Exploring Primes with DERIVE

Johann Wiesenbauer,
Technical Univ. of Vienna,
j.wiesenbauer@tuwien.ac.at

Since time immemorial problems concerning primes and their distribution have captivated both professionals and amateurs. This leads to the question whether this obvious fascination emerging from primes could also be used in classroom teaching. The main goal of my talk is to show that the answer is a definite "yes" and DERIVE can be of great help on that score. (All computations in the following were carried out on a Pentium 166 PC with 32 MB using DfW 4.09.)

Mersenne Primes or Mathematics for the Guinness Book of Records

Every now and then one can read in the newspaper that a new record prime had been found , e.g. when the current "record holder" $2^{3021377}-1$ was discovered by the 19 year-old student Roland Clarkson on January 27th, 1998. Clark, who was one of over 4000 volunteers world-wide participating in the Great Internet Mersenne Prime Search (GIMPS) founded by George Woltman, used a simple 200 MHz Pentium computer part-time for 46 days to prove this 909526-digit number prime.

The obvious question arises, why anyone cares about finding a prime that big. Well, the people of the GIMPS-project may do it for the glory or to learn more about the distribution of Mersenne primes, it is true, but there are also less obvious answers. In particular, those short and sweet programs provide an ideal hardware-test for the computer as they are intensely CPU and bus intensive and the output can be easily checked. For example, the program of George Woltron is now used by Intel to test every Pentium chip before it is shipped. As a further by-product of the quest, Richard Crandall has developed an improved version of the wellknown algorithm by Schoenhage and Strassen using Fast Fourier Transforms for multiplying large integers.

Another question any teacher should be prepared to answer deals with the fact that virtually all the past prime records are of the form 2^p-1, where p is a prime. (The latter condition for p is clearly necessary, since a nontrivial divisor k of p leads to the nontrivial divisor 2^k-1 of 2^p-1.) Numbers of this form are called Mersenne numbers after the French monk Marin Mersenne who stated in 1644 that the numbers $M_p := 2^p-1$ were prime for $p \le 257$ if and only if p belongs to the set {2,3,5,7,13,17, 19,31,67,127,257}. For Mersenne numbers - and this is the answer to the question above - an incredibly simple primality criterion holds:

Lucas-Lehmer Test (1930): Let the sequence $s_1, s_2, \ldots$ of integers be recursively defined by

$$s_1 = 4,\ s_{k+1} = s_k^2 - 2 \quad (k \ge 1)$$

Then for any odd prime p the Mersenne number 2^p-1 is prime if and only if it is a divisor of s_{p-1}.

To prevent the numbers s_k from getting unnecessarily large it is a good idea to compute them mod M_p only and to check finally whether $s_{p-1} \equiv 0 \bmod M_p$. A simple

DERIVE-implementation to test m, where m is a Mersenne number M_p for some odd prime, could look like this:

```
LUCAS_LEHMER(m) := IF(ITERATE(MOD(s_^2 - 2, m), s_, 4,
    LOG(m + 1, 2) - 2) = 0, true, false)
```

As an example we use it to check Mersenne's list:

```
SELECT(LUCAS_LEHMER(2^p_ - 1), p_, SELECT(PRIME(n_), n_, 3, 257))
[3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127]
```

As the computation shows (in 1.2s !) Mersenne was mistaken five times: The exponents 67 and 257 do not yield Mersenne primes as opposed to the missing exponents 61,89 and 107. By the way, the current list of all p's, where M_p is known to be prime, consists of the following 37 numbers:

2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377

When it comes to testing these exponents with DERIVE, numbers below 10000 are a matter of some minutes at most and numbers below 100000 are also within reach if you can do some time without your computer, but I wouldn't touch numbers above that. For exponents > 4000 it may also pay off to use the following modification of the built-in mod-function (for Mersenne numbers only!) that makes use of the simple congruence $A2^p + B = A(2^p - 1) + (A + B) \equiv A + B \bmod M_p$:

```
MODM(n, m) := MOD((n AND m) + FLOOR(n, m + 1), m)

LUCAS_LEHMER(m) := IF(ITERATE(MODM(s_^2 - 2, m), s_, 4,
    LOG(m + 1, 2) - 2) = 0, true, false)
```

The computation

```
LUCAS_LEHMER(2^9941 - 1) = true
```

takes 280.7s now vs. 305.5s with the old routine. (For bigger exponents the saving of time may be hours!)

