Power of 2 Problem

(22 February 2005, rev 17 August 2011)

Jim Stevenson

7^{th} Grade Problem: What is the largest power of 2 that divides 800! without a remainder?

Answer: 2^{797}

Solution (Jim Stevenson, 3 February 2005): All the factors in 800! = 800*799*798*…*3*2*1 are of the form 2^n * M for some n ≥ 0 and some M containing no factors of 2, that is, M is odd. So to solve the problem, we are looking to find out how many odd numbers we can multiply by a power of 2 (2^n n > 0) and still have a result less than 800. For example, the maximum integer times 2 that is less than or equal to 800 is 400. The number of odd numbers less than 400 is 200. So there are 200 numbers with only one factor of 2. Notice that a number with 2^2 in it is also divisible by 2^1, but the M multiplying 2^1 would no longer be odd. So all the numbers less than 800 that are divisible by 4 but no other power of 2 are distinct from those divisible by 2 and no other power of 2.

Power of 2			Largest integer M so that 2^n * M ≤ 800				Number of odd numbers ≤ M		Sum of exponents	
2^9	=	512	800 / 512 =	1.563	⇒	1	1 + 0/2 =	1	1 * 9 =	9
2^8	=	256	800 / 256 =	3.125	⇒	3	1 + 2/2 =	2	2 * 8 =	16
2^7	=	128	800 / 128 =	6.25	⇒	6	6 / 2 =	3	3 * 7 =	21
2^6	=	64	800 / 64 =	12.5	⇒	12	12 / 2 =	6	6 * 6 =	36
2^5	=	32	800 / 32 =	25	⇒	25	1 + 24 / 2 =	13	13 * 5 =	65
2^4	=	16	800 / 16 =	50	⇒	50	50 / 2 =	25	25 * 4 =	100
2^3	=	8	800 / 8 =	100	⇒	100	100 / 2 =	50	50 * 3 =	150
2^2	=	4	800 / 4 =	200	⇒	200	200 / 2 =	100	100 * 2 =	200
2^1	=	2	800 / 2 =	400	⇒	400	400 / 2 =	200	200 * 1 =	200
									Total	**797**

This solution is what is called a "bute force" solution (by examples), which is not considered elegant by typical mathematicians. The following alternative is definitely elegant and stems from the mind of an abstract algebraist (which I am not). It is a nice example of how algebraists think and approach such problems.

Alternate Solution 1 (Dr. Harold Stolberg, 9 February 2005)

I believe I have a solution to your problem and my result, if my lunch calculations are right, comes to an impossibly high number, but I guess the factorial is huge enough. I have as a max divisor of 800!, 2^{797}. The way I looked at it is to use the recursive iteration n!=n*(n-1)! and the fact that the exponent of odd numbers is zero. More succinctly, let u(n) be the exponent of 2 dividing n. Then clearly u(800!) = u(800) + u(799!). Using iteration and the above fact about odd numbers, u(800!) = u(2) + u(4) +...+ u(2*n) +...+ u(798) + u(800). But this series is easily computable because it autogenerates itself, using the logarithmic nature of u( ). Thus, it equals 400 + u(2) + u(4) + ... + u(400) [see JOS note below], (remember u(odd num)=0). Two or three iterations more, you get that u(800!) = 400 + 200 + 100 + 50 + 25 + u(2) + u(4) + ... + u(24). Note that the last item should have been u(25) keeping with the last pattern but that is equal to zero. Note also that that corresponds to the max power of 2 dividing 800, i.e. 32*25. One more iteration brings it down to u(800!)= 400 + 200 +100 + 50 + 25 + 12 + u(2) + u(4) + u(6) + u(8) + u(10) + u(12). But the latter are all computable so, if my arrangements are right, I get 797. This is all painful to write out, especially in email. Cute problem though.

[*JOS:* Filling in some steps:

Define: u(n) = max exponent of 2 dividing n. Note: u(2) = 1

Problem: To find u(800!) (or the power $2^{u(800!)}$).

