Frobenius problem: bounds, formulas and related problems

J.L. Ramírez Alfonsín

Université Montpellier 2

Theorem (Sylvester, 1882) $g(a_1, a_2) = a_1 a_2 - a_1 - a_2$.

Proof (by Nijenhuis and Wilf). Since $\gcd(a_1, a_2) = 1$ then any integer p is representable as $p = xa_1 + ya_2$ with $x, y \in \mathbb{Z}$.

Note : p can be represented in many different ways but the representation becomes unique if ask for $0 \leq x < a_2$. In this case, p is representable if $y \geq 0$ and it is not representable if $y < 0$.

Thus, the largest non representable value is when $x = a_2 - 1$ and $y = -1$. So,

$$g(a_1, a_2) = (a_2 - 1)a_1 + (-1)a_2 = a_1 a_2 - a_1 - a_2.$$

Theorem (Sylvester, 1882) $g(a_1, a_2) = a_1 a_2 - a_1 - a_2$.

Proof (by Nijenhuis and Wilf). Since $\gcd(a_1, a_2) = 1$ then any integer p is representable as $p = xa_1 + ya_2$ with $x, y \in \mathbb{Z}$.

Note : p can be represented in many different ways but the representation becomes unique if ask for $0 \leq x < a_2$. In this case, p is representable if $y \geq 0$ and it is not representable if $y < 0$.

Thus, the largest non representable value is when $x = a_2 - 1$ and $y = -1$. So,

$$g(a_1, a_2) = (a_2 - 1)a_1 + (-1)a_2 = a_1 a_2 - a_1 - a_2.$$

Theorem (Sylvester, 1882) $g(a_1, a_2) = a_1 a_2 - a_1 - a_2$.

Proof (by Nijenhuis and Wilf). Since $\gcd(a_1, a_2) = 1$ then any integer p is representable as $p = xa_1 + ya_2$ with $x, y \in \mathbb{Z}$.

Note : p can be represented in many different ways but the representation becomes unique if ask for $0 \leq x < a_2$. In this case, p is representable if $y \geq 0$ and it is not representable if $y < 0$.

Thus, the largest non representable value is when $x = a_2 - 1$ and $y = -1$. So,

$$g(a_1, a_2) = (a_2 - 1)a_1 + (-1)a_2 = a_1 a_2 - a_1 - a_2.$$

Theorem (Sylvester, 1882) $g(a_1, a_2) = a_1 a_2 - a_1 - a_2$.

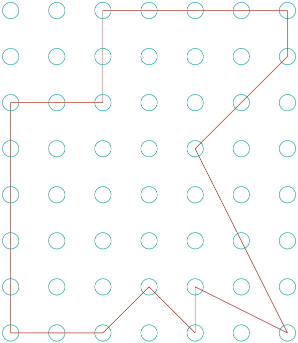
Proof (by Nijenhuis and Wilf). Since $\gcd(a_1, a_2) = 1$ then any integer p is representable as $p = xa_1 + ya_2$ with $x, y \in \mathbb{Z}$.

Note : p can be represented in many different ways but the representation becomes unique if ask for $0 \leq x < a_2$. In this case, p is representable if $y \geq 0$ and it is not representable if $y < 0$.

Thus, the largest non representable value is when $x = a_2 - 1$ and $y = -1$. So,

$$g(a_1, a_2) = (a_2 - 1)a_1 + (-1)a_2 = a_1 a_2 - a_1 - a_2.$$

A simplest lattice polygon.



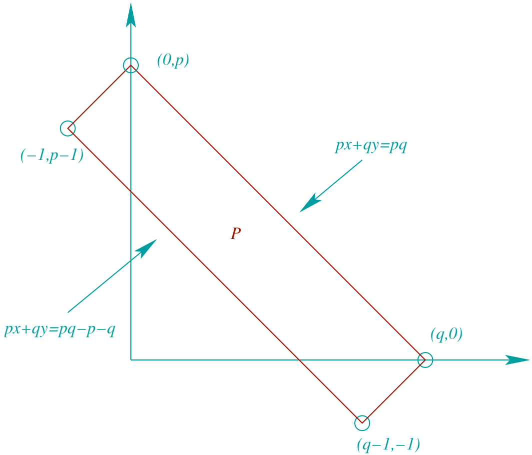
Theorem (Pick, 1899) Let S be a simplest lattice polygon. Then,

$$A(S) = I(S) + \frac{B(S)}{2} - 1$$

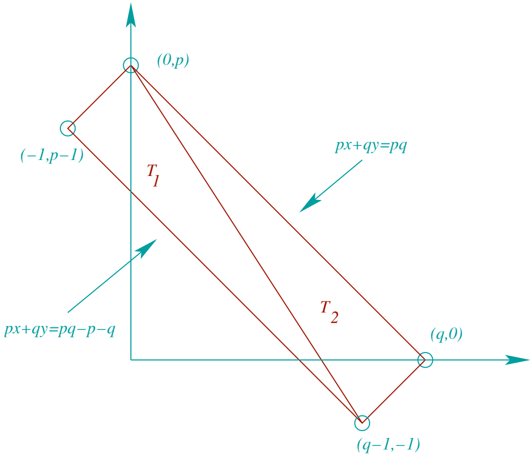
where $A(S)$ denotes the area of S, $I(S)$ and $B(S)$ are the number of lattice points in the interior of S and in the boundary of S respectively.

Second proof (for $g(p,q) = pq - p - q$)

Second proof (for $g(p,q) = pq - p - q$)



Second proof (for $g(p,q) = pq - p - q$).



$$A(T_1) = \frac{1}{2}\begin{vmatrix} q & 0 & 1 \\ 0 & p & 1 \\ -1 & p-1 & 1 \end{vmatrix} = \frac{1}{2}(q+p)$$

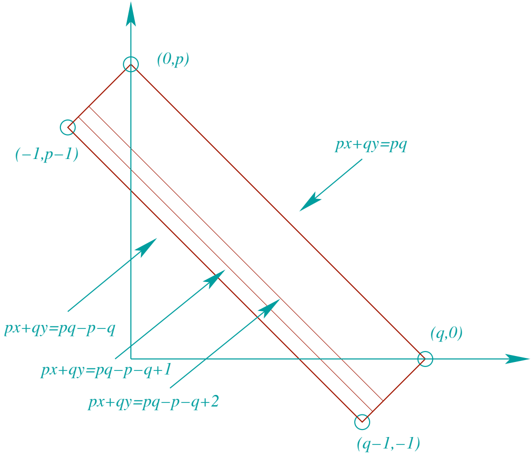
So, $A(P) = A(T_1) + A(T_2) = p + q$ and, by Pick's theorem, we have that $I(P) = p + q - 1$.

$$A(T_1) = \frac{1}{2}\begin{vmatrix} q & 0 & 1 \\ 0 & p & 1 \\ -1 & p-1 & 1 \end{vmatrix} = \frac{1}{2}(q+p)$$

So, $A(P) = A(T_1) + A(T_2) = p + q$ and, by Pick's theorem, we have that $I(P) = p + q - 1$.

Claim. Line $px + qy = pq - p - q + i$ contains exactly one point in $I(P)$ for each $i = 1, \ldots, p + q - 1$.

Claim. Line $px + qy = pq - p - q + i$ contains exactly one point in $I(P)$ for each $i = 1, \ldots, p + q - 1$.



Question : does there exist a formula for $g(a_1, a_2, a_3)$?

Theorem (Curtis, 1990) There is no finite set of polynomials $\{h_1, \ldots, h_m\}$ such that for each choice of a_1, a_2, a_3 there is some i such that $h_i(a_1, a_2, a_3) = g(a_1, a_2, a_3)$.

Question : does there exists a semi-explicit formula for $g(a_1, a_2, a_3)$?

Question : does there exist a formula for $g(a_1, a_2, a_3)$?

Theorem (Curtis, 1990) There is no finite set of polynomials $\{h_1, \ldots, h_m\}$ such that for each choice of a_1, a_2, a_3 there is some i such that $h_i(a_1, a_2, a_3) = g(a_1, a_2, a_3)$.

Question : does there exists a semi-explicit formula for $g(a_1, a_2, a_3)$?

Question : does there exist a formula for $g(a_1, a_2, a_3)$?

Theorem (Curtis, 1990) There is no finite set of polynomials $\{h_1, \ldots, h_m\}$ such that for each choice of a_1, a_2, a_3 there is some i such that $h_i(a_1, a_2, a_3) = g(a_1, a_2, a_3)$.

Question : does there exists a semi-explicit formula for $g(a_1, a_2, a_3)$?