If a given Mersenne numbers M_p is proved composite by the Lucas-Lehmer test, we are still left with the question how a nontrivial factorization for M_p looks like. You probably know the story of F.N.Cole who spend "three years of Sundays" on the following factorization of M_{67} (cf. [1])

```
FACTOR(2^67 - 1) = 193707721·761838257287
```

which takes DERIVE only 0.4s! But when trying to factor Mersenne numbers like e.g. M_{257} DERIVE would have a very hard time, too!

Here are some hints which could make this task easier. First of all, it is known that factors of a Mersenne number M_p are all of the special form 2kp+1 where either $k \equiv 0 \bmod 4$ or $k \equiv -p \bmod 4$ holds. Therefore, it may be a good idea to start with trial division dividing M_p through all primes of the above form until a certain boundary is

reached. If this fails, one must resort to one of the standard methods for factoring large numbers. As an example, I have implemented a variant of Pollard's (p-1)-method that works very well if the number N in question has a prime factor q such that q-1 splits up into many relatively small primefactors. By choosing e in a suitable way, e.g. as the product of all prime powers up to a certain boundary, the chances are that e is divisible by q - 1, which implies for any integer a coprime to N that

$$a^e = (a^{q-1})^{e/(q-1)} \equiv 1 \bmod q$$

and therefore $q \mid (a^e - 1, N)$.

In the following program we use numbers coprime to 210, i.e. not divisible by 2,3,5,7, instead of primes, because computing powers mod N is so fast that it doesn't pay off to discard composites. Moreover, they are even useful in providing powers of the small primes. For a and s the default values 3 and ∞, respectively, are taken unless you specify them otherwise.

PMINUS1(n, a, s) := GCD((ITERATE(IF(GCD(a_ - 1, n) > 1 OR IF(s < b_SUB2, true, false, false), [a_, b_], [MOD(a_^PRODUCT(b_), n), b_ + [0, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210, 210]]), [a_, b_], [MOD(IF(a, 3, a, 3)^160030080000, n), [210, 1, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 121, 127, 131, 137, 139, 143, 149, 151, 157, 163, 167, 169, 173, 179, 181, 187, 191, 193, 197, 199, 209]]))SUB1 - 1, n)

And here are some examples where you can see this routine at work.

$$\text{PMINUS1}(2^{67} - 1) = 193707721$$

$$\text{FACTOR}(193707721 - 1) = 2^3 \cdot 3^3 \cdot 5 \cdot 67 \cdot 2677$$

$$\text{PMINUS1}(2^{101} - 1) = 7432339208719$$

$$\text{FACTOR}(7432339208719 - 1) = 2 \cdot 3 \cdot 101 \cdot 44029 \cdot 278557$$

$$\text{PMINUS1}(2^{257} - 1) = 1155685395246619182673033$$

$$\text{FACTOR}(1155685395246619182673033 - 1)$$

$$2^3 \cdot 3^2 \cdot 19^2 \cdot 47 \cdot 67 \cdot 257 \cdot 439 \cdot 119173 \cdot 1050151$$

These result were obtained in 0.3 s, 51.8 s and 469.6s, respectively. In particular, in the second case this is more than ten times faster than the built-in factor routine, whereas in the third case I cannot draw a comparison for understandable reasons. You can also see that in all cases the preconditions for the factorization of q - 1 for the found prime q are fulfilled which accounts for the amazing performance.

A lot of open problems are connected with Mersenne primes. Let me conclude this chapter with a small sample of them(cf. [2]):

- Are there infinitely many Mersenne primes?
- Are there infinitely many Mersenne composites?
- Is every Mersenne number squarefree, i.e. a product of distinct primes?

- Is every perfect number, that is a number which is two times the sum of its positive divisors, of the form $2^{p-1}M_p$ for some Mersenne prime M_p or - to put it in another way as all even perfect numbers are of this form - do odd perfect numbers exist?

