Division Algorithm in Full

Raghavan

February 2025

1 Algorithm

Lemma 1 *For any two positive integers* a, b *where* $a = a'B^n + s$ *and* $b = b'B^n$ *for some* $n > 0$, $0 \le s < B^n$ *(B is some base) it is true that* $\left\lfloor \frac{a}{b} \right\rfloor = \left\lfloor \frac{a'}{b'} \right\rfloor$.
Proof: Clearly

$$\frac{a}{b} \ge \frac{a'}{b'} \Rightarrow \left\lfloor \frac{a}{b} \right\rfloor \ge \left\lfloor \frac{a'}{b'} \right\rfloor \tag{1}$$

. Also

$$\frac{a}{b} = \frac{a'}{b'} + \frac{s}{b'B^n} < \frac{a'}{b'} + \frac{B^n}{b'B^n} = \frac{a'}{b'} + \frac{1}{b'}$$

Now $\frac{a'}{b'} = \frac{qb'+t}{b'} \le \frac{qb'+b'-1}{b'} = q + 1 - \frac{1}{b'}$ where $q = \left\lfloor \frac{a'}{b'} \right\rfloor$, $0 \le t < b'$. Therefore

$$\frac{a}{b} < \frac{a'}{b'} + \frac{1}{b'} \le \left\lfloor \frac{a'}{b'} \right\rfloor + 1 - \frac{1}{b'} + \frac{1}{b'} \Rightarrow \left\lfloor \frac{a'}{b'} \right\rfloor \le \left\lfloor \frac{a'}{b'} \right\rfloor \tag{2}$$

Putting (1) and (2) together we get

$$\left\lfloor \frac{a}{b} \right\rfloor = \left\lfloor \frac{a'}{b'} \right\rfloor$$

■

Lemma 2 *For any two positive integers* a, b *where* $a = a'B^n + s$ *and* $b = b'B^n + t$ *for some* $n > 0$, $0 \le s, t < B^n$ *(B is some base) it is true that* $\left\lfloor \frac{a'}{b'} \right\rfloor \ge \left\lfloor \frac{a}{b} \right\rfloor \ge \left\lfloor \frac{a'}{b'} \right\rfloor - 2$.
Proof: Clearly

$$\left\lfloor \frac{a}{b} \right\rfloor \le \left\lfloor \frac{a'B^n + s}{b'B^n} \right\rfloor = \left\lfloor \frac{a'}{b'} \right\rfloor \quad \text{From Lemma 1} \tag{3}$$

Assume $2bb' \ge a$.
We can see that

$$\frac{a}{b} \ge \frac{a'B^n}{(b'+1)B^n} = \frac{a'}{b'+1} \Rightarrow a + ab' \ge ba' \Rightarrow a \ge ba' - ab'$$

Combining this with our assumption above we get

$$2bb' \geq a \geq ba' - ab' \;\;\Rightarrow\;\; 2bb' + ab' \geq ba' \Rightarrow 2 + \frac{a}{b} \geq \frac{a'}{b'} \tag{4}$$

(3) and (4) together gives us

$$\left\lfloor \frac{a'}{b'} \right\rfloor \geq \left\lfloor \frac{a}{b} \right\rfloor \geq \left\lfloor \frac{a'}{b'} \right\rfloor - 2$$

■

The above lemma will be the basis for our division algorithm. Suppose we want to compute $q = \lfloor \frac{a}{b} \rfloor$ where $a = \sum_{i=0}^{k-1} a_i B^i$, $\;b = \sum_{i=0}^{l-1} b_i B^i$. Let's assume w.l.g that $k \geq l$. Also let $q = \sum_{i=0}^{k-l} q_i B^i$. We will also use the following notation: for any number a, $A_t^* \equiv \sum_{i \geq t} a_i B^{i-t}$ and $a_t^* \equiv \sum_{i<t} a_i B^i$. Note that using this notation $a = A_t^*.B^t + a_t^*$ for any t. Notice that A_t^* is the number formed by the top $(k-t)$ digits of a and a_t^* is the number formed by the bottom t digits of a. Trivially $a = A_0^* = a_k^*$.

