The lattice reduction algorithm and applications (LLL and PSLQ)

Simon Plouffe
Centre for Experimental &
Constructive Mathematics

Simon Fraser University
BC, CANADA

Outline...

1) Continued fractions and the Euclidian Algorithm
2) The 60 degrees algorithm of Gauss
3) Generalized Euclidian algorithm
4) An application to LDE with polynomial coeff.
5) Results
6) Papers and books.

1) Continued fractions and Euclidian algorithm.

They are known since (at least) the invention of the well-tempered scale. Why ?

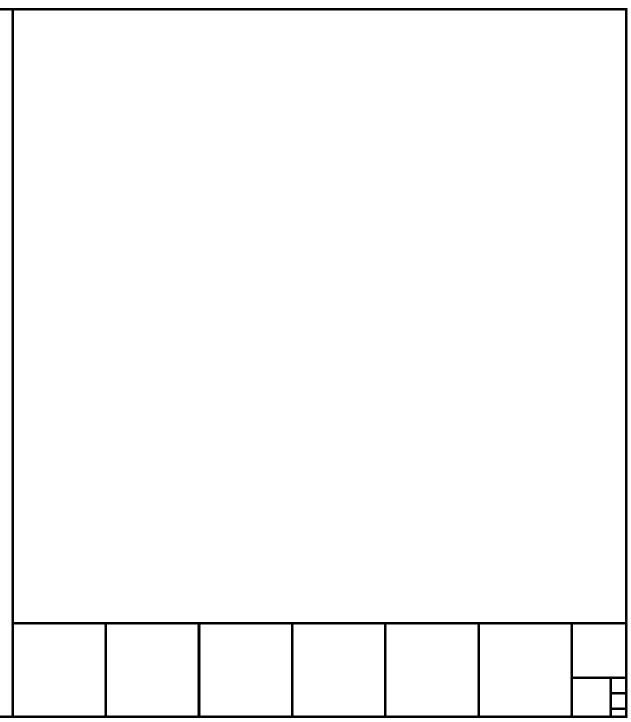
Find a good rational value of 2^(1/12) =
1.059463094359295... = v
and the fact that v**7 is almost 3/2, means that log(2)*(7/12) = log(3/2). The next BEST choice would have been the scale with 53 semi-tones, existed once but abandonned (~1920).

Rational approximations and continued fractions are natural in a sense that for a given x in R, x being irrational, the BEST rational approximation if the denominator is not bigger than M is given by the continued fraction development of x. Example if x=1.868132 then

Continued fraction of 1.868132...
is < 1,1,6,1,1,2,...

is given by the geometrical construction of a rectangle of sides 1 and 1.868132...
We remove SQUARES and count them.

Note : for ϕ we would obtain 1,1,1,1,1,1,....



To obtain the numbers : [1,1,6,1,1,2,... we can construct the rectangle but (of course) we use Euclidian algorithm.

We divide 1/x, take the quotient,
then the fractional part of 1/x : –1/x″.

and then go to the We divide...

If x is RATIONAL the algorithm STOPS eventually, if x is irrational itnever stops. Useful for constructing sprockets (engrenages), to play a numerical game with your pocket calculator, admire some paintings, the Parthenon in Greece is builded with rectangles of sides 1/1.6180339887...

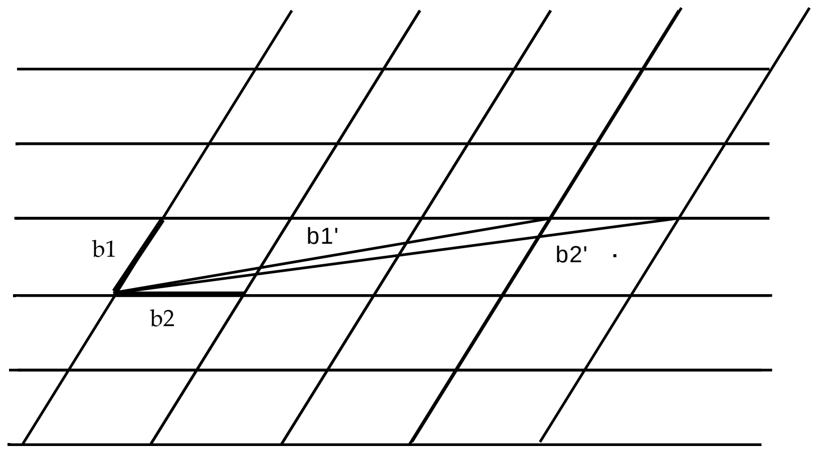
So, this algorithm can be used to solve the problem of having a good rational to approximate x. That is : x * b = a. Almost equal since a and b are in $\mathbb{Z}$ and x is irrational.