Fermat Primes or the Construction of Regular Polygons with Compass and Straight-edge

In a way the Fermat primes are the counterparts to Mersenne primes being of the form 2^k+1. Since any odd divisor i > 1 of k yields the nontrivial divisor $2^{k/i}+1$ of 2^k+1 we see at once that k must be a power of 2. Numbers of the form

$$F_m := 2^{2^m}+1 \quad (m \geq 0)$$

are called Fermat numbers after Fermat who conjectured in one of his letters that all these numbers must be prime, having noticed that this is true for m = 0,1,2,3,4. Strangely enough, no other Fermat primes have been found so far and thus it could well be that these are actually the only ones.

The counterpart to the Lucas-Lehmer test is

Pépin's Test (1877): The Fermat number F_m with m > 0 is prime if and only if

$$3^{(F_m-1)/2} \equiv -1 \bmod F_m .$$

Similar to the Lucas-Lehmer test this is an extremely simple and fast test and an implementation in DERIVE could look like this:

```
PEPIN(f) := IF(MODS(3^((f - 1)/2), f) = -1, true, false)

VECTOR(PEPIN(2^(2^m_) + 1), m_, 1, 10)

[true, true, true, true, false, false, false, false, false, false]
```

Although the computation time for the above example is surprisingly low (0.4s !) this is rather deceptive because the growth of Fermat numbers is enormous and somewhere in the region of m=16 or 17 are the limits of DERIVE. Using supercomputers the first undecided case is not very much higher, namely m=24, which again gives an impression of the rapid growth of these numbers.

Even so, there is still some hope that one can prove a given Fermat number composite by finding a small nontrivial factor. Here we can make use of a theorem by Euler who stated that every factor of a Fermat number F_m is of the form $k2^m+1$ for some natural number k. (Actually, Euler was the first who proved Fermat wrong by showing that 641 is a divisor of F_5.)

The following two DERIVE-routines can be used to compute a divisor t of F_m and the corresponding k in the representation $t = k2^{m+2}+1$ such that $t \leq s$ or $k \leq s$, respectively.

```
FFACTOR(m, s) := ITERATE(IF(MOD(2^2^m, t_) = t_ - 1, t_, IF(t_ > s, 1,
    t_ + 2^(m + 2), t_ + 2^(m + 2))), t_, 2^(m + 2) + 1)

FFACTOR_K(m, s) := (FFACTOR(m, s·2^(m + 2) + 1) - 1)/2^(m + 2)
```

And here are some examples:

```
FFACTOR_K(1945) = 5
SELECT(v_2 > 0, v_, VECTOR([m_, FFACTOR_K(m_, 100)], m_, 5, 100))`
```

$$\begin{bmatrix} 5 & 11 & 12 & 18 & 23 & 36 & 38 & 39 & 55 & 63 & 73 \\ 5 & 39 & 7 & 13 & 5 & 10 & 6 & 21 & 29 & 36 & 5 \end{bmatrix}$$

The first one deals with the huge Fermat number F_{1945} which according to Coxeter has more digits than the estimated number of particles in our universe and therefore can never be seen in full length. Nevertheless, DERIVE finds after only 11.7 s (!) the 587-digit divisor $5 \cdot 2^{1947} + 1$ of it. In the second example a list of all Fermat numbers F_m with $m \le 100$ that have a nontrivial divisor $k2^{m+2} + 1$ with $k \le 100$ is computed (in 21.2 s!)

As in the case of Mersenne numbers Pollard's (p-1)-method may also be of great help. The following example deals with the case m=10 that would have been a really "tough" one when using the above method and takes only 0.2 s now!

$$\text{PMINUS1}\left(2^{2^{10}} + 1, 9\right) = 6487031809$$

$$\frac{\text{PMINUS1}\left(2^{2^{10}} + 1, 9\right) - 1}{2^{12}} = 1583748$$

$$\text{FACTOR}(1583748) = 2^2 \cdot 3^2 \cdot 29 \cdot 37 \cdot 41$$

What are Fermat numbers actually good for? Well, since their binary representation apart from the first and the last bit consists of 0's only and as they do not have small prime divisors either, they are very well suited for certain purposes in cryptography e.g. when it comes to choosing a public key e for the RSA-cryptosystem. Furthermore, Fermat numbers are used in the algorithm of Schoenhage and Strassen mentioned above. Last but not least, Fermat primes play an important role when it comes to deciding whether for a given natural number $n \ge 3$ the regular n-gon can be constructed with compass and staight-edge only. According to a theorem of Gauss this is the case if and only if n is a power of 2 times a product of distinct Fermat primes. In the following I would like to use DERIVE to deal with the case n = 17, which gave the then 19-year old Gauss so much pleasure that he made up his mind to focus on mathe-mathics rather than old languages.