The lemma below essentially says that to compute $\lfloor \frac{a}{b} \rfloor$ we only need to focus on a_{k-1} and b_{l-1}, the most significant digits of a, b respectively.

Lemma 3 *For any $a = \sum_{i=0}^{k-1} a_i B^i$, $\;b = \sum_{i=0}^{l-1} b_i B^i$ with $k \geq l$ and $q = \sum_{i=0}^{k-l} q_i B^i = \lfloor \frac{a}{b} \rfloor$ it is true that*

$$\left\lfloor \frac{a_{k-1}}{b_{l-1}} \right\rfloor \geq q_{k-l} \geq \left\lfloor \frac{a_{k-1}}{b_{l-1}} \right\rfloor - 2$$

Proof: We can write $q = q_{k-l}B^{k-l} + q_{k-l}^*$, $\;a = a_{k-1}B^{k-1} + a_{k-1}^*$, $\;b = b_{l-1}B^{l-1} + b_{l-1}^*$ where $0 \leq q_{k-l}^* < B^{k-l}$, $\;0 \leq a_{k-1}^* < B^{k-1}$, $\;0 \leq b_{l-1}^* < B^{l-1}$. Finally let $a = b.q + r$ where $0 \leq r < b$. Therefore

$$\begin{aligned}
q.b \leq a &= q.b + r \qquad (5)\\
\left(q_{k-l}B^{k-l} + q_{k-l}^*\right).b \leq a &= \left(q_{k-l}B^{k-l} + q_{k-l}^*\right).b + r\\
q_{k-l}B^{k-l}.b \leq \left(q_{k-l}B^{k-l} + q_{k-l}^*\right).b \leq a &= \left(q_{k-l}B^{k-l} + q_{k-l}^*\right).b + r\\
q_{k-l} \leq \frac{a}{b.B^{k-l}} &= q_{k-l} + \frac{q_{k-l}^*.b + r}{b.B^{k-l}}\\
&< q_{k-l} + \frac{q_{k-l}^*.b + b}{b.B^{k-l}} = q_{k-l} + \frac{q_{k-l}^* + 1}{B^{k-l}}\\
&\leq q_{k-l} + \frac{B^{k-l} - 1 + 1}{B^{k-l}} = q_{k-l} + 1
\end{aligned}$$

Therefore $q_{k-l} \leq \frac{a}{b.B^{k-l}} < q_{k-l} + 1$. From the definition of $\lfloor . \rfloor$ we have that $\left\lfloor \frac{a}{b.B^{k-l}} \right\rfloor = q_{k-l}$.

Now

$$\left\lfloor \frac{a}{b.B^{k-l}} \right\rfloor = \left\lfloor \frac{a_{k-1}B^{k-1} + a_{k-1}^*}{\left(b_{l-1}B^{l-1} + b_{l-1}^*\right).B^{k-l}} \right\rfloor = \left\lfloor \frac{a_{k-1}B^{k-1} + a_{k-1}^*}{b_{l-1}B^{k-1} + b_{l-1}^*.B^{k-l}} \right\rfloor$$

Therefore we have the form of the Lemma 2 where we want to compute $\left\lfloor \frac{a_{k-1}B^{k-1}+s}{b_{l-1}B^{k-1}+t} \right\rfloor$ where $0 \le s, t < B^{k-1}$ — note that $b^*_{l-1} < B^{l-1}$. Now from Lemma 2 we get

$$\left\lfloor \frac{a_{k-1}}{b_{l-1}} \right\rfloor \ge q_{k-l} = \left\lfloor \frac{a_{k-1}B^{k-1}+s}{b_{l-1}B^{k-1}+t} \right\rfloor \ge \left\lfloor \frac{a_{k-1}}{b_{l-1}} \right\rfloor - 2$$

■

Lemma 3 is therefore saying that to get the most significant digit of q, we only only need to find $\left\lfloor \frac{a_{k-1}}{b_{l-1}} \right\rfloor$ — the actual q_{k-l} will be at most 2 less than the ratio of the most significant digits of a, b respectively.