Let L_1, L_2 and L_3 be the smallest positive integers such that there exist integers $x_{ij} \geq 0$, $1 \leq i, j \leq 3$, $i \neq j$ with

$$\begin{aligned} L_1 a_1 &= x_{12} a_2 + x_{13} a_3, \\ L_2 a_2 &= x_{21} a_1 + x_{23} a_3, \\ L_3 a_3 &= x_{31} a_1 + x_{32} a_2. \end{aligned}$$

Theorem (Denham 2000, R.A. and Rødseth 2009) Let a_1, a_2, a_3 be pairwise relatively prime positive integers and $\{i, j, k\} = \{1, 2, 3\}$. Then,

$$g(a_1, a_2, a_3) = \begin{cases} \max\{L_i a_i + x_{jk} a_k, L_j a_j + x_{ik} a_k\} - \sum_{n=1}^{3} a_n & \text{if } x_{ij} > 0 \\ & \text{for all } i, j, \\ L_j a_j + L_i a_i - \sum_{n=1}^{3} a_n & \text{if } x_{ij} = 0. \end{cases}$$

Let L_1, L_2 and L_3 be the smallest positive integers such that there exist integers $x_{ij} \geq 0$, $1 \leq i, j \leq 3$, $i \neq j$ with

$$\begin{aligned} L_1 a_1 &= x_{12} a_2 + x_{13} a_3, \\ L_2 a_2 &= x_{21} a_1 + x_{23} a_3, \\ L_3 a_3 &= x_{31} a_1 + x_{32} a_2. \end{aligned}$$

Theorem (Denham 2000, R.A. and Rødseth 2009) Let a_1, a_2, a_3 be pairwise relatively prime positive integers and $\{i, j, k\} = \{1, 2, 3\}$. Then,

$$g(a_1, a_2, a_3) = \begin{cases} \max\{L_i a_i + x_{jk} a_k, L_j a_j + x_{ik} a_k\} - \sum_{n=1}^{3} a_n & \text{if } x_{ij} > 0 \\ & \text{for all } i, j, \\ L_j a_j + L_i a_i - \sum_{n=1}^{3} a_n & \text{if } x_{ij} = 0. \end{cases}$$

Upper Bounds

Theorem (Brauer and Shockley 1962) Let $d = (a_1, \ldots, a_{n-1})$. Then, $g(a_1, \ldots, a_n) = dg(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}, a_n) + (d-1)a_n$.

Theorem (Schur 1942) $g(a_1, \ldots, a_n) \leq (a_1 - 1)(a_n - 1) - 1$.

Theorem (Selmer 1977) $g(a_1, \ldots, a_n) \leq 2a_n \left\lfloor \frac{a_1}{n} \right\rfloor - a_1$.

Theorem (Erdős and Graham 1972)
$g(a_1, \ldots, a_n) \leq 2a_{n-1} \left\lfloor \frac{a_n}{n} \right\rfloor - a_n$.

Upper Bounds

Theorem (Brauer and Shockley 1962) Let $d = (a_1, \ldots, a_{n-1})$. Then, $g(a_1, \ldots, a_n) = dg(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}, a_n) + (d-1)a_n$.

Theorem (Schur 1942) $g(a_1, \ldots, a_n) \leq (a_1 - 1)(a_n - 1) - 1$.

Theorem (Selmer 1977) $g(a_1, \ldots, a_n) \leq 2a_n \left\lfloor \frac{a_1}{n} \right\rfloor - a_1$.

Theorem (Erdős and Graham 1972) $g(a_1, \ldots, a_n) \leq 2a_{n-1} \left\lfloor \frac{a_n}{n} \right\rfloor - a_n$.

Upper Bounds

Theorem (Brauer and Shockley 1962) Let $d = (a_1, \ldots, a_{n-1})$. Then, $g(a_1, \ldots, a_n) = dg(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}, a_n) + (d-1)a_n$.

Theorem (Schur 1942) $g(a_1, \ldots, a_n) \leq (a_1 - 1)(a_n - 1) - 1$.

Theorem (Selmer 1977) $g(a_1, \ldots, a_n) \leq 2a_n \left\lfloor \frac{a_1}{n} \right\rfloor - a_1$.

Theorem (Erdős and Graham 1972) $g(a_1, \ldots, a_n) \leq 2a_{n-1} \left\lfloor \frac{a_n}{n} \right\rfloor - a_n$.

Upper Bounds

Theorem (Brauer and Shockley 1962) Let $d = (a_1, \ldots, a_{n-1})$. Then, $g(a_1, \ldots, a_n) = dg(\frac{a_1}{d}, \ldots, \frac{a_{n-1}}{d}, a_n) + (d-1)a_n$.

Theorem (Schur 1942) $g(a_1, \ldots, a_n) \leq (a_1 - 1)(a_n - 1) - 1$.

Theorem (Selmer 1977) $g(a_1, \ldots, a_n) \leq 2a_n \left\lfloor \frac{a_1}{n} \right\rfloor - a_1$.

Theorem (Erdős and Graham 1972)
$g(a_1, \ldots, a_n) \leq 2a_{n-1} \left\lfloor \frac{a_n}{n} \right\rfloor - a_n$.

Lower Bounds

Theorem (Davison 1994)
$g(a_1, a_2, a_3) \geq \sqrt{3}\sqrt{a_1 a_2 a_3} - a_1 - a_2 - a_3.$

Theorem (Hujter 1987) $2 \geq \liminf_{\frac{a_1 a_2}{a_3} \to \infty} \frac{g(a_1,a_2,a_3)}{\sqrt{a_1 a_2 a_3}} \geq \sqrt{2}.$

Theorem (Hujter 1982)
$g(a_1, \ldots, a_n) \geq \left(\frac{n-1}{n}\right) \left((n-1)! a_1 a_2 \cdots a_n\right)^{\frac{1}{n-1}} - \sum_{i=1}^{n} a_i.$

Theorem (Killingbergtrø 2000)
$g(a_1, \ldots, a_n) \geq \left((n-1)! a_1 a_2 \cdots a_n\right)^{\frac{1}{n-1}} - \sum_{i=1}^{n} a_i.$

Lower Bounds

Theorem (Davison 1994)
$g(a_1, a_2, a_3) \geq \sqrt{3}\sqrt{a_1 a_2 a_3} - a_1 - a_2 - a_3.$

Theorem (Hujter 1987) $2 \geq \liminf_{\frac{a_1 a_2}{a_3} \to \infty} \frac{g(a_1,a_2,a_3)}{\sqrt{a_1 a_2 a_3}} \geq \sqrt{2}.$

Theorem (Hujter 1982)
$g(a_1, \ldots, a_n) \geq \left(\frac{n-1}{n}\right) \left((n-1)! a_1 a_2 \cdots a_n\right)^{\frac{1}{n-1}} - \sum_{i=1}^{n} a_i.$

Theorem (Killingbergtrø 2000)
$g(a_1, \ldots, a_n) \geq \left((n-1)! a_1 a_2 \cdots a_n\right)^{\frac{1}{n-1}} - \sum_{i=1}^{n} a_i.$

Lower Bounds

Theorem (Davison 1994)
$g(a_1, a_2, a_3) \geq \sqrt{3}\sqrt{a_1 a_2 a_3} - a_1 - a_2 - a_3.$

Theorem (Hujter 1987) $2 \geq \liminf_{\frac{a_1 a_2}{a_3} \to \infty} \frac{g(a_1,a_2,a_3)}{\sqrt{a_1 a_2 a_3}} \geq \sqrt{2}.$

Theorem (Hujter 1982)
$g(a_1, \ldots, a_n) \geq \left(\frac{n-1}{n}\right) \left((n-1)! a_1 a_2 \cdots a_n\right)^{\frac{1}{n-1}} - \sum_{i=1}^{n} a_i.$

Theorem (Killingbergtrø 2000)
$g(a_1, \ldots, a_n) \geq \left((n-1)! a_1 a_2 \cdots a_n\right)^{\frac{1}{n-1}} - \sum_{i=1}^{n} a_i.$

Lower Bounds

Theorem (Davison 1994)
$g(a_1, a_2, a_3) \geq \sqrt{3}\sqrt{a_1 a_2 a_3} - a_1 - a_2 - a_3.$

Theorem (Hujter 1987) $2 \geq \liminf_{\frac{a_1 a_2}{a_3} \to \infty} \frac{g(a_1,a_2,a_3)}{\sqrt{a_1 a_2 a_3}} \geq \sqrt{2}.$

Theorem (Hujter 1982)
$g(a_1, \ldots, a_n) \geq \left(\frac{n-1}{n}\right) \left((n-1)! a_1 a_2 \cdots a_n\right)^{\frac{1}{n-1}} - \sum_{i=1}^{n} a_i.$

