A problem in MSE

- ***"How many rationals*** $\frac{2^n+1}{n^2}$ ***are integer" ?***[1]

1. The problem and some useful notations

First observation is, that the numerator is odd, so also the denominator, thus also n must be odd.

(1) $n = 2m+1$

For the following analysis we reformulate (introducing an uninteresting indeterminate cofactor x):

(2a) $2^n + 1 = n^2 x \qquad n, x \in N^+ \setminus 2N^+$

and

(2b) $2^n + 1 = \dfrac{2^{2n}-1}{2^n-1}$

We introduce the following general notation of the canonical primefactor-decomposition for some 2^n-1 :

(3) $2^n - 1 = p_1^{[n:\lambda_1](\alpha_1+\{n,p_1\})} \cdot p_2^{[n:\lambda_2](\alpha_2+\{n,p_2\})} \cdot p_3^{[n:\lambda_3](\alpha_3+\{n,p_3\})} \cdot \ldots$

Here only odd primefactors p_k need be considered.

In *(3)* the exponents are expressed in a problem specific notation which mean:

[m:p] "Divisibility" of m by p (like Iverson-brackets)
$[m:p] = 1$ if p divides m, else 0

{m,p}:= the exponent, to which the prime p occurs as factor of m
$\{m,p\} = \alpha$ => $m=p^\alpha \cdot x$ where $gcd(x,p)=1$

λ:= the "order of the multiplicative cyclic subgroup modulo p"
λ is the smallest $k>0$ such that the equation $[2^k-1:p] = 1$ holds

α:= the exponent to which p occurs first in $2^k - 1$ where $k=1,2,3,...$
$\{2^\lambda-1,p\} = \alpha$
α is 1 in most cases of p_k but $\alpha=2$ for $p=1093$ and $p=3511$
which are the two known "wieferich primes"

Note, that λ and α are constants for a given p and independent of n in formula (3)

Formula (2b) becomes then

$$2^n+1 = \frac{2^{2n}-1}{2^n-1} = \frac{p_1^{[2n:\lambda_1](\alpha_1+\{2n,p_1\})} \cdot p_2^{[2n:\lambda_2](\alpha_2+\{2n,p_2\})} \cdot p_3^{[2n:\lambda_3](\alpha_3+\{2n,p_3\})} \cdot \ldots}{p_1^{[n:\lambda_1](\alpha_1+\{n,p_1\})} \cdot p_2^{[n:\lambda_2](\alpha_2+\{n,p_2\})} \cdot p_3^{[n:\lambda_3](\alpha_3+\{n,p_3\})} \cdot \ldots}$$

which is also

(4)
$$2^n+1 = p_1^{[2n:\lambda_1](\alpha_1+\{2n,p_1\})-[n:\lambda_1](\alpha_1+\{n,p_1\})} \cdot p_2^{[2n:\lambda_2](\alpha_2+\{2n,p_2\})-[n:\lambda_2](\alpha_2+\{n,p_2\})} \cdot p_3^{[2n:\lambda_3](\alpha_3+\{2n,p_3\})-[n:\lambda_3](\alpha_3+\{n,p_3\})} \cdot \ldots$$

[1] http://math.stackexchange.com/questions/97229/how-many-rationals-of-the-form-large-frac2n1n2-are-integers

2. Assume only one primefactor in *n*

First we try, whether n can be an odd prime or a power of an odd prime. We find, using $n = p^a$, according to *(4)* the following, most general expression for the primefactorization:

$$\begin{aligned} 2^{p^a}+1 &= p_1^{[2p^a:\lambda_1](\alpha_1+\{2p^a,p_1\})-[p^a:\lambda_1](\alpha_1+\{p^a,p_1\})} \\ &\quad\cdot p_2^{[2p^a:\lambda_2](\alpha_2+\{2p^a,p_2\})-[p^a:\lambda_2](\alpha_2+\{p^a,p_2\})} \\ &\quad\cdot p_3^{[2p^a:\lambda_3](\alpha_3+\{2p^a,p_3\})-[p^a:\lambda_3](\alpha_3+\{p^a,p_3\})} \\ &\quad\cdot \ldots \end{aligned} \tag{5a}$$

First we rewrite it, where we only leave $p_k = p$ explicite and subsume all other primefactors in an (uninteresting) indeterminate x:

$$2^{p^a}+1 = p^{[2p^a:\lambda](\alpha+\{2p^a,p\})-[p^a:\lambda](\alpha+\{p^a,p\})} \cdot x \tag{5b}$$

