) + (m-1) + m.$$

Now assume m is not a power of 2, that is $b \geq 3$. Then we set

$$\begin{cases} y = 2^{a+1},\ x = \dfrac{b-1}{2} - 2^a \text{ if } b \geq 2^{a+1} + 1, \\ y = b,\ x = 2^a - \dfrac{b+1}{2} \text{ if } b \leq 2^{a+1} - 1. \end{cases}$$

Since b is odd this covers all cases.

3. The answer is $10^9 - 100$ which is divisible by 900.

Proof : write

$$10^{100} - 100 = 10^2(10^{98} - 1)$$

and

$$10^{10} - 1000 = 10^3(10^7 - 1).$$

Since 7 divides 98, $10^7 - 1$ divides $10^{98} - 1$ (use the identity $x^n - 1$ with $x = 10^7$ and $n = 14$). Further $10^7 - 1$ and 10 are relatively prime. Hence the gcd is $10^2(10^7 - 1) = 10^9 - 100$ which is a multiple of 900 ($10^7 - 1 = 999\,999$ is a multiple of 9).