Computations in p-adic Fields

Let p be a prime. Recall that the ring $\mathbb{Z}_p$ of *p-adic integers* consists of all expressions of the form

$$a_0 + a_1p + a_2p^2 + a_3p^3 + \cdots$$

where each $a_i \in \{0, 1, 2, \ldots, p{-}1\}$. Finite (i.e. terminating) sums of the form above give all the non-negative integers (written in 'reverse' base p notation); and allowing infinite sums, we obtain a much larger ring of numbers which includes all those rational numbers which, in reduced form, have no p in the denominator. It is important to recognize that the digits a_i are just integers, *not* integers mod p. Also, the p-adic expansion (in which a number is expressed in terms of *ascending* powers of p) is very different from the usual base p representation (in terms of *descending* powers of p). For example we have

$$\tfrac{8}{3} = 2.666666\ldots = 2 + \tfrac{6}{10} + \tfrac{6}{10^2} + \tfrac{6}{10^3} + \tfrac{6}{10^4} + \cdots \quad \text{(decimal expansion);}$$
$$\tfrac{8}{3} = \underbrace{2.313131\ldots}_{\text{base 5}} = 2 + \tfrac{3}{5} + \tfrac{1}{5^2} + \tfrac{3}{5^3} + \tfrac{1}{5^4} + \cdots \quad \text{(base 5 expansion);}$$
$$\tfrac{8}{3} = 1 + 2{\cdot}5 + 3{\cdot}5^2 + 5^3 + 3{\cdot}5^4 + \cdots \quad \text{(5-adic expansion).}$$

We will show, using the latter expansion as an example, how to obtain p-adic expansions of certain numbers, including rational numbers.

Allowing finitely many terms with negative exponent gives the field $\mathbb{Q}_p$ of *p-adic numbers*; these are all expressions of the form

$$a_kp^k + a_{k+1}p^{k+1} + a_{k+2}p^{k+2} + a_{k+3}p^{k+3} + \cdots$$

where $k \in \mathbb{Z}$ and $a_i \in \{0, 1, 2, \ldots, p{-}1\}$. In fact, $\mathbb{Q}_p$ is the field of quotients of $\mathbb{Z}_p$. It is an extension of the ordinary rationals: $\mathbb{Q} \subset \mathbb{Q}_p$.

Let us arbitrarily consider $p = 5$ and give some computational examples in $\mathbb{Q}_5$. For simplicity I'll begin with some 5-adic integers (so there will be no 5's in the denominator). An example is $\frac{8}{3}$. We wish to determine its 5-adic expansion

$$\tfrac{8}{3} = a_0 + a_15 + a_25^2 + a_35^3 + \cdots.$$

We can always find the coefficients $a_i \in \{0, 1, 2, 3, 4\}$ by brute force if necessary:

(1) $\qquad 8 = 3(a_0 + a_1 5 + a_2 5^2 + a_3 5^3 + \cdots).$

Since each $a_i \in \mathbb{Z}$ we can reduce modulo 5 to obtain $a_0 \equiv 1 \mod 5$, and the only possible digit is $a_0 = 1$. Substituting this into (1) and simplifying gives

(2) $\qquad 1 = 3(a_1 + a_2 5 + a_3 5^2 + a_4 5^3 + \cdots).$

This forces $3a_1 \equiv 1 \mod 5$ and so the only possible digit is $a_1 = 2$. Substituting this into (2) and simplifying again leaves

(3) $\qquad -1 = 3(a_2 + a_3 5 + a_4 5^2 + a_5 5^3 + \cdots).$

The only digit satisfying $3a_2 \equiv -1 \mod 5$ is $a_2 = 3$. Substituting this into (3) and simplifying again yields

(4) $\qquad -2 = 3(a_3 + a_4 5 + a_5 5^2 + a_6 5^3 + \cdots).$

The only digit satisfying $3a_3 \equiv -2 \mod 5$ is $a_3 = 1$. Substituting this into (4) and simplifying gives