The problem was solved. No more games. Until Gauss asked (and othersbefore him). Yes but what if we have x and y at the same time ?

We would then have to solve x*a + y*b + c = 0
(almost 0, since a,b,c are integers). Gauss (as usual) solved the problemby taking is favourite figure (the unit circle) and came with his 60Γ algorithm.

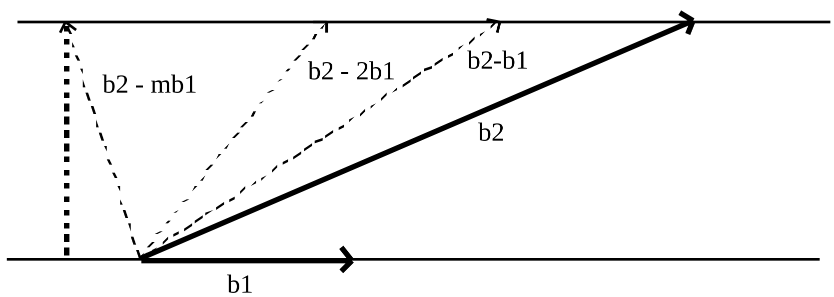
2) The 60Γ algorithm of Gauss

First we take 2 vectors in the plane, b1 and b2.
We can suppose that b2 ¿ b1, if not we rename them, ok.



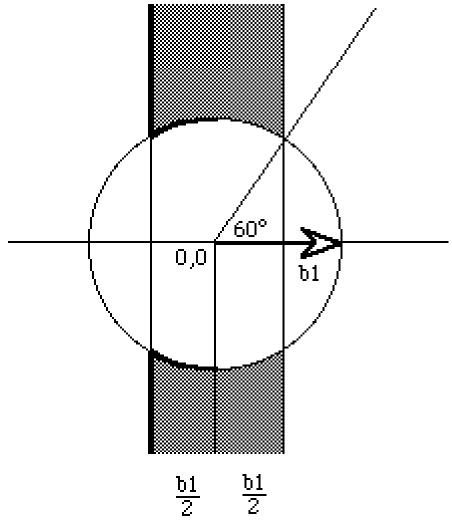
Le réseau est engendré par les vecteurs b1 et b2. On peut générer le même réseau en prenant les 2 vecteurs b1' et b2' qui sont des combinaisons linéaires des 2 premiers. Ici b1'=3*b2+b1 et b2'=4*b2+b1. La question consiste à savoir étant donné un réseau quelle est la base minimale.

The 2 vectors are generating a LATTICE.
The essential part of what Gauss found is that the same lattice can be generated by 2 vectors which are linear combinations of the 2 starting vectors. These 2 final vectors CAN be shorter, meaning the length. Also, they will bemore orthogonal, forming an angle of at least 60 degrees : AH !, here is from what the name come.



So, with the help of the figure we see that we canremove a certain number of times b1 from b2 and still have a lattice essentially the same. To stop we wait that theorthogonal projection of b2 over the b1 axe makes an angle of 60Γ at least.

In fact this is an equivalence class, more than that, this set of representation form a group.



Here we finally find the vectors lying in the shaded region.More precisely we havethe following...

Take 2 vectors, b1 et b2 linearly independants with b2¿b1.

Repeat until —b2— ﬄ —b1—
    exchange b2 and b1
    Replace b2 by b2 =b2 - m*b1 with m that satisfies the conditions.
end.

Simple !,

Yes for 2 values it goes well. The algorithm is not exactly what we would call thenatural generalization of the EA in 2 dimensions, but it works.

The problem came when someone asked, what if we have now, x, y and z?Apparently, Kronecker, Minkowski,and many others tried to graspwhat was behind the continued fractions ---¿ Euclidian algorithm, simultaneous approximations ---¿ proper generalization.

For further explanations see (in Maple) :

?kronecker ?minkowski ?lattice

First, we need a proper definition of what we are looking for in terms of Distanceand Angle. The equivalent of the 60Γdoes not work with a sphere in 3 dimensions.

For example, the formulation is : Find a Z-linear relation with k real numbers, Weare searching for the SHORTEST possible vectors BUT at the same time looking at vectorsthat are near orthogonal .

Second, the fact that (for example) x,y,z are irrational then we have to deal with irrationals (in a computer) and be sure when to stop in terms of numerical precision. In other words, the zero of the machine.

For the EA, the time of execution in term of STEPS is known and easily achieved, the same with the 60Γalgorithm : feasible by hand.

