

Where I can put my new Theorem of the Day

The web site <http://myweb.lsbu.ac.uk/~whitty/MathSci/TheoremOfTheDay> maintains a list of, say, L theorems. These are picked in turn to be displayed as ‘Theorem of the Day’. To do this, a javascript function measures the number of milliseconds since a fixed base date and divides this by 86400000, the number of milliseconds in twenty four hours. The result, rounded down, is a number of days, D , which increases by one every midnight. The theorem displayed on any given day is chosen as theorem number $D \pmod{L}$ in the list (indexed from 0 to $L - 1$).

As often as possible I choose another classic theorem and add a description of it to the web site; with respect to the above, this increases L to $L + 1$, while D remains fixed. My problem is that I want to do this without the order of presentation of the theorems (and today’s already chosen theorem in particular) being disturbed. So while adding the new theorem I have also to cycle the list of theorems round to bring position $D \pmod{L}$ into position $D \pmod{L + 1}$.

Now the question is, how do I discover the current value of D ? The answer I would like to give is that I use a scrupulously coded algorithm based on Dershowitz and Reingold’s timeless [Calendrical Calculations](#) (Cambridge University Press, 2001). The reality is that I cheat: I increase the theorem array size by 1, upload the java code, observe what theorem is now (illicitly) occupying today’s slot and make haste to re-upload with the correct theorem cycled into its rightful position.

However, in the process of pulling this fast one, I do get to find out the value of D ; and it seems worth mentioning how because it is a nice illustration of one of the Theorems of the Day: the [Chinese Remainder Theorem](#).

So, suppose that the day’s theorem is currently in position s in the list, the value of $D \pmod{L}$, and that, when I add the new theorem, the current theorem changes to $D \pmod{L + 1}$, which we notice is position t in the list. This is written as a pair of congruence equations in the unknown, D :

$$D \equiv s \pmod{L}, \quad D \equiv t \pmod{L + 1}. \quad (1)$$

Now the Chinese Remainder Theorem, in its simplest form, says that

$$x \equiv a \pmod{m}, \quad x \equiv b \pmod{n},$$

where $\gcd(m, n) = 1$, is solved, uniquely mod mn , by:

$$x = am(m^{-1} \pmod{n}) + bn(n^{-1} \pmod{m}), \quad (2)$$

where $m^{-1} \pmod{n}$ is the least positive multiple of m which has remainder 1 \pmod{n} .

Now it is easy to see that $L^{-1} \pmod{L + 1} = L$, since $L^2 = (L + 1)(L - 1) + 1 \equiv 1 \pmod{L + 1}$, and $(L + 1)^{-1} \pmod{L} = L + 1$, since $(L + 1)^2 = L^2 + 2L + 1 \equiv 1 \pmod{L}$. So equation (1) is solved by

$$\begin{aligned} D &= s(L + 1)((L + 1)^{-1} \pmod{L}) + tL(L^{-1} \pmod{L + 1}) \pmod{L(L + 1)} \\ &= s(L + 1)^2 + tL^2 \pmod{L(L + 1)} \end{aligned}$$

Example: suppose today’s theorem is number 4 in the list of 42. I add a new theorem and now the theorem displayed has changed to number 16 (out of 43). Then

$$D = 4 \times 43^2 + 16 \times 42^2 \pmod{42 \times 43} = 35620 \pmod{1806} = 1306.$$

A doubt remains in my mind: is there not some clever way to find out the value of D without making today’s theorem temporarily change? Perhaps instead of increasing L to $L + 1$ some other increased length L' would reveal D without changing from theorem s to t (L' does not have to be coprime to L ; provided $s \equiv t \pmod{\gcd(L, L')}$ an extended version of the Chinese Remainder Theorem still applies.) Or there is some other approach I have not thought of.