(5) $\qquad -1 = 3(a_4 + a_5 5 + a_6 5^2 + a_7 5^3 + \cdots).$

This is the same as (3) but with the subscripts shifted by 2, which means that our sequence of digits has started to repeat. The digits are therefore $1, 2, 3, 1, 3, 1, 3, 1, 3, 1, \ldots$ and so

$$\tfrac{8}{3} = 1 + 2{\cdot}5 + 3{\cdot}5^2 + 5^3 + 3{\cdot}5^4 + 5^5 + 3{\cdot}5^6 + 5^7 + \cdots.$$

We can verify this by collecting terms on the right hand side to obtain a geometric series:

$$\begin{aligned}\big(1{+}2{\cdot}5\big) &+ \big(3{\cdot}5^2{+}5^3\big) + \big(3{\cdot}5^4{+}5^5\big) + \big(3{\cdot}5^6{+}5^7\big) + \cdots \\ &= 11 + 200 + 200{\cdot}5^2 + 200{\cdot}5^4 + 200{\cdot}5^6 + \cdots \\ &= 11 + \tfrac{200}{1-25} \\ &= 11 - \tfrac{25}{3} \\ &= \tfrac{8}{3}\,.\end{aligned}$$

It is easy to obtain the 5-adic expansion for $-\frac{8}{3}$ from that of $\frac{8}{3}$:

$$-\tfrac{8}{3} = 4 + 2{\cdot}5 + 5^2 + 3{\cdot}5^3 + 5^4 + 3{\cdot}5^5 + 5^6 + 3{\cdot}5^7 + \cdots$$

as one can verify by adding the 5-adic expansions and watching all the terms cancel.

The partial sums of the 5-adic expansion of $\frac{8}{3}$ are

$$1,\ 11,\ 86,\ 211,\ 2086,\ 5211,\ 52086,\ 130211,\ \ldots.$$

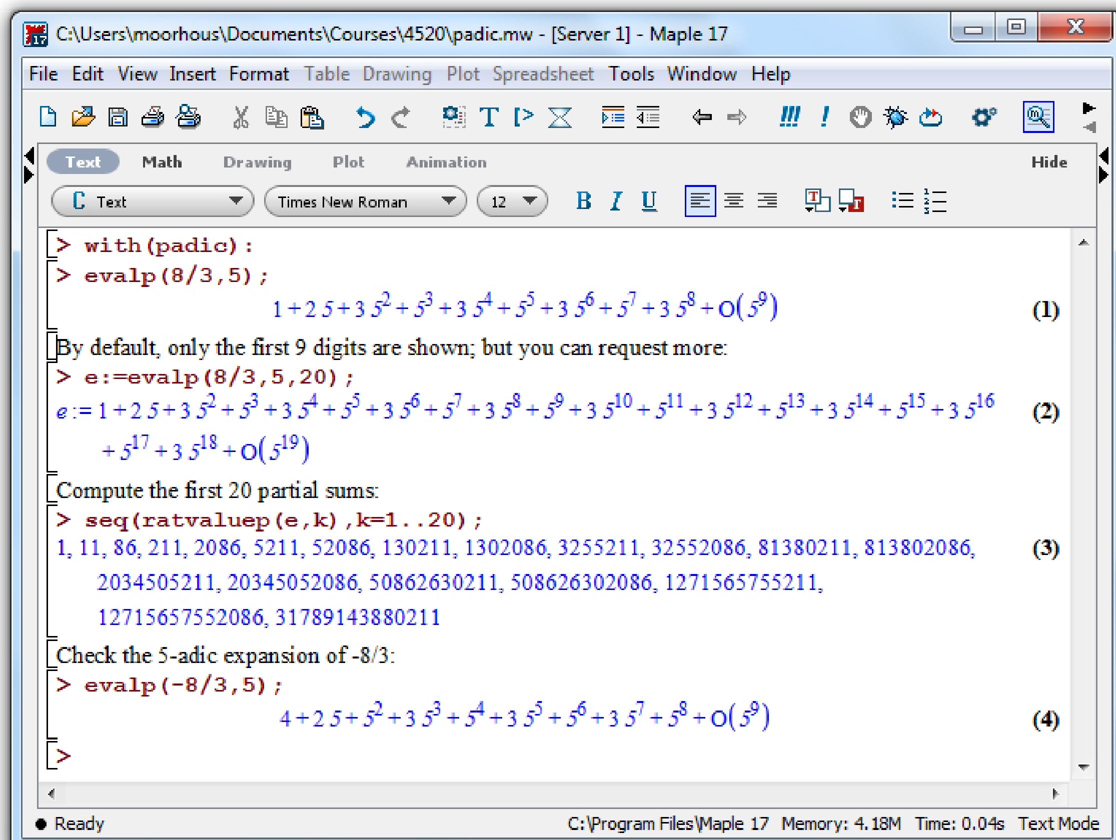
This sequence converges 5-adically to $\frac{8}{3}$, i.e. these partial sums get closer and closer to $\frac{8}{3}$ according to the 5-adic notion of distance, approaching $\frac{8}{3}$ in the limit. Indeed the k-th partial sum differs from $\frac{8}{3}$ by a multiple of 5^k which has size $5^{-k} \to 0$ as $k \to \infty$. To find the size of a nonzero rational number in $\mathbb{Q}_5$, first write it as $5^k \frac{a}{b}$ where $k, a, b \in \mathbb{Z}$, and a, b are not divisible by 5; then the 5-adic norm is given by