Theorem (Killingbergtrø 2000)
$g(a_1, \ldots, a_n) \geq \left((n-1)! a_1 a_2 \cdots a_n\right)^{\frac{1}{n-1}} - \sum_{i=1}^{n} a_i.$

Conjecture (Beihoffer,Hendry,Nijenhuis and Wagon) The expected value of $g(a_1, \ldots, a_n)$ is a small constant multiple of

$$\left(\frac{1}{2} n! \prod_{i=1}^{n} a_i\right)^{\frac{1}{n-1}} - \sum_{i=1}^{n} a_i.$$

Arithmetic and related sequences

Theorem (Brauer 1942)
$g(a, a+1, \ldots, a+k-1) = \left(\left\lfloor \frac{a-2}{k-1} \right\rfloor + 1\right) a - 1.$

Theorem (Roberts 1956) Let $a, d, s \in \mathbb{N}$ with $\gcd(a, d) = 1$. Then,
$g(a, a+d, \ldots, a+sd) = \left(\left\lfloor \frac{a-2}{s} \right\rfloor + 1\right) a + (d-1)(a-1) - 1.$

Theorem (Selmer 1977) Let $a, h, d, k \in \mathbb{N}^+$ with $\gcd(a, d) = 1$. Then,
$g(a, ha+d, ha+2d, \ldots, ha+kd) = ha \left\lfloor \frac{a-2}{k} \right\rfloor + a(h-1) + d(a-1).$

Theorem (R.A. and Rødseth 2009) Semi-explicit formula for $g(a, a+d, \ldots, a+kd, c)$ with $\gcd(a, d) = 1$.

Arithmetic and related sequences

Theorem (Brauer 1942)
$g(a, a+1, \ldots, a+k-1) = \left(\left\lfloor \frac{a-2}{k-1} \right\rfloor + 1\right) a - 1.$

Theorem (Roberts 1956) Let $a, d, s \in \mathbb{N}$ with $\gcd(a, d) = 1$. Then,
$g(a, a+d, \ldots, a+sd) = \left(\left\lfloor \frac{a-2}{s} \right\rfloor + 1\right) a + (d-1)(a-1) - 1.$

Theorem (Selmer 1977) Let $a, h, d, k \in \mathbb{N}^+$ with $\gcd(a, d) = 1$. Then,
$g(a, ha+d, ha+2d, \ldots, ha+kd) = ha \left\lfloor \frac{a-2}{k} \right\rfloor + a(h-1) + d(a-1).$

Theorem (R.A. and Rødseth 2009) Semi-explicit formula for $g(a, a+d, \ldots, a+kd, c)$ with $\gcd(a, d) = 1$.

Arithmetic and related sequences

Theorem (Brauer 1942)
$g(a, a+1, \ldots, a+k-1) = \left(\left\lfloor \frac{a-2}{k-1} \right\rfloor + 1\right) a - 1.$

Theorem (Roberts 1956) Let $a, d, s \in \mathbb{N}$ with $\gcd(a, d) = 1$. Then,
$g(a, a+d, \ldots, a+sd) = \left(\left\lfloor \frac{a-2}{s} \right\rfloor + 1\right) a + (d-1)(a-1) - 1.$

Theorem (Selmer 1977) Let $a, h, d, k \in \mathbb{N}^+$ with $\gcd(a, d) = 1$.
Then,
$g(a, ha+d, ha+2d, \ldots, ha+kd) = ha \left\lfloor \frac{a-2}{k} \right\rfloor + a(h-1) + d(a-1).$

Theorem (R.A. and Rødseth 2009) Semi-explicit formula for
$g(a, a+d, \ldots, a+kd, c)$ with $\gcd(a, d) = 1$.

Arithmetic and related sequences

Theorem (Brauer 1942)
$g(a, a+1, \ldots, a+k-1) = \left(\left\lfloor \frac{a-2}{k-1} \right\rfloor + 1 \right) a - 1.$

Theorem (Roberts 1956) Let $a, d, s \in \mathbb{N}$ with $\gcd(a, d) = 1$. Then,
$g(a, a+d, \ldots, a+sd) = \left(\left\lfloor \frac{a-2}{s} \right\rfloor + 1 \right) a + (d-1)(a-1) - 1.$

Theorem (Selmer 1977) Let $a, h, d, k \in \mathbb{N}^+$ with $\gcd(a, d) = 1$. Then,
$g(a, ha+d, ha+2d, \ldots, ha+kd) = ha \left\lfloor \frac{a-2}{k} \right\rfloor + a(h-1) + d(a-1).$

Theorem (R.A. and Rødseth 2009) Semi-explicit formula for $g(a, a+d, \ldots, a+kd, c)$ with $\gcd(a, d) = 1$.

Fibonacci Semigroups

A *Fibonacci semigroup* is a semigroup generated by *Fibonacci* numbers $F_{i_1}, \ldots, F_{i_r}$, $3 \leq i_1 < \cdots < i_r$ with $\gcd(F_{i_1}, \ldots, F_{i_r}) = 1$.

$g(F_i, F_{i+1}, F_{i+k}) = g(F_i, F_{i+1})$ since $F_{i+k} = F_k F_{i+1} + F_{k-1} F_i$.

Theorem (Marin, R.A. and Revuelta, 2007) Let $i, k \geq 3$ be integers and let $r = \lfloor \frac{F_i - 1}{F_k} \rfloor$. Then,

$$g(F_i, F_{i+2}, F_{i+k}) = \begin{cases} (F_i - 1)F_{i+2} - F_i(rF_{k-2} + 1) & \text{if } r = 0 \text{ or } r \geq 1 \text{ and } F_{k-2}F_i < (F_i - rF_k)F_{i+2}, \\ (rF_k - 1)F_{i+2} - F_i((r-1)F_{k-2} + 1) & \text{otherwise.} \end{cases}$$

Fibonacci Semigroups

A *Fibonacci semigroup* is a semigroup generated by *Fibonacci* numbers $F_{i_1}, \ldots, F_{i_r}$, $3 \leq i_1 < \cdots < i_r$ with $\gcd(F_{i_1}, \ldots, F_{i_r}) = 1$.

$g(F_i, F_{i+1}, F_{i+k}) = g(F_i, F_{i+1})$ since $F_{i+k} = F_k F_{i+1} + F_{k-1} F_i$.

Theorem (Marin, R.A. and Revuelta, 2007) Let $i, k \geq 3$ be integers and let $r = \lfloor \frac{F_i - 1}{F_k} \rfloor$. Then,

$$g(F_i, F_{i+2}, F_{i+k}) = \begin{cases} (F_i - 1)F_{i+2} - F_i(rF_{k-2} + 1) & \text{if } r = 0 \text{ or } r \geq 1 \text{ and } F_{k-2}F_i < (F_i - rF_k)F_{i+2}, \\ (rF_k - 1)F_{i+2} - F_i((r-1)F_{k-2} + 1) & \text{otherwise.} \end{cases}$$

Fibonacci Semigroups

A *Fibonacci semigroup* is a semigroup generated by *Fibonacci* numbers $F_{i_1}, \ldots, F_{i_r}$, $3 \leq i_1 < \cdots < i_r$ with $\gcd(F_{i_1}, \ldots, F_{i_r}) = 1$.

$g(F_i, F_{i+1}, F_{i+k}) = g(F_i, F_{i+1})$ since $F_{i+k} = F_k F_{i+1} + F_{k-1} F_i$.

Theorem (Marin, R.A. and Revuelta, 2007) Let $i, k \geq 3$ be integers and let $r = \lfloor \frac{F_i - 1}{F_k} \rfloor$. Then,

$$g(F_i, F_{i+2}, F_{i+k}) = \begin{cases} (F_i - 1)F_{i+2} - F_i(rF_{k-2} + 1) & \text{if } r = 0 \text{ or } r \geq 1 \text{ and } \\ & F_{k-2}F_i < (F_i - rF_k)F_{i+2}, \\ (rF_k - 1)F_{i+2} - F_i((r-1)F_{k-2} + 1) & \text{otherwise.} \end{cases}$$

Denumerant

Let $a_1, \ldots, a_n, m$ be positive integers. The denumerant denoted by $d(m; a_1, \ldots, a_n)$ is the number of nonnegative integer representations of m by $a_1, \ldots, a_n$, that is, the number of solutions of the form

$$m = \sum_{i=1}^{n} x_i a_i$$

with integers $x_i \geq 0$.