What Gauss actually showed was that the equation

$$(z^{17} - 1) / (z - 1) = z^{16} + z^{15} + \ldots + z + 1 = 0 \qquad (*)$$

can be solved and - what is equally important - that its solutions can be obtained from a finite set of rational numbers by applying the operations +,–, · , / and $\sqrt{\ }$ a finite number of times (let's call such complex numbers radical expressions for short). For example, $\varsigma := e^{2i\pi/17}$ is clearly a solution but this representation is not of the desired

form. Gauss had the idea to consider for all positive divisors e of 16 the following expressions

$$\eta_i^{(e)} := \zeta_i + \zeta_{i+e} + \zeta_{i+2e} + \ldots + \zeta_{i+(f-1)i} \quad , i = 0,1,\ldots,e-1$$

where $\zeta_k := \zeta^{3^k}$, k = 0,1, ..., 15, and f:=16/e. Just to see what we are talking about let us view these expressions on a DERIVE-screen. (Note that we had to change to the letter z here, because the letter ζ refers to Riemann's ζ-function in DERIVE that will be discussed later on.)

```
η(e,i):=Σ(z^MOD(3^j_,17),j_,[i,i+e,...,15])
VECTOR([e, VECTOR(η(e, i), i, 0, e - 1)], e, [1, 2, 4, 8, 16])
DisplayFormat:=Compressed
```

$$\begin{bmatrix} 1 & [z^{16}+z^{15}+z^{14}+z^{13}+z^{12}+z^{11}+z^{10}+z^{9}+z^{8}+z^{7}+z^{6}+z^{5}+z^{4}+z^{3}+z^{2}] \\ 2 & [z^{16}+z^{15}+z^{13}+z^{9}+z^{8}+z^{4}+z^{2}+z^{14}+z^{12}+z^{11}+z^{10}+z^{7}+z^{6}+z^{5}+z^{3}] \\ 4 & [z^{16}+z^{13}+z^{4}+z^{14}+z^{12}+z^{5}+z^{3}+z^{15}+z^{9}+z^{8}+z^{2}+z^{11}+z^{10}+z^{7}+z^{6}] \\ 8 & [z^{16}+z^{14}+z^{3}+z^{9}+z^{8}+z^{10}+z^{7}+z^{13}+z^{4}+z^{12}+z^{5}+z^{15}+z^{2}+z^{11}+z^{6}] \\ 16 & [z^{3}+z^{9}+z^{10}+z^{13}+z^{5}+z^{15}+z^{11}+z^{16}+z^{14}+z^{8}+z^{7}+z^{4}+z^{12}+z^{2}+z^{6}] \end{bmatrix}$$

In particular, we can see in the last row of this matrix that $\zeta_o, \zeta_1, \ldots, \zeta_{15}$ is just a rearrangement of the elements $\zeta, \zeta^2, \ldots, \zeta^{15}$. As we will see, it is exactly this rearrangement that plays a decisive role in Gauss' proof that all expressions in the matrix above (in particular the roots of our equation in the last row!) are radical expressions. This is clearly true for $\zeta_0^{(1)} = -1$. For $\zeta_0^{(2)}$ and $\zeta_1^{(2)}$ we have the following equations

$$\zeta_0^{(2)} + \zeta_1^{(2)} = -1, \quad \zeta_0^{(2)}\,\zeta_1^{(2)} = -4$$

Only the second one needs a proof which can be given by means of the following DERIVE-routine that reduces any polynomial expression in ζ modulo any given polynomial equation in ζ (in our case, of course, this will be always equation (*)):

```
RED(u, v) := ITERATE(RHS(v)·QUOTIENT(u_, LHS(v)) + REMAINDER(
   u_, LHS(v)), u_, u)
```