$$\left\|5^k \tfrac{a}{b}\right\|_5 = 5^{-k}.$$

So for example, the distance between the fourth partial sum and $\frac{8}{3}$ is

$$\left\|211 - \tfrac{8}{3}\right\|_5 = \left\|\tfrac{625}{3}\right\|_5 = \left\|\tfrac{5^4}{3}\right\|_5 = 5^{-4} = \tfrac{1}{625}\,.$$

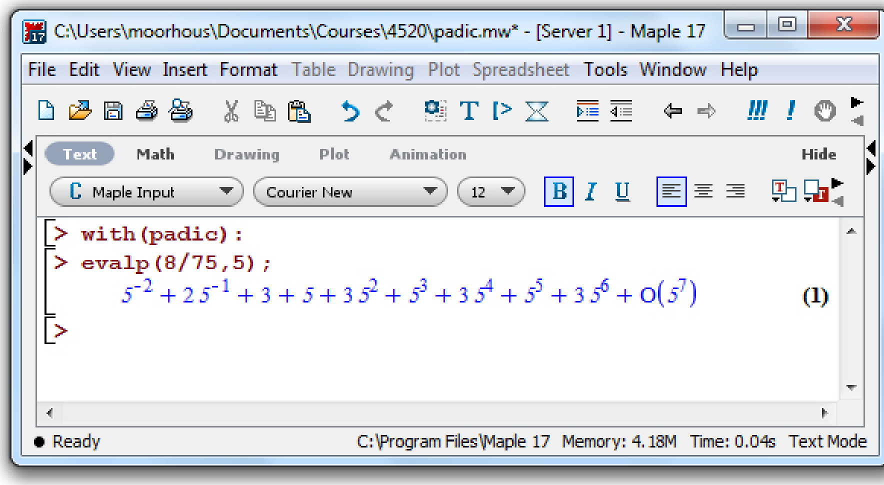
Let us check our computations using Maple. We first load the `padic` package. The command `evalp` gives the p-adic expansion, in the same way that `evalf` gives the decimal expansion.



As an example of a 5-adic number which is not a 5-adic integer, divide our previous example by 25 to obtain

$$\tfrac{8}{75} = 5^{-2} + 2{\cdot}5^{-1} + 3 + 5 + 3{\cdot}5^2 + 5^3 + 3{\cdot}5^4 + 5^5 + \cdots.$$

Check:



Most p-adic numbers have non-repeating expansions and so are irrational. As an example, let us compute the 7-adic expansion of $\pm\sqrt{2} \in \mathbb{Z}_7$:

$$\begin{aligned}
\pm\sqrt{2} &= b_0 + b_1 7 + b_2 7^2 + b_3 7^3 + b_4 7^4 + \cdots;\\
2 &= \big(b_0 + b_1 7 + b_2 7^2 + b_3 7^3 + b_4 7^4 + \cdots\big)^2\\
&= b_0^2 + (2b_0 b_1)7 + (2b_0 b_2 + b_1^2)7^2 + (2b_0 b_3 + 2b_1 b_2)7^3 + \cdots.
\end{aligned}$$