Theorem The generating function of $d(m; a_1, \ldots, a_n)$ is

$$f(z) = \frac{1}{(1 - z^{a_1})(1 - z^{a_2}) \cdots (1 - z^{a_n})}$$

Denumerant

Let $a_1, \ldots, a_n, m$ be positive integers. The denumerant denoted by $d(m; a_1, \ldots, a_n)$ is the number of nonnegative integer representations of m by $a_1, \ldots, a_n$, that is, the number of solutions of the form

$$m = \sum_{i=1}^{n} x_i a_i$$

with integers $x_i \geq 0$.

Theorem The generating function of $d(m; a_1, \ldots, a_n)$ is

$$f(z) = \frac{1}{(1 - z^{a_1})(1 - z^{a_2}) \cdots (1 - z^{a_n})}$$

Denumerant

Let $a_1, \ldots, a_n, m$ be positive integers. The denumerant denoted by $d(m; a_1, \ldots, a_n)$ is the number of nonnegative integer representations of m by $a_1, \ldots, a_n$, that is, the number of solutions of the form

$$m = \sum_{i=1}^{n} x_i a_i$$

with integers $x_i \geq 0$.

Theorem The generating function of $d(m; a_1, \ldots, a_n)$ is

$$f(z) = \frac{1}{(1 - z^{a_1})(1 - z^{a_2}) \cdots (1 - z^{a_n})}$$

Proof. Recall that $\frac{1}{1-z^r}$ has expansion $\sum_{i=0}^{\infty} z^{ir}$.

By taking $r = a_1, \ldots, a_n$ we have

$$\begin{aligned}
\prod_{i=1}^{\infty} \frac{1}{1-z^{a_i}} &= (1 + z^{1a_1} + z^{2a_1} \ldots) \times \cdots \times (1 + z^{1a_n} + z^{2a_n} \ldots) \\
&= \sum_{i_1=0}^{\infty} \cdots \sum_{i_n=0}^{\infty} z^{i_1 a_1 + \cdots + i_n a_n} \\
&= \sum_{i=0}^{\infty} c_i z^i.
\end{aligned}$$

where c_m is the number of solutions $i_1 a_1 + \cdots + i_n a_n = m$ in nonnegative integers $i_1, \ldots, i_n$, that is, $c_m = d(m; a_1, \ldots, a_n)$.

Remark : $g(a_1, \ldots, a_n)$ is the greatest integer k with $f^k(0) = 0$.

Proof. Recall that $\frac{1}{1-z^r}$ has expansion $\sum_{i=0}^{\infty} z^{ir}$.

By taking $r = a_1, \ldots, a_n$ we have

$$\begin{aligned}\prod_{i=1}^{\infty} \frac{1}{1-z^{a_i}} &= (1 + z^{1a_1} + z^{2a_1} \ldots) \times \cdots \times (1 + z^{1a_n} + z^{2a_n} \ldots) \\ &= \sum_{i_1=0}^{\infty} \cdots \sum_{i_n=0}^{\infty} z^{i_1 a_1 + \cdots + i_n a_n} \\ &= \sum_{i=0}^{\infty} c_i z^i.\end{aligned}$$

where c_m is the number of solutions $i_1 a_1 + \cdots + i_n a_n = m$ in nonnegative integers $i_1, \ldots, i_n$, that is, $c_m = d(m; a_1, \ldots, a_n)$.

Remark : $g(a_1, \ldots, a_n)$ is the greatest integer k with $f^k(0) = 0$.

Proof. Recall that $\frac{1}{1-z^r}$ has expansion $\sum_{i=0}^{\infty} z^{ir}$.

By taking $r = a_1, \ldots, a_n$ we have

$$\begin{aligned}\prod_{i=1}^{\infty} \frac{1}{1-z^{a_i}} &= (1 + z^{1a_1} + z^{2a_1} \ldots) \times \cdots \times (1 + z^{1a_n} + z^{2a_n} \ldots) \\ &= \sum_{i_1=0}^{\infty} \cdots \sum_{i_n=0}^{\infty} z^{i_1 a_1 + \cdots + i_n a_n} \\ &= \sum_{i=0}^{\infty} c_i z^i.\end{aligned}$$

where c_m is the number of solutions $i_1 a_1 + \cdots + i_n a_n = m$ in nonnegative integers $i_1, \ldots, i_n$, that is, $c_m = d(m; a_1, \ldots, a_n)$.

Remark : $g(a_1, \ldots, a_n)$ is the greatest integer k with $f^k(0) = 0$.

Proof. Recall that $\frac{1}{1-z^r}$ has expansion $\sum_{i=0}^{\infty} z^{ir}$.

By taking $r = a_1, \dots, a_n$ we have

$$\begin{aligned}\prod_{i=1}^{\infty} \frac{1}{1-z^{a_i}} &= (1 + z^{1a_1} + z^{2a_1} \dots) \times \cdots \times (1 + z^{1a_n} + z^{2a_n} \dots) \\ &= \sum_{i_1=0}^{\infty} \cdots \sum_{i_n=0}^{\infty} z^{i_1 a_1 + \cdots + i_n a_n} \\ &= \sum_{i=0}^{\infty} c_i z^i.\end{aligned}$$

where c_m is the number of solutions $i_1 a_1 + \cdots + i_n a_n = m$ in nonnegative integers $i_1, \dots, i_n$, that is, $c_m = d(m; a_1, \dots, a_n)$.

Remark : $g(a_1, \dots, a_n)$ is the greatest integer k with $f^k(0) = 0$.

Theorem (Shur, 1926) Let $a_1, \ldots, a_n$ be relatively prime integers. Then,

$$d(m; a_1, \ldots, a_n) \sim \frac{m^{n-1}}{(n-1)! \prod_{i=1}^{n} a_i} \text{ as } m \longrightarrow \infty.$$

Let p, q relatively prime integers. Then,

$$d(m; p, q) = \begin{cases} 0 \text{ or } 1 & \text{if } 0 < m < pq, \\ 1 & \text{for all } pq - p - q < m < pq, \\ 0 & \text{if } m = pq - p - q. \end{cases}$$

Question : Is there a formula for the case $n = 2$?

Theorem (Shur, 1926) Let $a_1, \dots, a_n$ be relatively prime integers. Then,

$$d(m; a_1, \dots, a_n) \sim \frac{m^{n-1}}{(n-1)! \prod_{i=1}^{n} a_i} \text{ as } m \longrightarrow \infty.$$

Let p, q relatively prime integers. Then,

$$d(m; p, q) = \begin{cases} 0 \text{ or } 1 & \text{if } 0 < m < pq, \\ 1 & \text{for all } pq - p - q < m < pq, \\ 0 & \text{if } m = pq - p - q. \end{cases}$$

Question : Is there a formula for the case $n = 2$?

Theorem (Shur, 1926) Let $a_1, \ldots, a_n$ be relatively prime integers. Then,

$$d(m; a_1, \ldots, a_n) \sim \frac{m^{n-1}}{(n-1)! \prod_{i=1}^{n} a_i} \text{ as } m \longrightarrow \infty.$$

Let p, q relatively prime integers. Then,

$$d(m; p, q) = \begin{cases} 0 \text{ or } 1 & \text{if } 0 < m < pq, \\ 1 & \text{for all } pq - p - q < m < pq, \\ 0 & \text{if } m = pq - p - q. \end{cases}$$

Question : Is there a formula for the case $n = 2$?

Theorem (Popoviciu 1953) Let p, q relatively prime integers. Then,

$$d(m; p, q) = \frac{m + pp'(m) + qq'(m)}{pq} - 1$$

where $p'(m)p \equiv -m \pmod{q}, 1 \leq p'(m) \leq q$ and $q'(m)q \equiv -m \pmod{p}, 1 \leq q'(m) \leq p$

Proof. Suppose $0 < m < pq - p - q$.

We have that pq divides $m + pp'(m) + qq'(m)$ and that $0 < m + pp'(m) + qq'(m) < 3pq$ then either $m + pp'(m) + qq'(m) = pq$ or $2pq$.

- If $m + pp'(m) + qq'(m) = pq$ then we claim that $d(m; p, q) = 0$, Otherwise, if $d(m; p, q) > 0$ then there are integers $s, t \geq 0$ such that $ps + qt = m$. So

$$pp'(m)+qq'(m)+ps+qt = pq \rightarrow p(p'(m)+s)+q(q'(m)+t) = pq$$

So, p divides $q'(m) + t$ and q divides $p'(m) + s$ but $0 < q'(m) + t \leq p$ and $0 < p'(m) + s \leq q$ and thus $p = q'(m) + t$ and $q = p'(m) + s$ obtaining that $2qp = pq$ contadiction !