Next this can be simplified because $\{2p^a,p_k\}=\{p^a,p_k\}$ if p and p_k are odd primes:

$$2^{p^a}+1 = p^{([2p^a:\lambda]-[p^a:\lambda])(\alpha+\{p^a,p\})} \cdot x \tag{5c}$$

and also, since $\{p^a,p\}=a$

$$2^{p^a}+1 = p^{([2p^a:\lambda]-[p^a:\lambda])(\alpha+a)} \cdot x \tag{5d}$$

Because our question (2a) with $n=p^a$ has this form

$$2^{p^a}+1=(p^a)^2 x = p^{2a} x \tag{5e}$$

we can equate the exponents and consider now the conditions where

(6) $2a \le ([2p^a : \lambda] - [p^a : \lambda])(\alpha + a)$

By Fermat's little theorem we know that λ must be smaller than p so $\lambda \le p-1$ and after Euler's totient-theorem it must equal or be a divisor of $\varphi(p)=p-1$.

On the other hand, to have $[2p^a : \lambda] - [p^a : \lambda] = 1$ the first bracket must evaluate to 1 and the second to 0, so λ must be even, since p (and so p^a) is odd. Moreover, since a number $1<\lambda<p$ cannot be a divisor of p if p is prime, so

(7a) $\lambda = 2$

From the definitions we have $2^\lambda-1=p^\alpha \cdot x$ so we know the following:

(7b) $2^\lambda-1 = 3 \quad ==> \quad p=3$
$\alpha = \{2^\lambda-1,p\}= \{3,3\} = 1 \quad ==> \quad \alpha=1$
$n = 3^a$ *(where a is still unknown)*

We get thus from $2a \le ([2p^a:2]-[p^a:2])(\alpha+\{p^a,p\})$ the solution for a

$$2a \le ([2 \cdot 3^a :2]-[3^a :2])(1+\{3^a ,3\}) = (1-0)(1+a) = 1+a$$

$==>$

(7c) $a = 1$

and finally for n

if $2^n + 1 = n^2 \cdot x$
(8) $n = p^a = 3^1 = 3$
and $2^3+1 = \cdot 3^2$

a single solution if we assume n as a'th power of a single odd prime.

3. Assume two primefactors in n

Next we check whether n can be a product of two primes/primepowers. We try $n=p^a\cdot q^b$ where we assume $p<q$

The equation *(5a)* above changes to

$$(9)\qquad \begin{aligned} 2^{p^a q^b}+1 &= p^{([2n:\lambda_p]-[n:\lambda_p])(\alpha_p+\{p^a q^b,p\})}\cdot q^{([2n:\lambda_q]-[n:\lambda_q])(\alpha_q+\{p^a q^b,q\})}\cdot x \\ &\overset{??}{=} n^2\cdot x = p^{2a}q^{2b}\cdot x \end{aligned}$$

and by comparision of exponents (and simplification):

$$(10a)\qquad 2a \le ([2p^a q^b:\lambda_p]-[p^a q^b:\lambda_p])(\alpha_p+a)$$

$$(10b)\qquad 2b \le ([2p^a q^b:\lambda_q]-[p^a q^b:\lambda_q])(\alpha_q+b)$$

We look at *(10a)*. Because $p<q$ it is also $\lambda_p<q$ and thus is neither a factor of p nor of q so must be $\lambda_p=2$ again and also immediately $p = 3$ again. Moreover, because in *(10a)* there is no relevant modification over *(6)* we get also that $a=1$, thus $n=3^1q^b$.

We insert this in *(10b)*:

$$(10c)\qquad 2b \le ([2\cdot 3\cdot q^b:\lambda_q]-[3\cdot q^b:\lambda_q])(\alpha_q+b)$$

We look now at *(10c)* Because λ_q cannot divide q or q^b we have that λ_q must be a divisor of 6 but not of 3; on the other hand we know that $2^{\lambda_q}-1=2^6-1$ does not contain any other primefactor besides 3 and 7. q cannot be 3, because $q>p=3$ by our definition; and if $q=7$ then $\lambda_q=3$ and $\alpha_q=1$. Then we have

$$(11)\qquad \begin{aligned} 2b &\le ([2\cdot 3\cdot 7^b:3]-[3\cdot 7^b:3])(1+b) \\ &= (1-1)(1+b) \\ &= 0 \\ \Rightarrow\quad b &= 0 \end{aligned}$$

So, if we assume n had two different primefactors, we get, that the second primefactor $q=7$ occurs to the zero^th power; thus again we get as the only solution:

$$2^n+1=x\cdot n^2$$
$$\Rightarrow\quad n=3^1\cdot 7^0=3$$

4. Assume more primefactors in n

That assumtion leads to a very similar conclusion as before. Let $r>q$ the new primefactor and its exponent c. Then the equations *(10a)* and *(10c)* become:

$$(12a)\qquad 2a \le ([2\cdot p^a\cdot q^b\cdot r^c:\lambda_p]-[p^a\cdot q^b\cdot r^c:\lambda_q])(\alpha_p+a)$$

Again λ_p must be even and cannot divide p,q,r so it must $\lambda_p=2$ and we know, that then uniquely $p=3$, and thus $\alpha_p=1$ and $a=1$

$$(12b)\qquad 2b \le ([2\cdot 3\cdot q^b\cdot r^c:\lambda_q]-[3\cdot q^b\cdot r^c:\lambda_q])(\alpha_q+b)$$

Also λ_q must be even and because $q<r$ and q and r are prime, λ_q cannot divide q or r and it must $\lambda_q=6$ But there is no primefactor q with $\lambda_q=6$.