The only values of $b_0 \in \{0,1,2,3,4,5,6\}$ satisfying $b_0^2 \equiv 2 \mod 7$ are 3 and 4. Whichever of these two choices we make, we can then uniquely solve for the remaining coefficients b_i. We thus obtain two possible values for $\pm\sqrt{2}$ in $\mathbb{Z}_7$ as expected. It is meaningless to distinguish which one is $\sqrt{2}$ and which one is $-\sqrt{2}$ since the ring $\mathbb{Z}_7$ is not ordered; more correctly, we have simply the two roots of $x^2 = 2$ in $\mathbb{Z}_7$. For now, let us arbitrarily choose $b_0 = 3$:

$$\begin{aligned}
2 &= \big(3 + b_1 7 + b_2 7^2 + b_3 7^3 + b_4 7^4 + \cdots\big)^2\\
&= 9 + (6b_1)7 + (6b_2 + b_1^2)7^2 + (6b_3 + 2b_1 b_2)7^3 + \cdots;\\
-1 &= 6b_1 + (6b_2 + b_1^2)7 + (6b_3 + 2b_1 b_2)7^2 + (6b_4 + 2b_1 b_3 + b_2^2)7^3 + \cdots;
\end{aligned}$$

The only digit $b_1 \in \{0,1,2,\ldots,6\}$ satisfying this mod 7 is $b_1 = 1$ so

$$\begin{aligned}
-1 &= 6 + (6b_2 + 1)7 + (6b_3 + 2b_2)7^2 + (6b_4 + 2b_3 + b_2^2)7^3 + \cdots;\\
-2 &= (6b_2) + (6b_3 + 2b_2)7 + (6b_4 + 2b_3 + b_2^2)7^2 + \cdots.
\end{aligned}$$

This gives $b_2 = 2$. Continuing in this way, we can solve for one coefficient b_i at a time to obtain

$$\sqrt{2} = 3 + 7 + 2{\cdot}7^2 + 6{\cdot}7^3 + 7^4 + 2{\cdot}7^5 + 7^6 + 2{\cdot}7^7 + 4{\cdot}7^8 + \cdots.$$

The partial sums of this sequence are

$$3,\ 10,\ 108,\ 2166,\ 4567,\ 38181,\ 155830,\ 1802916,\ 24862120, \cdots$$

which gives successively better approximate solutions of $x^2 = 2$ in $\mathbb{Z}_7$: the k-th approximation solves the equation $x^2 = 2$ within $\frac{1}{7^k}$ in $\mathbb{Q}_7$. For example,the fourth approximation 2166 satisfies

$$\left\|2166^2 - 2\right\|_7 = \left\|4691554\right\|_7 = \left\|1954{\cdot}7^4\right\|_7 = 7^{-4} = \tfrac{1}{2401}\,.$$

This naive approach requires k iterations to obtain k digits of $\sqrt{2}$.

There is a much faster approach, for which k iterations will give 2^k digits of $\sqrt{2}$: Newton's method. Recall (e.g. from Calculus I) that this method starts with an approximate root x_0 of the equation $f(x) = 0$, as the starting point of a sequence of approximate solutions $x_0, x_1, x_2, x_3, \ldots$ where each successive approximation is found from the previous approximation by

$$x_{k+1} = x_k - \frac{f(x_k)}{f'(x_k)}\,.$$

This sequence may not converge, for a variety of reasons: maybe the equation $f(x) = 0$ has no solution, or maybe the first guess x_0 was chosen poorly. But when it works, it works *fast*, doubling the number of digits of accuracy at every iteration (much faster than the naive approach which only adds one more digit of accuracy at every iteration). This phenomenon of *quadratic convergence* works in $\mathbb{Q}_p$ for the same reason that it works in $\mathbb{R}$ (see any calculus textbook), although we omit the proof here.