And here is the proof of the second equation given by DERIVE!

```
RED(η(2, 0)·η(2, 1), (z^17 - 1)/(z - 1) = 0) = -4
```

But this means that $\zeta_0^{(2)}$ and $\zeta_1^{(2)}$ are both the roots of the quadratic equation

$$w^2 + w - 4 = 0$$

with rational coefficients which implies that they too are radical expressions! After solving this equation with DERIVE, we have a small problem: Which of the two solutions is $\zeta_0^{(2)}$ and which one is $\zeta_1^{(2)}$? Again, DERIVE is of great help:

$$\text{RED}\left(\eta(2,\,0)\cdot\eta(2,\,1),\ \frac{z^{17}-1}{z-1}=0\right)=-4$$

$$\text{SOLVE}(w^2+w-4=0,\,w)=\left[w=\frac{\sqrt{17}}{2}-\frac{1}{2},\ w=-\frac{\sqrt{17}}{2}-\frac{1}{2}\right]$$

$$\text{APPROX}(\text{SOLVE}(w^2+w-4=0,\,w))=[w=1.56155,\ w=-2.56155]$$

$$\text{APPROX}(\text{RE}(\lim_{z\to\text{EXP}(2\cdot\hat{\imath}\cdot\pi/17)}[\eta(2,\,0),\,\eta(2,\,1)]))=[1.56155,\,-2.56155]$$

$$\left[\eta 20:=\frac{\sqrt{17}}{2}-\frac{1}{2},\ \eta 21:=-\frac{\sqrt{17}}{2}-\frac{1}{2}\right]$$

In a similar way we compute $\eta_0^{(4)}$ and $\eta_2^{(4)}$:

$$\text{RED}\left(\eta(4,\,0)\cdot\eta(4,\,2),\ \frac{z^{17}-1}{z-1}=0\right)=-1$$

$$\text{SOLVE}(w^2-\eta 20\cdot w-1=0,\,w)$$

$$\left[w=\sqrt{\frac{17}{8}-\frac{\sqrt{17}}{8}}+\frac{\sqrt{17}}{4}-\frac{1}{4},\ w=-\sqrt{\frac{17}{8}-\frac{\sqrt{17}}{8}}+\frac{\sqrt{17}}{4}-\frac{1}{4}\right]$$

$$[w=2.04948,\ w=-0.487928]$$

$$\text{APPROX}(\text{RE}(\lim_{z\to\text{EXP}(2\cdot\hat{\imath}\cdot\pi/17)}[\eta(4,\,0),\,\eta(4,\,2)]))=[2.04948,\,-0.487928]$$

$$\eta 40:=\sqrt{\frac{17}{8}-\frac{\sqrt{17}}{8}}+\frac{\sqrt{17}}{4}-\frac{1}{4}$$

$$\eta 42:=-\sqrt{\frac{17}{8}-\frac{\sqrt{17}}{8}}+\frac{\sqrt{17}}{4}-\frac{1}{4}$$

The results for $\eta_1^{(4)}$ and $\eta_3^{(4)}$ only differ from these by the sign of $\sqrt{17}$:

$$\eta 41:=\sqrt{\frac{\sqrt{17}}{8}+\frac{17}{8}}-\frac{\sqrt{17}}{4}-\frac{1}{4}$$

$$\eta 43:=-\sqrt{\frac{\sqrt{17}}{8}+\frac{17}{8}}-\frac{\sqrt{17}}{4}-\frac{1}{4}$$

Now we are ready to put the finishing touches:

$$\text{RED}\left(\eta(8,\,0)\cdot\eta(8,\,4),\ \frac{z^{17}-1}{z-1}=0\right)=z^{14}+z^{12}+z^5+z^3$$

$$\eta(4,\,1)=z^{14}+z^{12}+z^5+z^3$$

$$\text{RHS}\left((\text{SOLVE}(w^2-\eta 40\cdot w+\eta 41=0,\,w))_1\right)$$

$$\sqrt{\left(-\sqrt{\left(\frac{19\cdot\sqrt{17}}{128}+\frac{85}{128}\right)}+\frac{3\cdot\sqrt{17}}{16}+\frac{17}{16}\right)}+\sqrt{\left(\frac{17}{32}-\frac{\sqrt{17}}{32}\right)}+\frac{\sqrt{17}}{8}-\frac{1}{8}$$