- if $m + pp'(m) + qq'(m) = pq$ then just notice that

$$m = p(q - p'(m)) + q(p - q'(m))$$

and thus $d(m; p, q) = 1$.

Proof. Suppose $0 < m < pq - p - q$.

We have that pq divides $m + pp'(m) + qq'(m)$ and that $0 < m + pp'(m) + qq'(m) < 3pq$ then either $m + pp'(m) + qq'(m) = pq$ or $2pq$.

- If $m + pp'(m) + qq'(m) = pq$ then we claim that $d(m; p, q) = 0$, Otherwise, if $d(m; p, q) > 0$ then there are integers $s, t \geq 0$ such that $ps + qt = m$. So

$$pp'(m)+qq'(m)+ps+qt = pq \rightarrow p(p'(m)+s)+q(q'(m)+t) = pq$$

So, p divides $q'(m) + t$ and q divides $p'(m) + s$ but $0 < q'(m) + t \leq p$ and $0 < p'(m) + s \leq q$ and thus $p = q'(m) + t$ and $q = p'(m) + s$ obtaining that $2qp = pq$ contadiction !

- if $m + pp'(m) + qq'(m) = pq$ then just notice that

$$m = p(q - p'(m)) + q(p - q'(m))$$

and thus $d(m; p, q) = 1$.

Proof. Suppose $0 < m < pq - p - q$.

We have that pq divides $m + pp'(m) + qq'(m)$ and that $0 < m + pp'(m) + qq'(m) < 3pq$ then either $m + pp'(m) + qq'(m) = pq$ or $2pq$.

• If $m + pp'(m) + qq'(m) = pq$ then we claim that $d(m; p, q) = 0$, Otherwise, if $d(m; p, q) > 0$ then there are integers $s, t \geq 0$ such that $ps + qt = m$. So

$$pp'(m) + qq'(m) + ps + qt = pq \rightarrow p(p'(m) + s) + q(q'(m) + t) = pq$$

So, p divides $q'(m) + t$ and q divides $p'(m) + s$ but $0 < q'(m) + t \leq p$ and $0 < p'(m) + s \leq q$ and thus $p = q'(m) + t$ and $q = p'(m) + s$ obtaining that $2qp = pq$ contadiction !

• if $m + pp'(m) + qq'(m) = pq$ then just notice that

$$m = p(q - p'(m)) + q(p - q'(m))$$

and thus $d(m; p, q) = 1$.

Proof. Suppose $0 < m < pq - p - q$.

We have that pq divides $m + pp'(m) + qq'(m)$ and that $0 < m + pp'(m) + qq'(m) < 3pq$ then either $m + pp'(m) + qq'(m) = pq$ or $2pq$.

• If $m + pp'(m) + qq'(m) = pq$ then we claim that $d(m; p, q) = 0$, Otherwise, if $d(m; p, q) > 0$ then there are integers $s, t \geq 0$ such that $ps + qt = m$. So

$$pp'(m) + qq'(m) + ps + qt = pq \rightarrow p(p'(m) + s) + q(q'(m) + t) = pq$$

So, p divides $q'(m) + t$ and q divides $p'(m) + s$ but $0 < q'(m) + t \leq p$ and $0 < p'(m) + s \leq q$ and thus $p = q'(m) + t$ and $q = p'(m) + s$ obtaining that $2qp = pq$ contadiction !

• if $m + pp'(m) + qq'(m) = pq$ then just notice that

$$m = p(q - p'(m)) + q(p - q'(m))$$

and thus $d(m; p, q) = 1$.

Proof. Suppose $0 < m < pq - p - q$.

We have that pq divides $m + pp'(m) + qq'(m)$ and that $0 < m + pp'(m) + qq'(m) < 3pq$ then either $m + pp'(m) + qq'(m) = pq$ or $2pq$.

• If $m + pp'(m) + qq'(m) = pq$ then we claim that $d(m; p, q) = 0$, Otherwise, if $d(m; p, q) > 0$ then there are integers $s, t \geq 0$ such that $ps + qt = m$. So

$$pp'(m) + qq'(m) + ps + qt = pq \rightarrow p(p'(m) + s) + q(q'(m) + t) = pq$$

So, p divides $q'(m) + t$ and q divides $p'(m) + s$ but $0 < q'(m) + t \leq p$ and $0 < p'(m) + s \leq q$ and thus $p = q'(m) + t$ and $q = p'(m) + s$ obtaining that $2qp = pq$ contadiction !

• if $m + pp'(m) + qq'(m) = pq$ then just notice that

$$m = p(q - p'(m)) + q(p - q'(m))$$

and thus $d(m; p, q) = 1$.

Ehrhart polynomial

A polytope is called integral (resp. rational) if all its vertices have integer (resp. rational) coordinates. Let t be a positive integer and let $i(P,t)$ be the number of lattices points in a d-dimensional polytope P dilated by a factor of t, that is

$$i(P,t) = \#(tP \cap \mathbb{Z}^d)$$

where $tP = \{(tx_1,\dots,tx_n) | (x_1,\dots,x_n) \in P\}$.

Theorem (Ehrhart 1962) Let P be an integral polytope of dimension d. Then, $i(P,t)$ is always a polynomial, that is

$$i(P,t) = e_d(P)t^d + \cdots + e_0(P)$$

$i(P,t)$ is called the Ehrhart polynomial.

Ehrhart polynomial

A polytope is called integral (resp. rational) if all its vertices have integer (resp. rational) coordinates. Let t be a positive integer and let $i(P,t)$ be the number of lattices points in a d-dimensional polytope P dilated by a factor of t, that is

$$i(P,t) = \#(tP \cap \mathbb{Z}^d)$$

where $tP = \{(tx_1,\ldots,tx_n) | (x_1,\ldots,x_n) \in P\}$.

Theorem (Ehrhart 1962) Let P be an integral polytope of dimension d. Then, $i(P,t)$ is always a polynomial, that is

$$i(P,t) = e_d(P)t^d + \cdots + e_0(P)$$

$i(P,t)$ is called the Ehrhart polynomial.

Ehrhart polynomial

A polytope is called integral (resp. rational) if all its vertices have integer (resp. rational) coordinates. Let t be a positive integer and let $i(P,t)$ be the number of lattices points in a d-dimensional polytope P dilated by a factor of t, that is

$$i(P,t) = \#(tP \cap \mathbb{Z}^d)$$

where $tP = \{(tx_1,\dots,tx_n) | (x_1,\dots,x_n) \in P\}$.

Theorem (Ehrhart 1962) Let P be an integral polytope of dimension d. Then, $i(P,t)$ is always a polynomial, that is

$$i(P,t) = e_d(P)t^d + \cdots + e_0(P)$$

$i(P,t)$ is called the Ehrhart polynomial.

Some facts :

(a) $e_0 = 1$, $e_d = vol(P)$, e_{d-1} volume of the $(d-1)$-dimensional facets of P all other coefficients remain a mystery.

(b) For $n = 2$ Ehrhart polynomial correspond to Pick's theorem.

(c) When P is a unimodular zonotope (a polytope that tiles the space) there is a nice interpretation of the coefficients in terms of the Tutte polynomial associated to P.

(d) If P is rational then $i(P, t)$ is not a polynomial but a quasipolynomial (a function $f : \mathbb{N} \longrightarrow \mathbb{C}$ of the form $f = c_d(t)t^d + \cdots + c_0(t)$ where each $c_i(t)$ is a perodic function - with integer period - and $c_d(t)$ not the zero function).

Some facts :

(a) $e_0 = 1$, $e_d = vol(P)$, e_{d-1} volume of the $(d-1)$-dimensional facets of P all other coefficients remain a mystery.

(b) For $n = 2$ Ehrhart polynomial correspond to Pick's theorem.

(c) When P is a unimodular zonotope (a polytope that tiles the space) there is a nice interpretation of the coefficients in terms of the Tutte polynomial associated to P.

(d) If P is rational then $i(P,t)$ is not a polynomial but a quasipolynomial (a function $f : \mathbb{N} \longrightarrow \mathbb{C}$ of the form $f = c_d(t)t^d + \cdots + c_0(t)$ where each $c_i(t)$ is a perodic function - with integer period - and $c_d(t)$ not the zero function).

Some facts :

(a) $e_0 = 1,\ e_d = vol(P),\ e_{d-1}$ volume of the $(d-1)$-dimensional facets of P all other coefficients remain a mystery.

(b) For $n = 2$ Ehrhart polynomial correspond to Pick's theorem.

(c) When P is a unimodular zonotope (a polytope that tiles the space) there is a nice interpretation of the coefficients in terms of the Tutte polynomial associated to P.