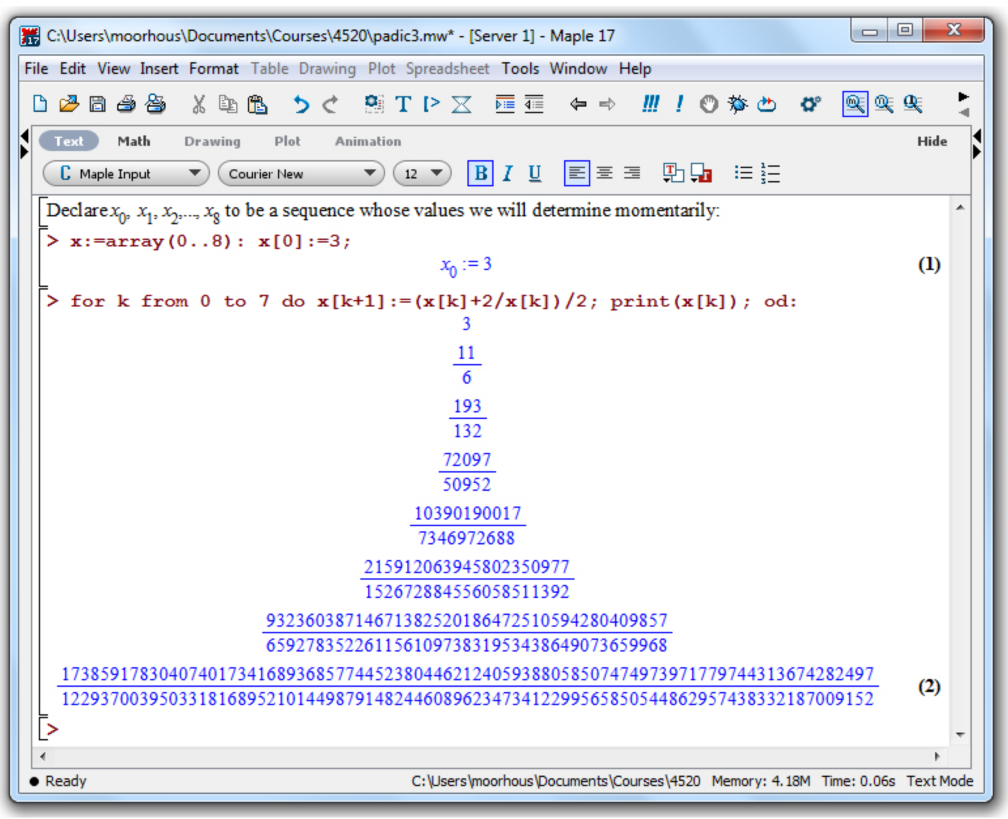
Let's illustrate Newton's Method for approximating $\sqrt{2}$ with initial guess $x_0 = 3$, the leading term of our 7-adic expansion. We are looking for a root of $f(x) = x^2 - 2$, where $f'(x) = 2x$ so successive guesses are given by

$$x_{k+1} = x_k - \frac{x_k^2 - 2}{2x_k} = \tfrac{1}{2}\big(x_k + \tfrac{2}{x_k}\big).$$

This gives

$$
\begin{aligned}
x_0 &= 3,\\
x_1 &= \frac{11}{6},\\
x_2 &= \frac{193}{132},\\
x_3 &= \frac{72097}{50952},\\
x_4 &= \frac{10390190017}{7346972688},\\
x_5 &= \frac{215912063945802350977}{152672884556058511392},\\
x_6 &= \frac{9323603871467138252018647251059428040985 7}{6592783522611561097383195343864907365996 8},\\
x_7 &= \frac{17385917830407401734168936857744523804462124059388058507474973971779744313674282497}{12293700395033181689521014498791482446089623473412299565850544862957438332187009152},
\end{aligned}
$$

etc. Here is a Maple session which completes these values:



This sequence converges to $\sqrt{2}$ in both $\mathbb{R}$ and $\mathbb{Q}_7$; and in both cases the convergence is quadratic. For example the decimal expansions of these approximations are given by

$$\begin{aligned}
x_0 &= 3.00000000000000000000000000000000000000000000000000000000000000000000\ldots\\
x_1 &= 1.83333333333333333333333333333333333333333333333333333333333333333333\ldots\\
x_2 &= 1.46212121212121212121212121212121212121212121212121212121212121212121\ldots\\
x_3 &= 1.41499842989480295179777045062019155283403988067200502433663055424713\ldots\\
x_4 &= 1.41421378004719758392002341413903456721275346600281250426229977023701\ldots\\
x_5 &= 1.41421356237311180087113641686894154181626390642479100754009420259950\ldots\\
x_6 &= 1.41421356237309504880168872430891641385044991878415404215410685807296\ldots\\
x_7 &= 1.41421356237309504880168872420969807856967187537694807318016021587533\ldots\\
x_8 &= 1.41421356237309504880168872420969807856967187537694807317667973799073\ldots
\end{aligned}$$

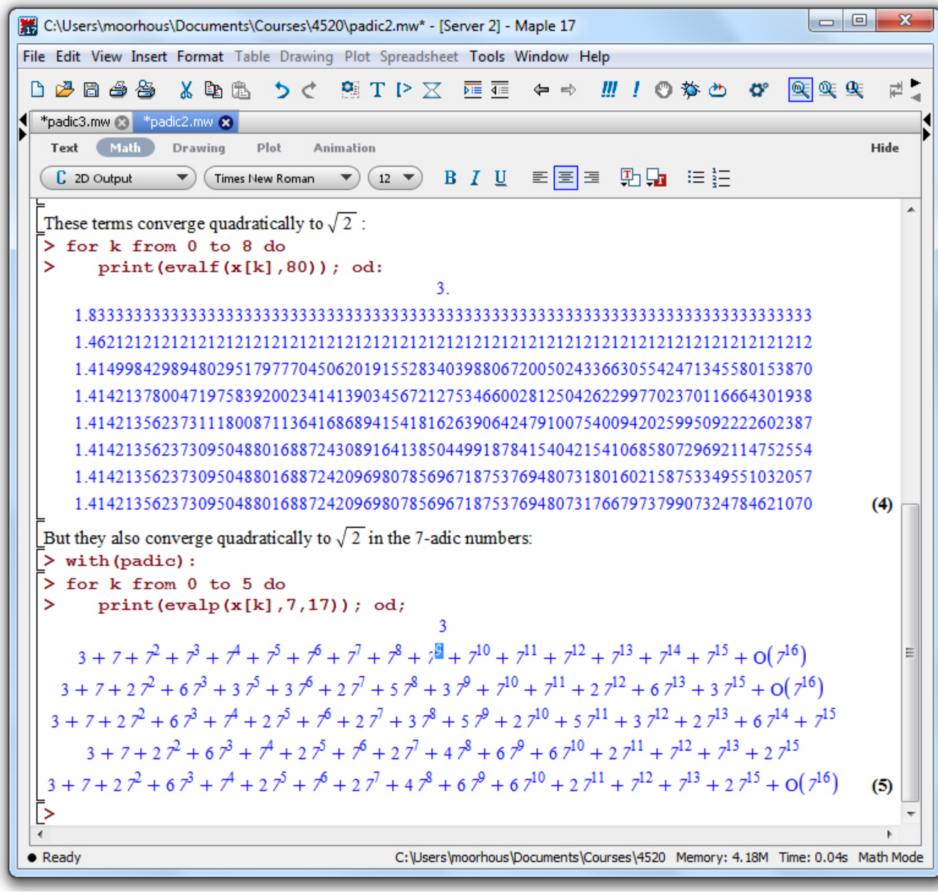
etc. The point is that at every iteration, we obtain not just one more digits of accuracy; rather, the number of digits of accuracy roughly doubles at every iteration. The sequence $x_0, x_1, x_2, \ldots$ is guaranteed to converge to $\sqrt{2}$ in $\mathbb{R}$ whenever the initial guess x_0 is positive. It will converge to the other root of $f(x) = 0$, i.e. $-\sqrt{2}$, if the inital guess x_0 is chosen to be negative. If we choose $x_0 = 0$, then x_1 and all subsequent terms are undefined.