$$\text{APPROX}\left(\text{RHS}\left(\left(\text{SOLVE}(w^2 - \eta 40 \cdot w + \eta 41 = 0,\ w)\right)_1\right)\right) = 1.86494$$

$$\text{APPROX}\left(\text{RE}\left(\lim_{z \to \text{EXP}(2 \cdot \hat{\imath} \cdot \pi/17)} \eta(8,\ 0)\right)\right) = 1.86494$$

$$\eta 80 := \sqrt{\left(-\sqrt{\left(\frac{19 \cdot \sqrt{17}}{128} + \frac{85}{128}\right)} + \frac{3 \cdot \sqrt{17}}{16} + \frac{17}{16}\right)} + \sqrt{\left(\frac{17}{32} - \frac{\sqrt{17}}{32}\right)} + \frac{\sqrt{17}}{8} - \frac{1}{8}$$

$$\eta(8,\ 0) = z^{16} + z$$

$$\text{APPROX}\left(2 \cdot \text{COS}\left(\frac{2 \cdot \pi}{17}\right)\right) = 1.86494$$

Since $\cos(2\pi/17) = \eta_0^{(8)}/2$ is a radical expression, the same must be true for $\sin(2\pi/17)$ and hence for $\zeta = \cos(2\pi/17) + i\sin(2\pi/17)$. This concludes the proof that a regular 17-gon can be constructed using only compass and straight-edge. It goes without saying that the same reasoning applies to the regular 257-gon and 65537-gon, though the latter case isn't exactly a pushover even for DERIVE!

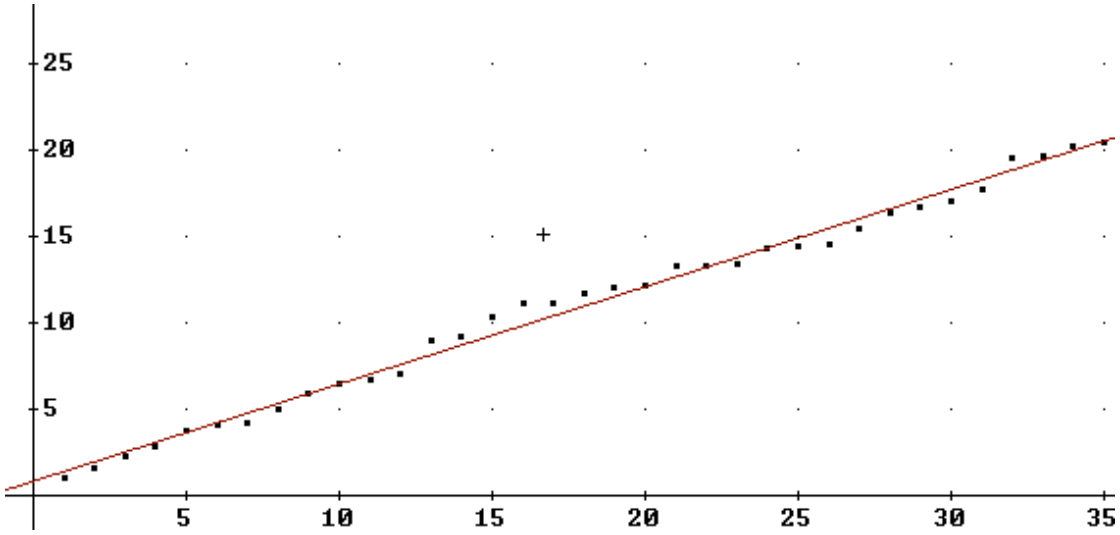
On the Distribution of Primes or the Glory and Misery of Experimental Math

There are two facts concerning the distribution of primes which are most striking and seem to contradict each other. On the one hand, their occurence in short intervals is extremely irregular and unpredictable, on the other hand, when viewed at large, amazing regularities become visible. As an introductory example, let's have a look at the graph of the function $_2\log(p^{(n)})$, where $p^{(n)}$ denotes the n-th prime leading to a Mersenne prime ordered by size. (As of today, this function is known without any gaps for n = 1,2,...,35 only.)