Important Fact 1: **u(n) = 0, for n odd** (that is, n not divisible by 2)
Important Fact 2: **u(m*n) = u(m) + u(n)** (logarithmic property)

Therefore,

u(800!) = u(800) + u(798) + … + u(2*n) + …+ u(2)
= u(2*400) + u(2*399) + … + u(2*n) + … u(2*1)
= u(2) + u(400) + u(2) + u(399) + … u(2) + u(n) + … + u(2) + u(1)
= 400*u(2) + u(400) + u(399) + … + u(n) + … + u(1)
= 400 + u(400) + u(398) + … + u(2*m) + … + u(2) (remember u(N) = 0 N odd)
= 400 + u(2*200) + u(2*199) + … + u(2*m) + … + u(2)
= 400 + 200 + u(200) + u(199) + … + u(m) + … + u(1)
= 400 + 200 + 100 + u(100) + u(99) + … + u(k) + … + u(1)
= 400 + 200 + 100 + 50 + u(50) + u(49) + … + u(s) + … + u(1)
= 400 + 200 + 100 + 50 + 25 + u(25) + u(24) + … + u(t) + … + u(1)
= 400 + 200 + 100 + 50 + 25 + 12 + u(12) + u(11) + … + u(1)
= 400 + 200 + 100 + 50 + 25 + 12 + 6 + u(6) + u(5) + … + u(1)
= 400 + 200 + 100 + 50 + 25 + 12 + 6 + 3 + u(3) + u(2) + u(1)
= 400 + 200 + 100 + 50 + 25 + 12 + 6 + 3 + 1
= 797]

The nice thing about Dr. Stolberg's solution is that it shows an obvious pattern that could generalize to compute u(n!) for any n:

$$\boxed{u(n!) = \begin{cases} \frac{n}{2} + u(\frac{n}{2}!) & \text{if n even} \\ \frac{n-1}{2} + u(\frac{n-1}{2}!) & \text{if n odd} \end{cases}} \qquad (*)$$

Then proceed recursively.

A second alternative solution is even more elegant—and surprising and humbling (to us mathematicians), because it comes from a theoretical physicist. This is a reminder that physicists have to be mathematicians too.

Alternate Solution 2 (Dr. Mark Suskin, 10 February 2005)

Harold: It's 2^{797}, which is really $2^{(800-3)}$ because there are three ones in the binary representation of 800. You, as a mathematician, probably have a slicker way to do it, but that's the solution from the physicist's corner.

[*JOS:* Filling in some steps!

Consider the binary expansion for n, where m is the largest exponent of 2 such that $2^m \le n$. Then

$$n = a_m 2^m + a_{m-1} 2^{m-1} + \ldots + a_1 2 + a_0$$

where the a_i equal 0 or 1, and $a_m = 1$. For example, omitting the powers of 2, as we do with decimals, we can write 800 in binary notation as

800 = 1100100000 ($n = a_m a_{m-1} \ldots a_1 a_0$)

Then the recursive relationship (*) from the previous solution means (noticing that the cases odd or even are both handled by using the binary coefficient, since it will be 1 if the number is odd and 0 if it is even):

$$\begin{aligned}
\mathrm{u}(n!) &= (n-a_0)\tfrac{1}{2} + \mathrm{u}((a_m 2^{m-1} + a_{m-1} 2^{m-2} + \ldots + a_1)!) \\
&= (n-a_0)\tfrac{1}{2} \\
&\quad + ((n-a_0)\tfrac{1}{2} - a_1)\tfrac{1}{2} \\
&\quad + (((n-a_0)\tfrac{1}{2} - a_1)\tfrac{1}{2} - a_2)\tfrac{1}{2} \\
&\quad + \ldots \\
&\quad + (\ldots(((n-a_0)\tfrac{1}{2} - a_1)\tfrac{1}{2} - a_2)\tfrac{1}{2} \ldots - a_{m-1})\tfrac{1}{2} \\
&= n\tfrac{1}{2} - a_0 \tfrac{1}{2} \\
&\quad + n\tfrac{1}{2^2} - a_0 \tfrac{1}{2^2} - a_1 \tfrac{1}{2} \\
&\quad + n\tfrac{1}{2^3} - a_0 \tfrac{1}{2^3} - a_1 \tfrac{1}{2^2} - a_2 \tfrac{1}{2} \\
&\quad + \ldots \\
&\quad + n\tfrac{1}{2^m} - a_0 \tfrac{1}{2^m} - a_1 \tfrac{1}{2^{m-1}} - a_2 \tfrac{1}{2^{m-2}} \ldots - a_{m-1} \tfrac{1}{2^1} \\
&= n(\tfrac{1}{2} + \tfrac{1}{2^2} + \tfrac{1}{2^3} + \ldots + \tfrac{1}{2^m}) \\
&\quad - a_0(\tfrac{1}{2} + \tfrac{1}{2^2} + \tfrac{1}{2^3} + \ldots + \tfrac{1}{2^m}) \\
&\quad - a_1(\tfrac{1}{2} + \tfrac{1}{2^2} + \tfrac{1}{2^3} + \ldots + \tfrac{1}{2^{m-1}}) \\
&\quad - a_2(\tfrac{1}{2} + \tfrac{1}{2^2} + \tfrac{1}{2^3} + \ldots + \tfrac{1}{2^{m-2}}) \\
&\quad - \ldots \\
&\quad - a_{m-1} \tfrac{1}{2^1} \\
&= n(1 - \tfrac{1}{2^m}) - a_0(1 - \tfrac{1}{2^m}) - a_1(1 - \tfrac{1}{2^{m-1}}) - a_2(1 - \tfrac{1}{2^{m-2}}) - \ldots - a_{m-1}(1 - \tfrac{1}{2^1})
\end{aligned}$$