Similar phenomena are observed in the 7-adic setting, where the expansions of the same sequence 3, $\frac{11}{6}$, $\frac{193}{132}$, ... are given by

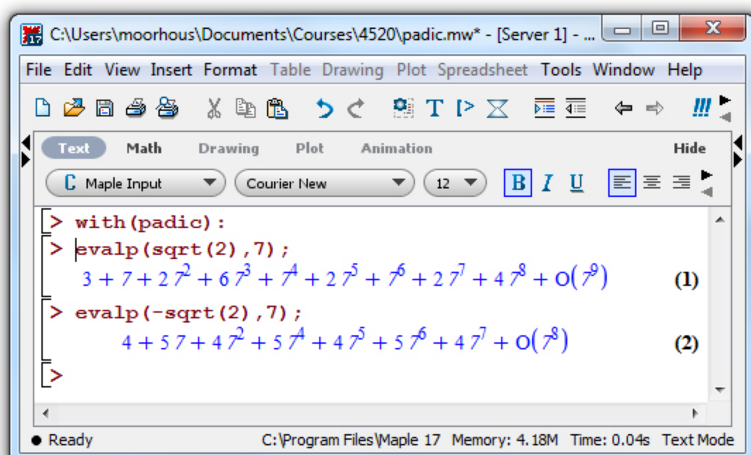
$$\begin{aligned}
x_0 &= 3\\
x_1 &= 3 + 7 + 7^2 + 7^3 + 7^4 + 7^5 + 7^6 + 7^7 + 7^8 + 7^9 + 7^{10} + 7^{11} + 7^{12} + 7^{13} + 7^{14} + \cdots\\
x_2 &= 3 + 7 + 2{\cdot}7^2 + 6{\cdot}7^3 + 3{\cdot}7^5 + 3{\cdot}7^6 + 2{\cdot}7^7 + 5{\cdot}7^8 + 3{\cdot}7^9 + 7^{10} + 7^{11} + 2{\cdot}7^{12} + 6{\cdot}7^{13} + \cdots\\
x_3 &= 3 + 7 + 2{\cdot}7^2 + 6{\cdot}7^3 + 7^4 + 2{\cdot}7^5 + 7^6 + 2{\cdot}7^7 + 3{\cdot}7^8 + 5{\cdot}7^9 + 2{\cdot}7^{10} + 5{\cdot}7^{11} + 3{\cdot}7^{12} + \cdots\\
x_4 &= 3 + 7 + 2{\cdot}7^2 + 6{\cdot}7^3 + 7^4 + 2{\cdot}7^5 + 7^6 + 2{\cdot}7^7 + 4{\cdot}7^8 + 6{\cdot}7^9 + 6{\cdot}7^{10} + 2{\cdot}7^{11} + 7^{12} + \cdots\\
x_5 &= 3 + 7 + 2{\cdot}7^2 + 6{\cdot}7^3 + 7^4 + 2{\cdot}7^5 + 7^6 + 2{\cdot}7^7 + 4{\cdot}7^8 + 6{\cdot}7^9 + 6{\cdot}7^{10} + 2{\cdot}7^{11} + 7^{12} + \cdots
\end{aligned}$$

etc. Note that once again, the number of digits of accuracy in our representation of $\sqrt{2}$ doubles with every iteration. The convergence to $\sqrt{2}$ is guaranteed for any initial guess x_0 congruent to $3 \mod 7$; and for any initial guess x_0 congruent to $4 \mod 7$, the resulting sequence converges to $-\sqrt{2}$. For other values of x_0, the sequence either fails to converge, or becomes undefined after the first term. Typically, Newton's Method may fail to converge if the first guess is not close enough to the desired root. Also, our sequence 1, $\frac{11}{6}$, $\frac{193}{132}$, ... does not converge in $\mathbb{Q}_5$, and for similar reasons ($x_0 = 3$ does not solve the congruence

$x^2 - 2 \equiv 0 \mod 5$). All these expansions, both decimal and 7-adic, were computed using Maple:



Now I should also disclose that Maple internally implements the required iterative procedure and so it is able to display the 7-adic expansion of $\sqrt{2}$ with a direct command:



Once again, we can list as many digits as desired; and they agree with the digits we found by explicit computation.