We still have to ensure that the precondition for Lemma 2 is satisfied, i.e., $2b_{l-1}\left(b_{l-1}B^{k-1}+t\right) \ge a$. This is easily done by assuming that $b_{l-1} \ge \frac{B}{2}$. With this the LHS is at least $B\left(b_{l-1}B^{k-1}+t\right)$. Note that both $a_{k-1}B^{k-1}+s$ and $b_{l-1}B^{k-1}+t$ are k-digit numbers. Therefore $B\left(b_{l-1}B^{k-1}+t\right)$ will be a $(k+1)$-digit number and hence must be greater than a, the numerator.

So for all the above to work, we have replaced the assumption of Lemma 2 by a new assumption – that $b_{l-1} \ge \frac{B}{2}$. We will take care of this later.

We can now use the result of Lemma 3 recursively to compute q. To see how to go forward let's extend the above procedure to the next significant digit of the quotient and see what happens. Suppose we found the correct q_{k-l}. Let's rewrite (5) above as

$$A^*_{k-l}.B^{k-l} + a^*_{k-l} = \left(q_{k-l}.B^{k-l} + q^*_{k-l}\right).b + r \tag{6}$$

$$\left(A^*_{k-l} - q_{k-l}.b\right).B^{k-l} + a^*_{k-l} = q^*_{k-l}.b + r$$

$$\tilde{A}^*_{k-l}.B^{k-l} + \tilde{a}_{k-l-1}.B^{k-l-1} + \tilde{a}^*_{k-l-1} = \left(q_{k-l-1}.B^{k-l-1} + q^*_{k-l-1}\right).b + r \tag{7}$$

$$\left(\tilde{A}^*_{k-l}.B + \tilde{a}_{k-l-1}\right).B^{k-l-1} + \tilde{a}^*_{k-l-1} = \left(q_{k-l-1}.B^{k-l-1} + q^*_{k-l-1}\right).b + r$$

$$\tilde{A}^*_{k-l-1}.B^{k-l-1} + \tilde{a}^*_{k-l-1} = \left(q_{k-l-1}.B^{k-l-1} + q^*_{k-l-1}\right).b + r \tag{8}$$

From step (7) we have used $\tilde{a}$ to denote the number for which $\tilde{A}^*_{k-l} = \left(A^*_{k-l} - q_{k-l}.b\right)$ and $\tilde{a}^*_{k-l} = a^*_{k-l}$ ($\tilde{a}$ is the number obtained by replacing A^*_{k-l} by $\left(A^*_{k-l} - q_{k-l}.b\right)$ in a. Clearly (8) has exactly the same form as (6), with $(k-l)$ replaced by $(k-l-1)$ and of course a replaced by $\tilde{a}$. We can therefore use Lemma 3 again on (8) to obtain q_{k-l-1}. We can repeat this process till we obtain all the digits of q i.e., till $\tilde{a}$ on the LHS becomes less than b. The final $\tilde{a}$ will then be the remainder r.

Putting all of the above together, the full algorithm is shown as Algorithm 1.

A few things to note about Algorithm 1.

1. The only explicit division we do is by b_{l-1} which is clearly at most $(B-1)$ — the algorithm therefore reduces the general division to division by single digits.

2. The notation we have used is convenient because we have assumed a to have constant length throughout (with 0's padded to the left as necessary).

Algorithm 1 `Divide`(a, b)

1: $a = a_{k-1}B^{k-1} + a^*_{k-1}, \quad b = b_{l-1}B^{l-1} + b^*_{l-1}$
2: Let $a_k \leftarrow 0$
3: **for** $i = (k-l), \ldots, 0$ **do**
4: $\quad q_i \leftarrow \left\lfloor \frac{a_{i+l} * B + a_{i+l-1}}{b_{l-1}} \right\rfloor$
5: $\quad$ **while** $q_i.b > A^*_i$ **do** ⊳ This loop will happen at most twice
6: $\quad\quad q_i \leftarrow q_i - 1$
7: $\quad$ **end while**
8: $\quad a \leftarrow (A^*_i - q_i.b).B^i + a^*_i$ ⊳ RHS was denoted as $\tilde{a}$ in the description above.
9: **end for**

3. We still need to address the assumption we made in the box — that $b_{l-1} \geq \frac{B}{2}$. What if $b_{l-1} < \frac{B}{2}$? We have $a = q.b + r \Rightarrow c.a = q.(c.b) + (c.r)$ for any constant c. So if we divide $c.a$ by $c.b$ instead of dividing a by b we would still get exactly the same quotient. We can finally divide the remainder obtained by c again to get the actual r. This should work as long as c is a small constant. We can now pick an appropriate c such that the most significant digit of $c.b$ is at least $\frac{B}{2}$. If you are not convinced that this can always be done, please see the Appendix (I suggest you try proving this yourself first!!)