From that, it waited until 1979. Ferguson and Forcade came with a formulation of the problem in modern terms. (lots of technical details omitted),

The main idea was that YES we can do it BUT at what cost ?, They proved that (original paper), it can be done in polynomial time for k entries. Not very effective in terms of the exponent. (n^2 is not too bad but n^8 is horrible).

Then in 1982, an idea (recycled) from the original Gauss paper (60 degrees) came from Europe (Kannan & al.). This is what became known as the Lenstra-Lenstra-Lovasz (LLL) algorithm or the lattice reduction algorithm. In that context, the x s could be complex or real.

In 1986, Ferguson-Forcade-Bailey came with a reasonnable polynomial time (interesting enough for mortal humans). Their idea was essentially giving the same results as the LLL algorithm but formulated differently. Apparently the current implementation of FFB is the most efficient but does not apply so easily to arbitrary x s (complex or real), x being too big or too small .

Here are some difficulties for an implementation : Let s say we are looking for a linear combination of the powers of the same real number x. That is,(for k fixed),

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots a_k x^k = 0$$

Then if the a s are integers (could be rational), it implies that for a small zero this would test if x is algebraic.

Given that zero (not smaller than the smallest number), then the a s are limited to 1/0 in size. If x is near 1, then for fixed k, x**k will be smaller than that number.

If we have k constants a, they are even more limited.

IF x is NOT near 1, there is a limit to k.
IF k is BIG then x MUST be small.

So, the algorithm works IF these conditions are satisfied. These are the usual limitations of an algorithm that can inverse a matrix with real entries : near singular values.

The same would apply for a formulation in term of a Z-linear combinations of arbitrary k vectors. They have to be of the same size.

The LLL-PSLQ algorithms are deterministic. It means that it does not use high speed guessing or Monte-Carlo methods. For example, let s take ¯ , e and gamma and try to find a Z-linear combination, that is :

$$a\pi + bE + c\gamma + d = 0$$

So, by using HSG we can find (not too bad)relations but it may take time. WE fix a,b,c,d being randomly chosen among an interval of integers and we keep the quadruplet ONLY when it is near 0. Or we could use a brute force method, we construct a table of n*Pi, sort them, construct a huge table of m*exp(1) and sort them, we look for fuzzy matchs and keep those (n,m) we then construct another huge table of p*gamma...(sort, fuzzy math them).

These methods are working for Mickey Mouse examples but the method has limits exp(Pi)-Pi =19,999099979...
Or this one : g*Catalan -G(7/12) = -1 'very' nearly.

If we think a little about it, any problem that can be linearized is a potential candidate for LLL.

--¿ powers of a given number x, if we have a relation then we test if x is algebraic.

--¿ a combination of real constants. In 1957 , Good noticed that the ratio of the mass of proton to electron is near 6*Pi^5, but an experiment conducted by Ferguson and Bailey found that there are too many to be considered seriously. They also tried with a bunch of real numbers: Zeros of Riemann Zeta function, the Feigenbaum constant, gamma,Pi, Zeta(3), Zeta(5), ...
They found nothing with that but later found that the Zwinnterton-Dyer constant is algebraic of degree 12.
Eddington formulated a complicated theory with the fine structure constant (at the time it was 137), but later it was found to be 137,03... he came out with another theory. These ideas were tested also : Nothing really interesting exist with 10 digits or less.

--¿ If we have 2 quantities, a and b, we can test if they are algebraically independant. We list 1,a,b, ab, a^2b,a^2b^2, ... it may (with actual computers) be tested up to degree 8.

--¿ Fermat had a method of factoring using the fact that a number n could be represented or not by a quadratic form. Today there is a way to use LLL to find very particular representation of n using elliptic curves. The coefficients of those can be found using LLL.

An application to Linear Differential Equations with polynomial coefficients

The Problem :

Given A = (a_0, a_1, a_2, ... a_k) a_i are in Z.

We want to verify automatically that

$$S(z) = \sum_{n \geq 0} a_n z^n$$

is algebraic.

In other words,

$$\sum c_{ijk} S(z)^j z^k = 0$$

Where is this coming from ?

(A long time ago), puzzled by playing the number game on my programmable calculator. I stumbled on the number -51= 7.14142842854285... a nice number with a pattern...
In fact by fooling around it, -51/14 is more interesting.
,the number 0.510102030610203...
(combinatorialists) would recognize that we have the sequence 1,1,2,3,6,10,20,30,... This is the zig-zag Pascal central sequence !.

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
...

Yes but less vernacular would be to say that the sequence is in fact generated by an algebraic generating function. That is the two central columns can be generatedby expanding, Hansel and Gretel here.

$$\frac{1}{(1 - 4\,z)^{1/2}}$$

$$1/2\,\frac{-1 + 4\,z + (1 - 4\,z)^{1/2}}{1 - 4\,z}$$

So, by putting z=1/100 we have the phenomena explained.