(d) If P is rational then $i(P,t)$ is not a polynomial but a quasipolynomial (a function $f : \mathbb{N} \longrightarrow \mathbb{C}$ of the form $f = c_d(t)t^d + \cdots + c_0(t)$ where each $c_i(t)$ is a perodic function - with integer period - and $c_d(t)$ not the zero function).

Some facts :

(a) $e_0 = 1$, $e_d = vol(P)$, e_{d-1} volume of the $(d-1)$-dimensional facets of P all other coefficients remain a mystery.

(b) For $n = 2$ Ehrhart polynomial correspond to Pick's theorem.

(c) When P is a unimodular zonotope (a polytope that tiles the space) there is a nice interpretation of the coefficients in terms of the Tutte polynomial associated to P.

(d) If P is rational then $i(P, t)$ is not a polynomial but a quasipolynomial (a function $f : \mathbb{N} \longrightarrow \mathbb{C}$ of the form $f = c_d(t)t^d + \cdots + c_0(t)$ where each $c_i(t)$ is a perodic function - with integer period - and $c_d(t)$ not the zero function).

What's the relationship between denumerants and Ehrhart polynomial?

Let $a_1, \ldots, a_n$ relatively prime integers. Consider the following rational polytope

$$P = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : x_i \geq 0, \sum_{i=1}^{n} a_i x_i \leq 1\}.$$

P has vertices $(0, \ldots, 0), (\frac{1}{a_1}, 0, \ldots, 0), \ldots, (0, \ldots, 0, \frac{1}{a_n})$. Thus geometrically, $d(m; a_1, \ldots, a_n)$ enumerates the lattices points on the skewed facet $(\sum_{i=1}^{n} a_i x_i = 1)$ of P

$g(a_1, \ldots, a_n)$ is the largest integer t such that the skewed facet of the dilated polytope tP contains no lattice point, that is, the largest integer t such that $d(t; a_1, \ldots, a_n) = 0$.

What's the relationship between denumerants and Ehrhart polynomial?

Let $a_1, \ldots, a_n$ relatively prime integers. Consider the following rational polytope

$$P = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : x_i \geq 0, \sum_{i=1}^{n} a_i x_i \leq 1\}.$$

P has vertices $(0, \ldots, 0), (\frac{1}{a_1}, 0, \ldots, 0), \ldots, (0, \ldots, 0, \frac{1}{a_n})$. Thus geometrically, $d(m; a_1, \ldots, a_n)$ enumerates the lattices points on the skewed facet $(\sum_{i=1}^{n} a_i x_i = 1)$ of P

$g(a_1, \ldots, a_n)$ is the largest integer t such that the skewed facet of the dilated polytope tP contains no lattice point, that is, the largest integer t such that $d(t; a_1, \ldots, a_n) = 0$.

What's the relationship between denumerants and Ehrhart polynomial ?

Let $a_1, \ldots, a_n$ relatively prime integers. Consider the following rational polytope

$$P = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : x_i \geq 0, \sum_{i=1}^{n} a_i x_i \leq 1\}.$$

P has vertices $(0, \ldots, 0), (\frac{1}{a_1}, 0, \ldots, 0), \ldots, (0, \ldots, 0, \frac{1}{a_n})$. Thus geometrically, $d(m; a_1, \ldots, a_n)$ enumerates the lattices points on the skewed facet $(\sum_{i=1}^{n} a_i x_i = 1)$ of P

$g(a_1, \ldots, a_n)$ is the largest integer t such that the skewed facet of the dilated polytope tP contains no lattice point, that is, the largest integer t such that $d(t; a_1, \ldots, a_n) = 0$.

What's the relationship between denumerants and Ehrhart polynomial ?

Let $a_1, \ldots, a_n$ relatively prime integers. Consider the following rational polytope

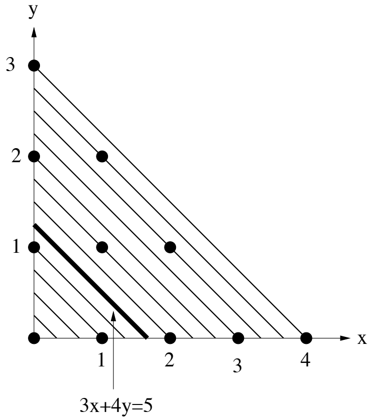
$$P = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : x_i \geq 0, \sum_{i=1}^{n} a_i x_i \leq 1\}.$$

P has vertices $(0, \ldots, 0), (\frac{1}{a_1}, 0, \ldots, 0), \ldots, (0, \ldots, 0, \frac{1}{a_n})$. Thus geometrically, $d(m; a_1, \ldots, a_n)$ enumerates the lattices points on the skewed facet $(\sum_{i=1}^{n} a_i x_i = 1)$ of P

$g(a_1, \ldots, a_n)$ is the largest integer t such that the skewed facet of the dilated polytope tP contains no lattice point, that is, the largest integer t such that $d(t; a_1, \ldots, a_n) = 0$.

Example : Let $a_1 = 3$ and $a_2 = 4$. Then $P = \{(x, y)|3x + 4y \leq 1\}$ and the hypothenuse of the t-dilated triangle is given by $3x + 4y = t$. This line has no integer points if $t = 5$ but it always does for any integer $t \geq 6$

Example : Let $a_1 = 3$ and $a_2 = 4$. Then $P = \{(x, y) | 3x + 4y \leq 1\}$ and the hypothenuse of the t-dilated triangle is given by $3x + 4y = t$. This line has no integer points if $t = 5$ but it always does for any integer $t \geq 6$



Gaps

Let $S = \langle a_1, \ldots, a_n \rangle$. The positive elements of $\mathbb{N} \setminus S$ are called the gaps of S. Let $N(S) = \#(\mathbb{N} \setminus S)$.

Theorem (R.A., 2007) Let $a, k \geq 1$ be integers and let $S = \langle a, a+1, \ldots, a+k \rangle$ be a semigroup with gaps $l_1 < \cdots < l_{N(S)}$. Let $v_m = (m+1)(a-1) - k\left(\frac{m(m+1)}{2}\right)$, $v_{-1} = 0$ and $r = \left\lfloor \frac{a-2}{k} \right\rfloor$. Then,

$$N(S) = v_r \text{ and } l_i = t_i(a+k) + i - v_{t_i - 1}$$

for each $i = 1, \ldots, N(S)$ where t_i is the smallest integer such that $v_{t_i} \geq i$.

Gaps

Let $S = \langle a_1, \ldots, a_n \rangle$. The positive elements of $\mathbb{N} \setminus S$ are called the gaps of S. Let $N(S) = \#(\mathbb{N} \setminus S)$.

Theorem (R.A., 2007) Let $a, k \geq 1$ be integers and let $S = \langle a, a+1, \ldots, a+k \rangle$ be a semigroup with gaps $l_1 < \cdots < l_{N(S)}$. Let $v_m = (m+1)(a-1) - k\left(\frac{m(m+1)}{2}\right)$, $v_{-1} = 0$ and $r = \left\lfloor \frac{a-2}{k} \right\rfloor$. Then,

$$N(S) = v_r \text{ and } l_i = t_i(a+k) + i - v_{t_i - 1}$$

for each $i = 1, \ldots, N(S)$ where t_i is the smallest integer such that $v_{t_i} \geq i$.

Gaps

Let $S = \langle a_1, \ldots, a_n \rangle$. The positive elements of $\mathbb{N} \setminus S$ are called the gaps of S. Let $N(S) = \#(\mathbb{N} \setminus S)$.

Theorem (R.A., 2007) Let $a, k \geq 1$ be integers and let $S = \langle a, a+1, \ldots, a+k \rangle$ be a semigroup with gaps $l_1 < \cdots < l_{N(S)}$. Let $v_m = (m+1)(a-1) - k\left(\frac{m(m+1)}{2}\right)$, $v_{-1} = 0$ and $r = \left\lfloor \frac{a-2}{k} \right\rfloor$. Then,

$$N(S) = v_r \text{ and } l_i = t_i(a+k) + i - v_{t_i - 1}$$

for each $i = 1, \ldots, N(S)$ where t_i is the smallest integer such that $v_{t_i} \geq i$.

Theorem (R.A., 2007) Let p, q be positive integers with $\gcd(p,q) = 1$. Let $g_k(\langle p,q\rangle)$ the number of gaps of $\langle p,q\rangle$ in the interval $[pq-(k+1)(p+q),\ldots,pq-k(p+q)]$, for each $0 \le k \le \left\lfloor \frac{pq}{p+q} \right\rfloor - 1$. Then,

$$g_k(\langle p,q\rangle) = \begin{cases} 1 & \text{if } k = 0 \\ 2(k+1) + \left\lfloor \frac{kq}{p} \right\rfloor + \left\lfloor \frac{kp}{q} \right\rfloor & \text{if } 1 \le k \le \left\lfloor \frac{pq}{p+q} \right\rfloor - 1. \end{cases}$$

Calculating $N(S)$

Theorem (Sylvester 1882) $N(\langle a_1, a_2\rangle) = \frac{1}{2}(a_1 - 1)(a_2 - 1)$.