4. The running time analysis is simple — steps 4 and 8 are constant time operations. Step 5 involves multiplying b by a single digit q_i — so this requires time $O(\texttt{len}(b))$ and this may get repeated at most twice. So the time for each iteration of the loop in steps 3-8 is $O(\texttt{len}(b))$. Number of iterations is $\texttt{len}(q)$. Therefore the overall running time is $O(\texttt{len}(q).\texttt{len}(b))$.

2 Numeric Example

Let's apply the algorithm we have described for a division between two arbitrary positive integers in base 10. Suppose we want to divide 3689023156 by 87659. For our reference

$$3689023156 = (42083) * (87659) + 69459$$

Also $k = 10, l = 5$. We will use braces to show where the current $i + l - 1$ is (step 4 of the algorithm, to indicate the digit of a we will be using next) and boldface to show where the current i is (step 8) during the run of the algorithm. So we start with $a = (3)(6890\mathbf{23156})$.

1. $i = k - l = 5$. $\lfloor 3/8 \rfloor = 0$. $q_5 = 0$. Nothing to be done. The new a is $(36)(8902\mathbf{3156})$.

2. $i = 4$. First guess for $q_4 = \lfloor 36/8 \rfloor = 4$. $4 * 87659 = 350636 < A^*_4 = 368902$. So q_4 is indeed 4. The new a becomes $(018)(2663\mathbf{156})$ where $18266 = 368902 - 350636$. Note the 0-padding on the left.

3. $i = 3$. $q_3 = \lfloor 018/8 \rfloor = 2$. $2 * 87659 = 175318 < A^*_3 = 0182663$. So 2 is the correct q_3. The new a is now $(0007)(3451\mathbf{56})$.

4. $i = 2$. $a_2 = 0007$. $q_2 = 0$. The new a is (00073)(4515**6**).

5. $i = 1$. $a_1 = 00073$. First guess for $q_1 = \lfloor 73/8 \rfloor = 9$. But $9 * 87659 = 788931 > 734515$. Let's therefore try $q_1 = 8$. Now $8 * 87659 = 701272 < 734515$. So q_1 is in fact 8. The new a becomes (000033)(2436) where $33243 = 734515 - 701272$.

6. $i = 0$. $a_0 = 000033$. $q_0 = 4$ is the first guess. Again $4 * 87659 = 350636 > 332436$. Let's try $q_0 = 3$. $3 * 87659 = 262977 < 332436$. This is correct. The remainder is therefore $332436 - 262977 = 69459$.

7. The quotient q is therefore 42083 and the remainder 69459.

3 Appendix: Choosing c to ensure that $c.b$ remains a l digit number and $(c.b)_{l-1} \geq \frac{B}{2}$

Clearly

$$
\begin{aligned}
b_{l-1}.B^{l-1} \leq b \leq b_{l-1}.B^{l-1} + B^{l-1} - 1 \\
c.b_{l-1}.B^{l-1} \leq c.b \leq c.b_{l-1}.B^{l-1} + c.\left(B^{l-1} - 1\right) \\
< c.b_{l-1}.B^{l-1} + c.B^{l-1} \\
= c.(b_{l-1} + 1).B^{l-1}
\end{aligned}
$$

Therefore the most significant digit of $c.b$ is bounded to the interval $[c.b_{l-1} \ldots c(b_{l-1} + 1)]$. So if we pick c to be something like $\frac{B}{2b_{l-1}}$ this interval becomes $\frac{B}{2} \ldots \left(\frac{B}{2} + \delta\right)]$ for some $\delta < \frac{b}{2}$. Therefore we have ensured that $(c.b)_{l-1} \geq \frac{B}{2}$ and $c.b$ remains a l digit number.

This becomes particularly convenient when we work in binary — c will be some small power of 2 and multiplication by c ends up as a simple left shift.