If we think about what we have we can come with this General Idea

$$Ly(x) = 0$$

gfun (sequence to P-recurrence)

Generate first terms

Evaluate at small point

Heat LLL and collect information (coefficients)

Find algebraic equation with a numerical gizmo-trick.

We could certify using gfun + comparison.

This would be a semi-algorithm.

Statement of the semi-algorithm

we have

$$P_k(x)y^{(k)}(x)+P_{k-1}(x)y^{(k-1)}(x)+\ldots+P_1(x)y^{(1)}(x)+P_0(x)y(x)=0$$

or $\quad L\,y(x) = 0$ for short

We want to find an algebraic solution.

One way to solve that problem: gfun

share library of MapleV
ftp to Waterloo.
F. Bergeron,
S. Plouffe,
<u>B. Salvy</u>,
<u>P. Zimmermann</u>
just type : readshare(gfun,calculus);
with(gfun);

With only one command :listtoalgeq( );

It uses undetermined coefficients method.
Example : Catalan Numbers : 1,2,5,14,42,...

at the terminal prompt...

```
-- [1,1,2,5,14,42,132,429,...];

-- listtoalgeq( ,S(z));
```

after a few centi-seconds...

$$1 - S(z) + z\, S(z)^2$$

The positive root w.r.t S(z) is,

$$\frac{1}{2}\,\frac{1 - (1 - 4\,z)^{1/2}}{z}$$

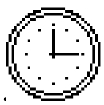
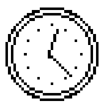
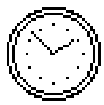
So, we expand this into a series and we get the so-called Catalannumbers. What is the problem with that ?

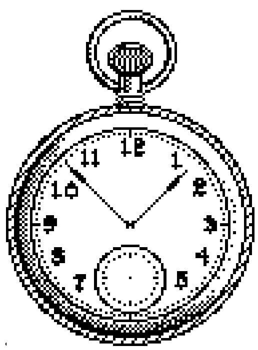
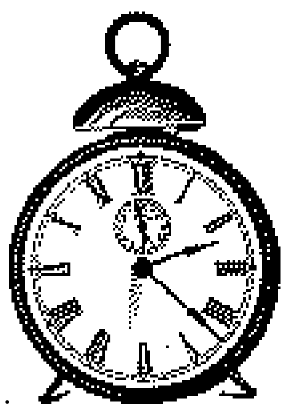
This approach is limited.

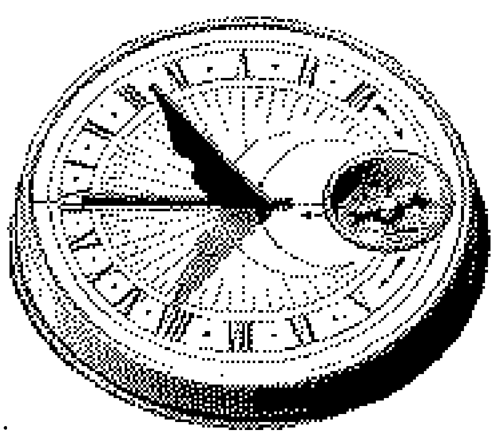
A = (1,1,1,3,16,75,309,1183,...)

J.W. Moon
Journal of
Combinatorial Theory B,
Vol 21, PP. 74 (1976)
Related to tournaments.

¿ listtoalgeq(,A(z));

then ... ... ... ... ...

... ... ....

... ...

and so on.

Another solution is

a method based on the LLL algorithm.

The problem can be solved in polynomial time.

Essentially the LLL algorithm can do the following thing.

(It can do a lot more also.)

From a in $\mathbb{R}$ ----------¿ P(a) being the a polynomial from which a is a root.

LLL gives us the minimal polynomial in polynomial time.

(with smallest coeffs.).
P(a) having coefficients in $\mathbb{Q}$. We know this can be done.

Some important remarks.

If S(z) is algebraic then

1) c such that $[z^n]\, S(z) \approx c^n$,we suppose c¿1. This is a necessary condition.

2) If m in N then S(1/m) is an algebraic number.

3) If 1/m ¡¡ c then S(1/m) can be evaluated with great numerical precision. The smaller is 1/m the better is the precision.

4) The sequence A=(a_0, a_1, a_2, ... ,a_k) is P-recurrent or D-finite. We can say that it satisfies a linear reccurence with polynomial coefficients. It has to be.
[Comtet 64, Stanley 80]
These 2 definitions are equivalent and GFUN can go from one representation to the other. If we have a algebraic equation--- LDE (or P-recurrence) , it is the converse which is not solved yet.LDE with polynomial coefficients = P-recurrence. But not coefficients to coefficients (unfortunately).