using the geometric progression formula

$$1 + r + r^2 + r^3 + \ldots + r^m = \frac{1 - r^{m+1}}{1 - r}$$

which implies

$$\tfrac{1}{2} + \tfrac{1}{2}^2 + \tfrac{1}{2}^3 + \ldots + \tfrac{1}{2}^m = \tfrac{1}{2}(1 + \tfrac{1}{2} + \tfrac{1}{2}^2 + \tfrac{1}{2}^3 + \ldots + \tfrac{1}{2}^{m-1}) = \tfrac{1}{2}\frac{1 - \tfrac{1}{2}^m}{1 - \tfrac{1}{2}} = 1 - \tfrac{1}{2}^m$$

Then

$$\text{u(n!)} = n - a_0 - a_1 - a_2 - \ldots - a_{m-1} - \tfrac{1}{2^m}(n - (a_0 + a_1 2^1 + a_2 2^2 + \ldots + a_{m-1} 2^{m-1}))$$
$$n - a_0 - a_1 - a_2 - \ldots - a_{m-1} - \tfrac{1}{2^m}(a_m 2^m)$$

So that

$$\boxed{\text{u(n!)} = n - (a_0 + a_1 + a_2 + \ldots + a_m)} \qquad (**)$$

Then for n = 800, $a_9 = a_8 = a_5 = 1$, and the rest = 0, so that u(800!) = 800 - 3 = 797.]

Alternate Solution 2a (Jim Stevenson, 22 February 2005)

The following discussion might come under the heading of mathematical noodling. From the outside it might appear that it is much ado about nothing and that the reason for even bothering seems obscure. It concerns proving equation (**) above using *mathematical induction*. One might argue we already proved the equation for all n, so why bother? That is true, but it offers an alternate approach. What really gives the impression of circular reasoning, is that we need to start with the equation (**)! Usually how the approach works is to try some simple examples for n = 1, 2, 3, say, and then *guess* at the general formula for n. Once having a *guess*, we need to *prove* it holds for all n.

The idea of mathematical induction is the following:

Principle of Mathematical Induction:

Given: (i) Statement P(n) associated with each natural number n = 1, 2, 3, …
(ii) P(1) is true.
(iii) For all natural numbers k = 1, 2, 3, … , if P(k) is true, then P(k+1) is true.

Then: For all natural numbers n = 1, 2, 3, …. , P(n) is true.

The strange thing about this approach is that in place of the original infinite set of statements to prove, P(n), we try to prove another infinite set of statements, S(k) = "P(k) => P(k+1)", where "A => B" means *A implies B* or *if A, then B*. For this to work, it must be easier to prove the S(k) than the P(n). An analogy might be we wish to prove we can knock down a whole set of dominoes with one push. P(n) might be "domino n will fall". Now if we check that for every pair of dominoes, if the first one falls the next one will, say by separating them by half their height, then if we make the first domino fall, we can be assured they all will fall.