Theorem (Brauer and Shockley 1962)

$$N(S) = \frac{1}{m} \sum_{w \in Ap(S;m)} w - \frac{1}{2}(m-1).$$

Calculating $N(S)$

Theorem (Sylvester 1882) $N(\langle a_1, a_2\rangle) = \frac{1}{2}(a_1 - 1)(a_2 - 1).$

Theorem (Brauer and Shockley 1962)

$$N(S) = \frac{1}{m}\sum_{w\in Ap(S;m)} w - \frac{1}{2}(m-1).$$

Calculating $N(S)$

Theorem (Sylvester 1882) $N(\langle a_1, a_2\rangle) = \frac{1}{2}(a_1 - 1)(a_2 - 1)$.

Theorem (Brauer and Shockley 1962)

$$N(S) = \frac{1}{m} \sum_{w \in Ap(S;m)} w - \frac{1}{2}(m-1).$$

Theorem (Brown and Shiue, 1993) Let $S(a,b)=\sum\{n|n\in\mathbb{N}\setminus\langle a,b\rangle\}$. Then,

$$S(a,b)=\frac{1}{12}(a-1)(b-1)(2ab-a-b-1).$$

Theorem (Rødseth 1994) Let $S_n(a,b)=\sum\{m^n|m\in\mathbb{N}\setminus\langle a,b\rangle\}$. Then,

$$S_{n-1}(a,b)=\frac{1}{n(n+1)}\sum_{i=0}^{n}\sum_{j=1}^{n-1}\binom{n+1}{i}\binom{n+1-i}{j}B_iB_ja^{n-j}b^{n-i}-\frac{1}{n}B_n.$$

where B_i are Bernoulli numbers.

Theorem (Brown and Shiue, 1993) Let $S(a,b)=\sum\{n|n\in\mathbb{N}\setminus\langle a,b\rangle\}$. Then,

$$S(a,b)=\frac{1}{12}(a-1)(b-1)(2ab-a-b-1).$$

Theorem (Rødseth 1994) Let $S_n(a,b)=\sum\{m^n|m\in\mathbb{N}\setminus\langle a,b\rangle\}$. Then,

$$S_{n-1}(a,b)=\frac{1}{n(n+1)}\sum_{i=0}^{n}\sum_{i=1}^{n-1}\binom{n+1}{i}\binom{n+1-i}{j}B_iB_ja^{n-j}b^{n-i}-\frac{1}{n}B_n.$$

where B_i are Bernoulli numbers.

Let g be a positive integer and let n_r be the number of numerical semigroups with *minimal set* of generators containing exactly g gaps.

Theorem (Bras-Amorós 2007) $n_g \geq n_{g-1} + n_{g-2}$ for all $g \leq 50$.

Let $n(g, r)$ be the number of numerical semigroups with g gaps and with minimal generating set of cardinality r.

Proposition (Eliahou and R.A. 2011) $n(g, 2) \geq 1$ for all g.

Let g be a positive integer and let n_r be the number of numerical semigroups with *minimal set* of generators containing exactly g gaps.

Theorem (Bras-Amorós 2007) $n_g \geq n_{g-1} + n_{g-2}$ for all $g \leq 50$.

Let $n(g, r)$ be the number of numerical semigroups with g gaps and with minimal generating set of cardinality r.

Proposition (Eliahou and R.A. 2011) $n(g, 2) \geq 1$ for all g.

Let g be a positive integer and let n_r be the number of numerical semigroups with *minimal set* of generators containing exactly g gaps.

Theorem (Bras-Amorós 2007) $n_g \geq n_{g-1} + n_{g-2}$ for all $g \leq 50$.

Let $n(g, r)$ be the number of numerical semigroups with g gaps and with minimal generating set of cardinality r.

Proposition (Eliahou and R.A. 2011) $n(g, 2) \geq 1$ for all g.

Let g be a positive integer and let n_r be the number of numerical semigroups with *minimal set* of generators containing exactly g gaps.

Theorem (Bras-Amorós 2007) $n_g \geq n_{g-1} + n_{g-2}$ for all $g \leq 50$.

Let $n(g, r)$ be the number of numerical semigroups with g gaps and with minimal generating set of cardinality r.

Proposition (Eliahou and R.A. 2011) $n(g, 2) \geq 1$ for all g.

Theorem (Eliahou and R.A. 2011) Let $g = 2^k$, $k \in \mathbb{N}$. Write $k + 1 = 2^t s$, $t \in \mathbb{N}$ and s odd. Then,

$$n(2^k, 2) = (s + 1)/2.$$

Question : what about $n(p^k, 2)$ for odd primes p ?

Theorem (Eliahou and R.A. 2011) There is a formula for $n(p^k, 2)$ for $k = 1, \ldots, 8$.

Theorem (Eliahou and R.A. 2011) Let $g = 2^k$, $k \in \mathbb{N}$. Write $k+1 = 2^t s$, $t \in \mathbb{N}$ and s odd. Then,

$$n(2^k, 2) = (s+1)/2.$$

Question : what about $n(p^k, 2)$ for odd primes p ?

Theorem (Eliahou and R.A. 2011) There is a formula for $n(p^k, 2)$ for $k = 1, \ldots, 8$.

Theorem (Eliahou and R.A. 2011) Let $g = 2^k$, $k \in \mathbb{N}$. Write $k + 1 = 2^t s$, $t \in \mathbb{N}$ and s odd. Then,

$$n(2^k, 2) = (s + 1)/2.$$

Question : what about $n(p^k, 2)$ for odd primes p ?

Theorem (Eliahou and R.A. 2011) There is a formula for $n(p^k, 2)$ for $k = 1, \ldots, 8$.

Remark :

$n(g,2) = \#\{(u,v) \in \mathbb{N}^2 | 1 \leq u \leq v, uv = 2g, \gcd(u+1, v+1) = 1\}$

So, we focus on factorizations $2p^k = uv$ with $u = p^{k-1}$ and $v = 2p$ and this factorization contributes 1 to $n(p^k, 2)$ if $\gcd(p^{k-1}+1, 2p+1) = 1$.

For, we need to know the prime factors of $2^m + 1$ for m odd.

This is an ancient open problem. It is not even known whether there are finitly or infinitely many Fermat or Marsenne primes, i.e., primes of the form $2^{2^t} + 1$ or $2^q - 1$ with $t \geq 1$ and q prime.

Remark :

$n(g,2) = \#\{(u,v) \in \mathbb{N}^2 | 1 \leq u \leq v, uv = 2g, \gcd(u+1, v+1) = 1\}$

So, we focus on factorizations $2p^k = uv$ with $u = p^{k-1}$ and $v = 2p$ and this factorization contributes 1 to $n(p^k, 2)$ if $\gcd(p^{k-1}+1, 2p+1) = 1$.

For, we need to know the prime factors of $2^m + 1$ for m odd.

This is an ancient open problem. It is not even known whether there are finitly or infinitely many Fermat or Marsenne primes, i.e., primes of the form $2^{2^t} + 1$ or $2^q - 1$ with $t \geq 1$ and q prime.

Remark :

$n(g,2) = \#\{(u,v) \in \mathbb{N}^2 | 1 \leq u \leq v, uv = 2g, \gcd(u+1, v+1) = 1\}$

So, we focus on factorizations $2p^k = uv$ with $u = p^{k-1}$ and $v = 2p$ and this factorization contributes 1 to $n(p^k, 2)$ if $\gcd(p^{k-1} + 1, 2p + 1) = 1$.

For, we need to know the prime factors of $2^m + 1$ for m odd.

This is an ancient open problem. It is not even known whether there are finitly or infinitely many Fermat or Marsenne primes, i.e., primes of the form $2^{2^t} + 1$ or $2^q - 1$ with $t \geq 1$ and q prime.

Remark :

$n(g,2) = \#\{(u,v) \in \mathbb{N}^2 | 1 \leq u \leq v, uv = 2g, \gcd(u+1, v+1) = 1\}$

So, we focus on factorizations $2p^k = uv$ with $u = p^{k-1}$ and $v = 2p$ and this factorization contributes 1 to $n(p^k, 2)$ if $\gcd(p^{k-1} + 1, 2p + 1) = 1$.