5) Once a P-recurrence is found for a given sequence we can calculate as much terms as we want in almost linear time with respect to n.

Let s take back our example,

A=(1,1,1,3,16,75,309,1183,...) with gfun , we search for a P-recurrence with the method mentioned earlier.

By using the command listtorec(); and a few seconds of cpu time.

This same recurrence can be used to calculate many hundreds of terms on the sequence in linear time.

The command rectoproc(); can write for us the procedure for doing so.

The command listtoseries(); will simply put this sequence into a huge serie.

The new serie S(z) (with many hundreds terms) can now be evaluated at S(1/m), S(1/m+1), ...

We then calculate :

$$P_{\min}(S(\frac{1}{m+i})) = P_i(x)$$

If the family of the polynomials $P_i(x)$ is compatible :

Meaning that if the D^r of the x^j are stable then the $P_i(x)$ are candidates.

It will be only necessary then to use the ordinary Newton interpolation formula. (the standard command interp(); of MapleV does that).

So we simply type...

```
---listtorec(sequence,a(n));

[{a(2) = 1, a(1) =
                         2                        2
     (- 2/3 n - 4/3 n ) a(n) + (- 1 + n + n ) a(n + 1)

                           2                                     2         3
 + (1/2 - 1/3 n - 1/6 n ) a(n + 2) + 1/2 + 1/6 n - 1/6 n  + 1/2 n
}]
```

and then we transform that into a automatic procedure...

```
--- rec:=rectoproc(",a(n));


rec :=proc(n)
 options remember;
     if not type(n,nonnegint) then ERROR(`invalid arguments`) fi;
     (28*procname(n-2)*n-24*procname(n-2)-8*
     procname(n-2)*n^2+6*procname(n-1)-18*procname(n-1)*n+6*
     procname(n-1)*n^2-27+41*n-19*n^2+3*n^3)/(-3-2*n+n^2)
 end;
```

This enables us to calculate MANY terms of the sequence (a few hundreds are usually enough). We then evaluate at a small point the series. For example, with z=1/100 we get,

vf(1)=1.0101031678212823716552055561609286005621598883696894333057529335554251502946005895235476218
779502658194451441638078870571504439504376872895472273851614986495234010381316955783224517854275313
928538072030439238987853080896923313046663

We recognize the first few terms of the sequence...

We just have to use (then) ALGDEP of Pari-GP.
WE are in Maple and to exit from it and to pass from Pari-GP back to Maple we use (Unix piping of files).Maple is loosy at formating numbers but in the process we use scripts to format the numbers properly.

WE can now collect our polynomials from ALGDEP of Pari-GP.

$$922556408004\,x^2 - 9041033588479200\,x + 9131435376040000$$
$$980100000000\,x^2 - 9799999702020000\,x + 9897020403050401$$
$$1040604010000\,x^2 - 10614139675759200\,x + 10718190400203216$$
$$1104189046416\,x^2 - 11486856353906376\,x + 11598369273824917$$
$$1170979365924\,x^2 - 12421725705345216\,x + 12541154909460736$$
$$1241102946304\,x^2 - 13422503799519360\,x + 13550326173504225$$
$$1314691560000\,x^2 - 14493133991044800\,x + 14629850124065296$$
$$1391880848400\,x^2 - 15637754317171560\,x + 15783889435204501$$
$$1472810396836\,x^2 - 16860705112257696\,x + 17016810038701632$$
$$1557623810304\,x^2 - 18166536843458976\,x + 18333188987567041$$
$$1646468789904\,x^2 - 19560018171877920\,x + 19737822545544400$$
$$1739497210000\,x^2 - 21046144243456200\,x + 21235734506893941$$

There is a pattern visible there...We collect the coefficients of EACH degree and interpolate using interp(); of Maple.

--- interp(POLYNOMS(i),t,100);

$$(1 - 9z + 32z^2 - 57z^3 + 54z^4 - 24z^5 + 4z^6 - t + 10tz - 42tz^2 + 98tz^3 - 137tz^4 + 112tz^5 - 48tz^6 + 8tz^7 + t^2z^2 - 8t^2z^3 + 26t^2z^4 - 44t^2z^5 + 41t^2z^6 - 20t^2z^7 + 4t^2z^8) / z^8$$

This is an algebraic equation. We used 100 since we had the interpolation point 1/100 Now we have to solve this eqaution to get the CLOSED algebraic generating function. We could stop there and say we have a solution . But un this case, it is of degree 2, with respect to t.