Assuming that NUMBER.MTH had been loaded before, you can do this by approximating the vector

```
m := VECTOR([n_, LOG(MERSENNE_DEGREE(n_), 2)], n_, 1, 35)
```

and plotting the result.



Since the independence is strikingly close to linearity, from a statistical point of view the obvious next step is to draw the regression line.

```
APPROX(FIT(APPEND([ x  a·x + b ], m))) = 0.563132·x + 0.832723
APPROX(EXP(-euler_gamma)) = 0.561459
```

By heuristic reasoning the slope of this line should be $e^{-\gamma}$, where γ is Euler's constant defined by

$$\gamma := \lim\left(\sum_{k=1}^{n} 1/k - \log n\right)$$

We are facing here a typical dilemma that occurs quite often when dealing with the distribution of primes: On the one hand, we can't even prove that there are infinitely many Mersenne primes, but when accepting some plausible assumptions we can do even more, namely set up a formula that reflects their growth to infinity.

When speaking of the distribution of primes there are several functions that come into play in a natural way. One of them is $\pi(x)$ which counts for a positive real number x the number of primes below x. According to the Prime Number Theorem, which was conjectured by Legendre and Gauss and proven by Hadamard and de la Vallée-Poussin in 1896, $\pi(x)$ is asymptotically equal to x/ln x and also to the so-called logarithmic integral

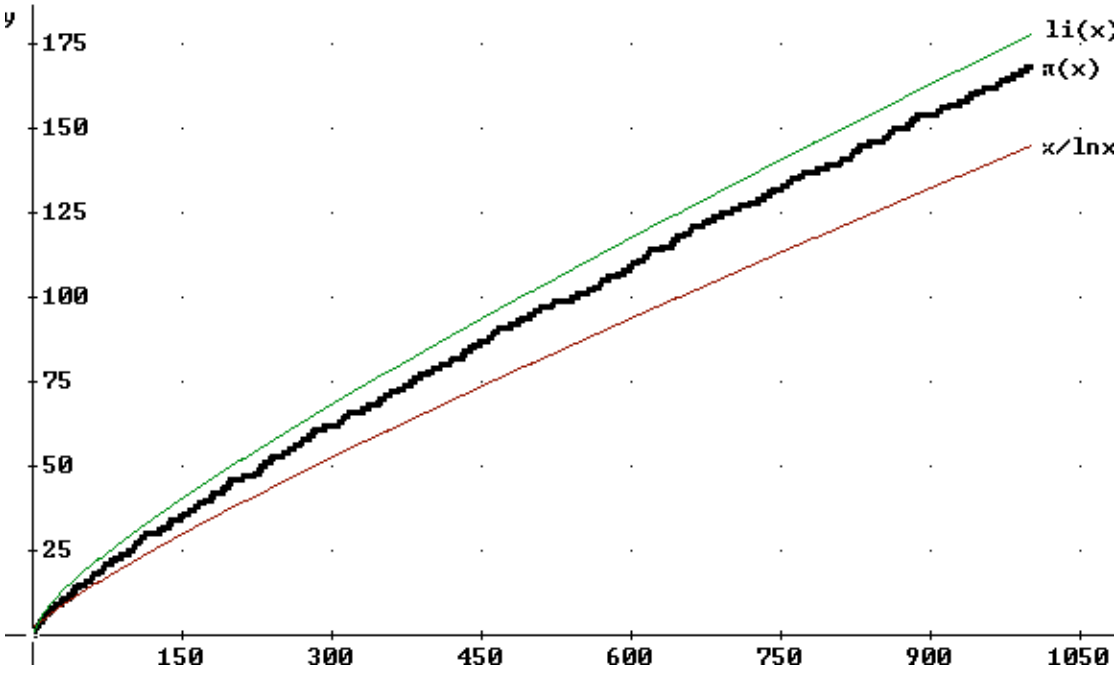
$$\mathrm{li}(x) := \int_0^x dt / \ln t$$

that is, the relative error when replacing $\pi(x)$ by one of these functions goes to 0 as x goes to infinity. In particular, we may conclude from this that the "density of primes" in a small interval around x should be close to 1/ln x.