So the statement P(n) is

P(n): "u(n!) = $n - (a_0 + a_1 + a_2 + \ldots + a_m)$ where the a_i, i = 0, …, m, are the coefficients of the binary expansion of n."

Then P(1): u(1!) = 1 – $(a_0 + a_1 + a_2 + \ldots + a_m)$. Now $n = a_m 2^m + a_{m-1} 2^{m-1} + \ldots + a_1 2 + a_0 = 1$ means all $a_i = 0$, except a_0, which must equal 1. Therefore u(1!) = 1 – 1 = 0, and 0 is the exponent of the largest power of 2 dividing n = 1 evenly (recall that $2^0 = 1$, by convention).

Now suppose P(k): "u(k!) = $k - (a_0 + a_1 + a_2 + \ldots + a_s)$ where the a_i, i = 0, …, s, are the coefficients of the binary expansion of k." is true (so that $k = a_s 2^s + a_{s-1} 2^{s-1} + \ldots + a_1 2 + a_0$). We want to use this to prove P(k+1): "u((k+1)!) = $k + 1 - (b_0 + b_1 + b_2 + \ldots + b_t)$ where the b_i, i = 0, …, t, are the coefficients of the binary expansion of k+1." (so that $k+1 = b_t 2^t + b_{t-1} 2^{t-1} + \ldots + b_1 2 + b_0$). Using the property u((k+1)!) = u(k+1) + u(k!), we have

u((k+1)!) = u(k+1) + $k - (a_0 + a_1 + a_2 + \ldots + a_s)$

Let v = u(k+1). Then 2^v divides k+1 evenly (and is the largest power of 2) so that its binary representation is

$$k+1 = b_t 2^t + b_{t-1} 2^{t-1} + \ldots + b_v 2^v = 2^v (b_t 2^{t-v} + b_{t-1} 2^{t-1-v} + \ldots + b_v)$$

where $b_v = 1$ (since 2^v is the largest power of 2 dividing k +1). So we have

u((k+1)!) = $v + k - (a_0 + a_1 + a_2 + \ldots + a_s)$

Now k + 1 is 1 added to k. What would the binary coefficients a_i of k have to be to make all the b_i = 0 for i < v and b_v = 1? We would have the v coefficients a_i = 1 for i = 0, 1, 2, …, $v - 1$, and a_v = 0. Hence,

u((k+1)!) = $k - (a_{v+1} + \ldots + a_s)$

Furthermore, all the b_i for i > v (if there are any) would have to be the same as the a_i (so that $s = t$). Hence,

u((k+1)!) = $k - (b_{v+1} + \ldots + b_t) = k + 1 - (1 + b_{v+1} + \ldots + b_t)$

and because b_v = 1 and b_i = 0 for i < v,

u((k+1)!) = $k + 1 - (b_v + b_{v+1} + \ldots + b_t)$
$= k + 1 - (b_0 + b_1 + \ldots + b_t)$

which is P(k+1). (There is some fussing with the end conditions, where $v = t$ or $v = 0$, for example.) So now we have proved for all k that P(k) => P(k+1). Therefore by mathematical induction we have proved for all n, P(n) is true.

This is not a very elegant proof. In fact it is ugly. Perhaps there is a more elegant proof by induction. Again this is more an exercise in the mathematical game of finding proofs. It still really begs the question of how we got equation (**) in the first place. It is not at all obvious, in fact, that a formula for something involving all integers from 1 to n only involves the binary expansion of the last number.

Alternate Solution 2b (Dr. Harold Stolberg, 22 February 2005)

My induction proof is concerned with Mark's formula, that is, using the exponential notation, that u(n!)= n - (number of ones in the binary expansion of n). Call that number of 1's, O(n) for the sake of writing that statement out.

Proof: Evident for the first few n's. Two cases: let n be odd. Then u(n!) = u(n) + u((n-1)! = u((n-1)!) from the logarithmic, or if you prefer, homomorphic property of u, the relation n! = n*(n-1)! and the fact that u(n)=0 since n is odd. By induction, u((n-1)!) = n-1 - (number of 1's in the binary expansion of n-1) = n-1 - O(n-1). But since n is odd, n-1 is even, which means that its binary expansion ends in 0. But then O(n) = O(n-1) + 1 since you add a one to the even number to get its successor. But then u(n!) = u((n-1)!) = n-1 - O(n-1) = n-1 - O(n)+1 = (mirabile dictu!) n-O(n), which is the formula that you want for n. The case for n even, I did differently – although I suspect that a similar argument to the above works – and involves binary multiplication by 2, but after writing so many parenthesis, I'm not sure that I want to type some more at this time.