We just have then to solve with respect to t, take the positive solution and VOIL .

$$-1/2 \left(\frac{-1 + 10z - 42z^2 + 98z^3 - 137z^4 + 112z^5 - 48z^6 + 8z^7}{z^2 (2z-1)^2 (z-1)^4} \right.$$

$$\left. \frac{(-(-1+4z)(2z-1)^4 (z-1)^8)^{1/2}}{z^2 (2z-1)^2 (z-1)^4} \right)$$

This is (by expanding into a series) now easy to verify that IT IS indeed the solution It constitutes a computer-proof of it. Since we can construct the differential equation-P-recurrence. If it is the same then difference is 0. We can also
verify many terms of the sequence being the same.

Of course, that method was used extensively over ALL sequences in the EIS at the time We found about 25 original generating functions not found by other methods (BruteForce method).

1, 2, 9, 54, 378, 2916, 24057, 208494, 1876446, 17399772, 165297834, 1602117468, 15792300756,157923007560, 1598970451545, 16365932856990
Rf. : CJM 15 254 63; 33 1039 81. JCT 3 121 67.

$$\frac{-1 + 18 z + (-(12 z - 1)^3)^{1/2}}{54 z^2}$$

1, 3, 12, 56, 288, 1584, 9152, 54912, 339456
Rf. : CJM 15 269 63.

$$\frac{3 (1 - 8 z)^{1/2} + 8 z - 3 (1 - 8 z)^{3/2}}{4 (1 + (1 - 8 z)^{1/2})^3 z}$$

1, 0, 4, 6, 24, 66, 214, 676, 2209,7296, 24460, 82926, 284068, 981882, 3421318, 12007554, 42416488, 150718770, 538421590, 1932856590, 6969847484
Rf. : CJM 15 265 63.

$$\frac{(1 + z) ((- 4 z + 1)^{3/2} - 1 + 6 z - 6 z^2 - 4 z^3 - 6 z^4) + 4 z^5}{2 (2 z^5 (z + 2)^3 (1 + z))}$$

1, 3, 10, 33, 111, 379, 1312, 4596, 16266, 58082, 209010, 757259,2760123, 10114131, 37239072, 137698584, 511140558, 1904038986, 7115422212, 26668376994
Rf. : IC 16 351 70.

$$\frac{1 - 3 z - z^2 - (- (- 1 + 4 z) (- 1 + z + z^2)^2)^{1/2}}{2 (2 z^4 + z^5)}$$

1, 4, 15, 54, 193, 690, 2476, 8928, 32358, 117866, 431381, 1585842, 5853849, 21690378, 80650536, 300845232, 1125555054, 4222603968, 15881652606
Rf. : IC 16 351 70.

$$\frac{1 - 4 z + z^2 + 2 z^3 - (- (- 1 + 4 z) (z^2 + 2 z - 1)^2)^{1/2}}{2 (2 z^5 + z^6)}$$

1, 14, 120, 825, 5005, 28028, 148512, 755820, 3730650, 17978180, 84987760, 395482815
Rf. : CAY 13 95. AEQ 18 385 78.

$$\frac{1/2 (1 - 21 z + 180 z^2 - 800 z^3 + 1920 z^4 - 2304 z^5 + 1024 z^6}{(z^5 (4 z - 1)^5)}$$

$$-\ \frac{-\left(-\left(10 z^{4} - 50 z^{3} + 40 z^{2} - 11 z + 1\right)^{2} (4 z - 1)^{5}\right)^{1/2}\ )}{(z^{5} (4 z - 1)^{5})}$$

1, 1, 1, 3, 16, 75, 309, 1183,4360, 15783, 56750, 203929, 734722, 2658071, 9662093, 35292151, 129513736, 477376575, 1766738922, 6563071865, 24464169890

Rf. : JCT B21 75 76.

$$\frac{- 1/2 \left(- 1 + 10 z - 42 z^{2} + 98 z^{3} - 137 z^{4} + 112 z^{5} - 48 z^{6} + 8 z^{7}\right.}{(z^{2} (2 z - 1)^{2} (z - 1)^{4})}$$

$$+ \quad \frac{\left(- (- 1 + 4 z) (2 z - 1)^{4} (z - 1)^{8}\right)^{1/2}\ )}{(z^{2} (2 z - 1)^{2} (z - 1)^{4})}$$

1, 3, 9, 25, 69, 189, 518, 1422, 3915, 10813, 29964, 83304, 232323, 649845, 1822824, 5126520, 14453454, 40843521, 115668105, 328233969, 933206967, 2657946907, 7583013474

Rf. : JCT A23 293 77.