Unfortunately, at present $\pi(x)$ is not available as a DERIVE-function, but for small values of x, say x < 100 000, the following implementation should suffice:

PRIMEPI(x) := LIM(SUM(PRIME(k_), k_, 1, x), [true, false], [1, 0])

It was used to produce the following graphs (note that li(x) should be implemented as 1.045+ INT(1/lnt,t,2,x) to avoid the singularity at x=1):



Judging from these graphs only one might be tempted to say that x/ln x is always below $\pi(x)$ (apart from the small region $x \le 17$) and li(x) is always above it. This also remains true when looking at larger tables for $\pi(x)$ that reach up to 10^{20} at present. But only the first conjecture is true, whereas the second one is completely wrong. What is more, Littlewood has proved that the difference $li(x) - \pi(x)$ changes its sign infinitely often! This is clearly a warning that one shouldn't jump to conclusions that are only based on numerical evidence!

Another very important function related to the distribution of primes is Riemann's ζ-function. It is for complex numbers s with Re(s)>1 defined by

$$\zeta(s) = \prod_p 1/(1-p^{-s})$$

where p runs through all primes, and by the fundamental theorem of elementary number theory this can also be written as

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

By a standard method called "analytic continuation" ζ(s) can be defined on the entire complex plane, and then it is analytic everywhere except for a pole of order 1 at s =1. It is easy to see that ζ(s) has trivial zeros at -2,-4,-6,... and that all nontrivial zeros are symmetric about the line Re(s)=1/2. According to the notorious Riemann hypothesis (RH), which is probably the most important unsolved mathematical problem, all nontrivial zeros are exactly on this line. In 1986 it was shown by Brent, van de Lune, te Riele and Winter that the first 1 500 000 001 nontrivial zeros do indeed have real part ½, but we already know that numerical evidence can be misleading.

There are a lot of equivalent formulations of RH and some of them are quite interesting. First of all, Koch showed in 1901 that RH is equivalent to

$$\pi(x) = li(x) + O(\sqrt{x}\ln x).$$

(The meaning of f(x)=O(g(x)) is that f(x)/g(x) is bounded.) Roughly spoken, this would imply that when approximating $\pi(x)$ by li(x) about the first half of the digits remain correct. By using more sophisticated implementations of PRIMEPI(x) (cf. [3]) this could be checked with DERIVE for any $x < 10^9$ in less than one hour.

Another equivalent formulation of RH is closely related to certain properties of Moebius μ-function. Its definition can be easily deduced from the following DERIVE-implementation:

```
MOEBIUS_MU(n) := PRODUCT(IF(PRIME(k_), -1, 0), k_, FACTORS(
   FACTOR(n)))
```

If the function M(n) is defined by $M(n) := \sum_{k=1}^{n} \mu(k)$ for every natural number n, then

$$M(n) = O(n^r) \text{ for all } r > 1/2$$

is equivalent to RH. Again, DERIVE could be used to check the growth of M(n) for small values of n. In particular, one could try to replace μ in the definition of M by

```
RANDOM_MU(n) := IF(RANDOM(1) < 6/PI^2, (-1)^RANDOM(2), 0)
```

and would notice that there is seemingly not much difference as regards the growth of M(n). If this were really true, this would imply the condition for M above and thus RH! Since the assumed random behaviour of μ reflects only the fact that are no striking

irregularities in the distribution of primes, RH means from a philosophical point of view that primes behave as regularly as possible!

There are are lot of other interesting things that could be said about RH (cf. also [4] as regards its relation to Farey fractions!) and the distribution of primes, but I hope I have already reached my goal to show that exploring prime numbers with such a powerful tool like DERIVE at hand can be very rewarding indeed.

References

[1] Bell E.T., Mathematics: Queen & Servant of Science, Tempus Books, 1987

[2] Ribenboim P., The New Book of Prime Number Records, Springer-Verlag, 1995

[3] Wiesenbauer J., Abzählen von Primzahlen mit DERIVE, ÖMG-Didaktikreihe, Heft 27, 1997 (196-206)

[4] Wiesenbauer J., Titbits from Algebra and Number Theory, Derive-Newsletter #27, Sept. 1997 (34-38)