For, we need to know the prime factors of $2^m + 1$ for m odd.

This is an ancient open problem. It is not even known whether there are finitly or infinitely many Fermat or Marsenne primes, i.e., primes of the form $2^{2^t} + 1$ or $2^q - 1$ with $t \geq 1$ and q prime.

Symmetry

Let $g_S = \{g(s_1, \ldots, s_n) - s | s \in S\}$.

Remark : S and g_S are disjoint sets
(otherwise, $x = g(S) - s$ for some $s \in S$ and since $x \in S$ then $g(S) - s + s = g(S) \in S$!)

A semigroup S is called symmetric if $S \cup g_S = \mathbb{Z}$.

Theorem Semigroup $\langle p, q \rangle$ is always symmetric.

Symmetry

Let $g_S = \{g(s_1, \ldots, s_n) - s | s \in S\}$.

Remark : S and g_S are disjoint sets
(otherwise, $x = g(S) - s$ for some $s \in S$ and since $x \in S$ then $g(S) - s + s = g(S) \in S$!)

A semigroup S is called symmetric if $S \cup g_S = \mathbb{Z}$.

Theorem Semigroup $\langle p, q \rangle$ is always symmetric.

Symmetry

Let $g_S = \{g(s_1, \ldots, s_n) - s | s \in S\}$.

Remark : S and g_S are disjoint sets
(otherwise, $x = g(S) - s$ for some $s \in S$ and since $x \in S$ then $g(S) - s + s = g(S) \in S$!)

A semigroup S is called symmetric if $S \cup g_S = \mathbb{Z}$.

Theorem Semigroup $\langle p, q \rangle$ is always symmetric.

Symmetry

Let $g_S = \{g(s_1, \ldots, s_n) - s | s \in S\}$.

Remark : S and g_S are disjoint sets
(otherwise, $x = g(S) - s$ for some $s \in S$ and since $x \in S$ then $g(S) - s + s = g(S) \in S$!)

A semigroup S is called symmetric if $S \cup g_S = \mathbb{Z}$.

Theorem Semigroup $\langle p, q \rangle$ is always symmetric.

Symmetry

Let $g_S = \{g(s_1, \ldots, s_n) - s | s \in S\}$.

Remark : S and g_S are disjoint sets
(otherwise, $x = g(S) - s$ for some $s \in S$ and since $x \in S$ then $g(S) - s + s = g(S) \in S$!)

A semigroup S is called symmetric if $S \cup g_S = \mathbb{Z}$.

Theorem Semigroup $\langle p, q \rangle$ is always symmetric.

Theorem (R.A. and Rødseth 2009) Complete characterization of symmetry for $\langle a, a+d, \ldots, a+kd, c\rangle$ with $\gcd(a,d)=1$.

Theorem (R.A. and Rødseth 2009) Complete characterization of symmetry for $\langle a, b, c\rangle$.

Let $S=\langle a_1,\ldots,a_n\rangle$ and let $d_i=\gcd(a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_n)$. The *derived* semigroup of S is defined as the semigroup generated by $\{a_1/\prod_{j\neq 1} d_j, \ldots, a_n/\prod_{j\neq n} d_j\}$.

Theorem (Frőberg, Gottlieb and Hăggkvist 1987, R.A. and Rødseth 2009) $\langle a_1, a_2, a_3\rangle$ is symmetric if and only if its derived is generated by two elements.

Theorem (R.A. and Rødseth 2009) Complete characterization of symmetry for $\langle a, a+d, \ldots, a+kd, c\rangle$ with $\gcd(a,d)=1$.

Theorem (R.A. and Rødseth 2009) Complete characterization of symmetry for $\langle a, b, c\rangle$.

Let $S = \langle a_1, \ldots, a_n\rangle$ and let $d_i = \gcd(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$. The *derived* semigroup of S is defined as the semigroup generated by $\{a_1/\prod_{j\neq 1} d_j, \ldots, a_n/\prod_{j\neq n} d_j\}$.

Theorem (Frőberg, Gottlieb and Hăggkvist 1987, R.A. and Rødseth 2009) $\langle a_1, a_2, a_3\rangle$ is symmetric if and only if its derived is generated by two elements.

Theorem (R.A. and Rødseth 2009) Complete characterization of symmetry for $\langle a, a+d, \ldots, a+kd, c\rangle$ with $\gcd(a,d)=1$.

Theorem (R.A. and Rødseth 2009) Complete characterization of symmetry for $\langle a, b, c\rangle$.

Let $S=\langle a_1,\ldots,a_n\rangle$ and let $d_i=\gcd(a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_n)$. The *derived* semigroup of S is defined as the semigroup generated by $\{a_1/\prod_{j\neq 1} d_j, \ldots, a_n/\prod_{j\neq n} d_j\}$.

Theorem (Frőberg, Gottlieb and Hăggkvist 1987, R.A. and Rødseth 2009) $\langle a_1, a_2, a_3\rangle$ is symmetric if and only if its derived is generated by two elements.

Theorem (R.A. and Rødseth 2009) Complete characterization of symmetry for $\langle a, a+d, \ldots, a+kd, c\rangle$ with $\gcd(a,d)=1$.

Theorem (R.A. and Rødseth 2009) Complete characterization of symmetry for $\langle a, b, c\rangle$.

Let $S = \langle a_1, \ldots, a_n\rangle$ and let $d_i = \gcd(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$. The *derived* semigroup of S is defined as the semigroup generated by $\{a_1/\prod_{j\neq 1} d_j, \ldots, a_n/\prod_{j\neq n} d_j\}$.

Theorem (Frőberg, Gottlieb and Hăggkvist 1987, R.A. and Rødseth 2009) $\langle a_1, a_2, a_3\rangle$ is symmetric if and only if its derived is generated by two elements.

Vector generalization

Let $x_1, \ldots, x_n$ be d-dimensional integer vectors and let $A = (x_1, \ldots, x_n)$ be a $(d \times n)$-matrix containing a basis. A pseudo-conductor of vectors $x_1, \ldots, x_n$ is a vector $h \in \{Ax | x \in \mathbb{Z}_+^n\}$ such that any integral vector of the set $h + \{Ax | x \in Q_{\geq 0}\}$ is a nonnegative integer combination of $x_1, \ldots, x_n$.

Theorem Let $\{\Omega_1, \ldots, \Omega_r\}$ be the set of all $(d \times d)$-matrices with columns choosen from A. Then,

$$\gcd(|det(\Omega_1)|, \ldots, |det(\Omega_r)|) = 1$$

if and only if a pseudo-conductor exists.

Vector generalization

Let $x_1, \ldots, x_n$ be d-dimensional integer vectors and let $A = (x_1, \ldots, x_n)$ be a $(d \times n)$-matrix containing a basis. A pseudo-conductor of vectors $x_1, \ldots, x_n$ is a vector $h \in \{Ax | x \in \mathbb{Z}_+^n\}$ such that any integral vector of the set $h + \{Ax | x \in Q_{\geq 0}\}$ is a nonnegative integer combination of $x_1, \ldots, x_n$.

Theorem Let $\{\Omega_1, \ldots, \Omega_r\}$ be the set of all $(d \times d)$-matrices with columns choosen from A. Then,

$$\gcd(|det(\Omega_1)|, \ldots, |det(\Omega_r)|) = 1$$

if and only if a pseudo-conductor exists.

Theorem Let $x_1, \ldots, x_n$ be d-dimensional integer vectors and let $x_0 \in \{Ax | x \in \ Q_{\geq 0}\}$ such that $x_0, x_1, \ldots, x_n$ generated $\mathbb{Z}^n$. Then,

$$p = |det(A)|x_0 - \sum_{i=0}^{n} x_i$$

is a pseudo-conductor.

Exemple : For $n = 1$, $x_1 = a$ and $A = (a)$ in this case we take $x_0 = b > a$ (which is in the cone generated by a).
Therefore, $det(A) = a$ and
$p = |a|b - (a + b) = ab - a - b = g(a, b)$.

Theorem Let $x_1, \ldots, x_n$ be d-dimensional integer vectors and let $x_0 \in \{Ax | x \in \ Q_{\geq 0}\}$ such that $x_0, x_1, \ldots, x_n$ generated $\mathbb{Z}^n$. Then,

$$p = |det(A)|x_0 - \sum_{i=0}^{n} x_i$$

is a pseudo-conductor.

Exemple : For $n = 1$, $x_1 = a$ and $A = (a)$ in this case we take $x_0 = b > a$ (which is in the cone generated by a).
Therefore, $det(A) = a$ and
$p = |a|b - (a + b) = ab - a - b = g(a, b)$.