$$\frac{1 - 3 z + 2 z^{3} - \left(- (3 z^{2} + 2 z - 1) (- 1 + 2 z)^{2}\right)^{1/2}}{2 z^{6}}$$

1, 4, 14, 44, 133, 392, 1140, 3288, 9438, 27016, 77220, 220584, 630084, 1800384, 5147328, 14727168, 42171849, 120870324, 346757334, 995742748, 2862099185
Rf. : JCT A23 293 77.

$$\frac{1 - 4 z + 2 z^{2} + 4 z^{3} - z^{4} - (- (- 1 + 2 z + 3 z^{2}) (1 - 3 z + z^{2} + z^{3})^{2})^{1/2}}{z^{8}}$$

1, 5, 20, 70, 230, 726, 2235, 6765, 20240, 60060, 177177, 520455, 1524120, 4453320, 12991230, 37854954, 110218905, 320751445, 933149470, 2714401580, 7895719634
Rf. : JCT A23 293 77.

$$\frac{- 1/2 (- 1 + 5 z - 5 z^{2} - 5 z^{3} + 5 z^{4} + z^{5}}{z^{10}} +$$

$$\frac{(- (z + 1) (3 z - 1) (z^{2} + z - 1)^{2} (z^{2} - 3 z + 1))^{1/2})}{z^{10}}$$

1, 6, 27, 104, 369, 1242, 4037, 12804, 39897, 122694, 373581, 1128816, 3390582, 10136556, 30192102, 89662216, 265640691, 785509362, 2319218869, 6839057544
Rf. : JCT A23 293 77.

$$\frac{1/2 (1 - 6 z + 9 z^{2} + 4 z^{3} - 12 z^{4} + 2 z^{6}}{z^{12}} -$$

$$\frac{(- (z + 1) (3 z - 1) (z - 1)^{2} (2 z - 1)^{2} (2 z^{2} + 2 z - 1))^{1/2})}{z^{12}}$$

1, 2, 6, 16, 45, 126, 357, 1016, 2907, 8350, 24068, 69576, 201643, 585690, 1704510, 4969152, 14508939, 42422022, 124191258, 363985680, 1067892399, 3136046298, 9217554129
Rf. : Comtet Louis, Advanced Combinatorics, p. 78.

$$\frac{z + (z + 1)^{1/2} (1 - 3 z)^{1/2} - 1}{2 (z^2 (z + 1)^{1/2} (1 - 3 z)^{1/2})}$$

1, 3, 9, 26, 75, 216, 623, 1800, 5211, 15115, 43923
Rf. : AAM 9 340 88.

$$\frac{1 - 3 z - (- (3 z^2 + 2 z - 1) (- 1 + 2 z)^2)^{1/2}}{2 (3 z^4 - z^3)}$$

Bibliography

[AS1] M. Abramowitz and I. A. Stegun, Handbook of Mathematical Functions, National Bureau of Standards, Washington DC, 1964; Dover, NY, 1965.

[BaKa] A. Bachem, R. Kannann, Lattices and the basis reduction algorithm, Carnegie Mellon University, rapport interne. 1984.

[BP] F. Bergeron, S. Plouffe, Computing the generating function of a serie given its first terms, Rapport de recherche #164, Universit du Qubec Montral, octobre 1991. Prepublication, Journal of Experimental Mathematics 1992.

[Cohen] Henri Cohen, A Course in Computational Algebraic Number Theory, Springer Verlag, Grad. Text in Mathematics, #138.

[Comtet74] Comtet, L, Advanced Combinatorics, Reidel 1974.

[Comtet64] Comtet, L, Calcul pratique des coefficients de Taylor d une fonction algbrique L enseignement Mathmatique 10 (1964), 267-270.

[gfun] B. Salvy, P. Zimmermann, Gfun: A Maple Package for the manipulation of Generating and holonomic functions in One Variable. Rapport Technique, INRIA, Novembre 1992.

[GKP] R. L. Graham, D. E. Knuth and O. Patashnik, Concrete Mathematics, Addison-Wesley, Reading, MA, 1990.

[Kannan] Kannan R., Algorithmic Theory of Numbers, Annual Review of Computer Science, vol. 2, (1987), pp. 231-267.

[LLL] Kannan, Lenstra, Lovasz, 16Th ACM Symposium on the Theory of Computation, (1984).

[M5] B.W. Char, K.O. Geddes, G.H. Gonnet, B.L. Leong, M.B. Monagan, S.M. Watt, MAPLE V Library Reference Manual, Springer Verlag, (1991), Waterloo Maple Publishing.