[*JOS:* Adding details.

The statement to prove by induction is

P(n): u(n!) = n – O(n) where O(n) = number of ones in the binary expansion of n

We have already shown P(1) is true. Now assume P(k-1) is true and use it to prove P(k).

Case 1. k is odd

Then by the logarithmic (homomorphic) property, the fact that u(k) = 0 for odd k, and the fact that P(k-1) is assumed true, we have

u(k!) = u(k (k-1)!) = u(k) + u((k-1)!) = 0 + k – 1 – O(k-1)

Since k is odd and k-1 is even, the binary representation for k-1 ends in a 0. Therefore, adding a 1 to k-1 only changes the last (zeroth) binary coefficient for k from a 0 to a 1, and so increases the number of ones in the binary expansion by one, so that O(k) = O(k-1) + 1. Thus

u(k!) = k – O(k)

which is P(k). So we have proved for all odd k, P(k-1) => P(k). Now we need to consider the case of even k.

Case 2. k even

Again assuming P(k-1) is true and all the previously mentioned properties for u(k), we have

u(k!) = u(k) + u((k-1)!) = u(k) + k-1 – O(k-1)

What we would like to show is that O(k) = O(k-1) +1 – u(k). This turns out to really be the argument used in Alternate Solution 2a. Let ν = u(k). Then ν represents the exponent for the largest power of 2 dividing k evenly. This means the ν^{th} binary coefficient of k is a 1 and all smaller coefficients are 0, whereas the zeroth coefficient of k-1 is 1. To arrive at k by adding 1 to k-1 means we must have had ones in the binary expansion for k-1 from 0 to ν-1 and a zero for the ν^{th} coefficient. So by adding 1 to k-1 we have subtracted ν ones and added a single 1 to O(k-1), which is exactly the statement O(k) = O(k-1) +1 – u(k). Thus P(k) is true for k even as well, and we have proved for all even k, P(k-1) => P(k).

Therefore we have proved for all k, P(k-1) => P(k). And so by the Principle of Mathematical Induction, P(n) is true for all n.

Comment: This argument seems to be a cleaner version of my 2a solution.

Alternate Solution 1a (Jim Stevenson, 22 February 2005)

Perhaps a better application of the Principle of Mathematical Induction would be to prove equation (*), since that was conjectured and not actually proved. Then the statement P(n) would be

$$\text{P(n):}\quad u(n!) = \begin{cases} \frac{n}{2} + u(\frac{n}{2}!) & \text{if n even} \\ \frac{n-1}{2} + u(\frac{n-1}{2}!) & \text{if n odd} \end{cases}$$

Now P(1): u(1!) = 0/2 + u(0!). By convention 0! = 1, so u(1) = 0, and therefore u(1!) = 0. Now suppose we assume P(k) is true and try to use this to prove P(k+1).

Case 1. k+1 is odd

This means k is even, so

$$u((k+1)!) = u(k+1) + u(k!) = 0 + \tfrac{k}{2} + u(\tfrac{k}{2}!) = \tfrac{(k+1)-1}{2} + u(\tfrac{(k+1)-1}{2}!)$$

Case 2. k+1 even

This means k is odd, so

$$\begin{aligned} u((k+1)!) &= u(k+1) + u(k!) = u(k+1) + \tfrac{k-1}{2} + u(\tfrac{k-1}{2}!) \qquad \text{(assuming P(k))} \\ &= u(2\tfrac{(k+1)}{2}) + \tfrac{k-1}{2} + u(\tfrac{k-1}{2}!) = u(2) + u(\tfrac{k+1}{2}) + \tfrac{k-1}{2} + u(\tfrac{k-1}{2}!) \\ &= 1 + u(\tfrac{k+1}{2}) + \tfrac{k-1}{2} + u(\tfrac{k-1}{2}!) = \tfrac{k+1}{2} + u(\tfrac{k+1}{2}!) \end{aligned}$$

So P(k+1) is true, assuming the validity of P(k). Hence, P(n) is true for all n.