[Pari] C. Batut, D. Bernardi, H. Cohen, M. Olivier, User s guide to PARI-GP, Version 1.36, Univers Bordeaux I, document interne, 8 Dcembre 1991.

[Plo] S. Plouffe, Approximations de sries gnratrices et quelques conjectures, Mmoire de Matrise, Universit du Qubec Montral, Aot 1992.

[Plouffe,Sloane] The Encyclopedia of Integer Sequences, Academic Press, San Diego, 1995.

[Sl] N.J.A. Sloane, A Handbook of Integer Sequences, Academic Press, New York, 1973.

[Sta80] R. Stanley, Differentiably finite power series, European Journal of Combinatorics, vol. 1,(1980),p.175-188.

[Tutte] W. T. Tutte, A Census of planar maps, Canadian Journal of Mathematics, Vol. 15, (1963) page 249-271.

Abbreviations of references

[AAM] Advances in Applied Mathematics

[CAY] A. Cayley, Collected Mathematical Papers, Vols. 1--13, Cambridge Univ. Press, London, 1889--1897.

[CJM] Canadian Journal of Mathematics

[JCT] Journal of Combinatorial Theory.

[IC] Information and Control.

[AEQ] Aequationes Mathematicae.

[C1] L. Comtet, Advanced Combinatorics, Reidel, Dordrecht, Holland, 1974.

In a mail from Gilbert Labelle (UQAM)1993.

Cher Simon(acker),

En rapport avec le calcul de la fraction limite du nombre de noeuds d'un quadtre
e
aleatoire ayant 2, 3 ou 4 enfants, j'ai besoin d'une meilleure comprehension de
la
constante suivante :

C = int(ln(t)*ln(1-t)/(1+t), t = 0 .. 1)
= 0.24307035167006157756270472396758221716815796300633230408140831530120777467206658987650326814

En fait, j'ai pu montrer que la constante C est de la forme

C = A + B - Pi^2*ln(2)/6 ou A et B sont donnees par

A = sum(H(1, k)/k**2/2**k, k = 1 .. infinity)
= 0.63196619783816790666244823201527531815667137165817275551526056796541176920941569629429336479
evalue par moi : .6319661978381679066624482320152753181566713716581727555152605680

B = sum(H(2, k)/k/2**k, k = 1 .. infinity)
= 0.75128556447474642837483635094465624422811643271281180112016972208864887861644568136653492101

et ou les H(i, k) sont les nombres harmoniques generalises definis par

H(i, k) = sum(1/j**i, j = 1 .. k).

Incidemment, la constante Pi^2*ln(2)/6 a comme valeur

1.1401814106428527574745798589923493452166298413646522525540219747528528731537947877843250176

Pourrais-tu passer ces nombres A LA MOULINETTE et m'en dire des nouvelles
au plus tot ...

Merci d'avance,

Gamma Lambada (Hula Hop, Twist, Rock n'Roll et tout le tralala ...)
--
Gilbert Labelle tel : (514) 987-6168
LACIM - Dept. math. et info. fax : (514) 987-8477
Universite du Quebec a Montreal gilbert@lacim.uqam.ca
C.P. 8888, Succ. "A"
Montreal (Quebec)
CANADA H3C 3P8

I tried those constants with Pari-GP.

3.141592653589793238462643383279502884197169399375105820974944592
9.869604401089358618834490999876151135313699407240790626413349374

31.00627668029982017547631506710139520222528856588510769414453809
.5772156649015328606065120900824024310421593359399235988057672349
.6931471805599453094172321214581765680755001343602552541206800095
1.098612288668109691395245236922525704647490557822749451734694334
1.414213562373095048801688724209698078569671875376948073176679738
1.732050807568877293527446341505872366942805253810380628055806979
6.841088463857116544847479153954096071299779048187913515324131847
1.202056903159594285399738161511449990764986292340498881792271555
2.678938534707747633655692940974677644128689377957301100950428327
1.354117939426400416945288028154513785519327266056793698394022468
.2430703516700615775627047239675822171681579630063323040814083
lindep([%1,%2,%3,%4,%5,%6,%7,%8,%9,%10,%11,%12,%13]

$$13/8 \ \mathrm{Zeta}(3) - 1/12 \ \mathrm{Pi}^2 \ \ln(2)$$

¿ evalf(”);

1.383251762312914335037284582959931562384787804370984556635430290

Allo Gilbert et Louise ,bonne nouvelle, j'ai trouve (ou plutotPari-Gp-LLL) a trouve l'expression pour les 3 constantes a,b,c !!!

a = Zeta(3)-Pi**2log(2)/12
b=Zeta(3)*5/8

et donc c = 13/8 * Zeta(3) + Pi**2*log(2)/4

These results where later explained.