Thus no additional solution for more primefactors in n is possible.

Appendix: A solution by G. Woeginger, Internation Math Olympiad (IMO) 1990[2]

The following is a (slightly reformatted) full citation of a relevant internet-page, see footnote 2

Problem 3: Determine all integers greater than 1 such that $(2^n + 1)/n^2$ is an integer.

Solution *by Gerhard Wöginger, Technical University, Graz*

Answer: $n = 3$.

Since $2^n + 1$ is odd, n must also be odd.
Let p be its smallest prime divisor.
Let x be the smallest positive integer such that $2^x = -1 \ (mod\ p)$, and let y be the smallest positive integer such that $2^y = 1 \ (mod\ p)$. y certainly exists and indeed $y < p$, since $2^{p-1} = 1 \ (mod\ p)$. x exists since $2^n = -1 \ (mod\ p)$.
Write $n = ys + r$, with $0 <= r < y$. Then $- 1 = 2^n = (2^y)^s 2^r = 2^r \ (mod\ p)$, so $x <= r < y$ (r cannot be 0, since $- 1$ is not $1 \ (mod\ p)$).
Now write $n = hx + k$, with $0 <= k < x$. Then $-1 = 2^n = (-1)^h 2^k \ (mod\ p)$. Suppose $k > 0$. Then if h is odd we contradict the minimality of y, and if h is even we contradict the minimality of x. So $k = 0$ and x divides n. But $x < p$ and p is the smallest prime dividing n, so $x = 1$. Hence $2 = -1 \ (mod\ p)$ and so $p = 3$.
Now suppose that 3^m is the largest power of 3 dividing n. We show that m must be 1. Expand $(3 - 1)^n + 1$ by the binomial theorem, to get (since n is odd): $1 - 1 + n.3 - 1/2\ n(n - 1)\ 3^2 + ... = 3n - (n - 1)/2\ n\ 3^2 + ...$. Evidently $3n$ is divisible by 3^{m+1}, but not 3^{m+2}. We show that the remaining terms are all divisible by 3^{m+2}. It follows that 3^{m+1} is the highest power 3 dividing $2^n + 1$. But $2^n + 1$ is divisible by n^2 and hence by 3^{2m}, so m must be 1.

The general term is $(3^m a)Cb\ 3^b$, for $b >= 3$. The binomial coefficients are integral, so the term is certainly divisible by 3^{m+2} for $b >= m+2$. We may write the binomial coefficient as $(3^m a/b)\ (3^m - 1)/1\ (3^m - 2)/2\ (3^m - 3)/3\ ...\ (3^m - (b-1))\ /\ (b - 1)$. For b not a multiple of 3, the first term has the form $3^m\ c/d$, where 3 does not divide c or d, and the remaining terms have the form c/d, where 3 does not divide c or d. So if b is not a multiple of 3, then the binomial coefficient is divisible by 3^m, since $b > 3$, this means that the whole term is divisible by at least 3^{m+3}. Similarly, for b a multiple of 3, the whole term has the same maximum power of 3 dividing it as $3^m\ 3^b/b$. But b is at least 3, so $3^b/b$ is divisible by at least 9, and hence the whole term is divisible by at least 3^{m+2}.

We may check that $n = 3$ is a solution. If $n > 3$, let $n = 3\ t$ and let q be the smallest prime divisor of t. Let w be the smallest positive integer for which $2^w = -1 \ (mod\ q)$, and v the smallest positive integer for which $2^v = 1 \ (mod\ q)$. v certainly exists and $< q$ since $2^{q-1} = 1 \ (mod\ q)$. $2^n = -1 \ (mod\ q)$, so w exists and, as before, $w < v$.
Also as before, we conclude that w divides n.
But $w < q$, the smallest prime divisor of n, except 3. So $w = 1$ or 3. These do not work, because then $2 = -1 \ (mod\ q)$ and so $q = 3$, or $2^3 = -1 \ (mod\ q)$ and again $q = 3$, whereas we know that $q > 3$.

The solutions given on this site are not always complete, they are designed to be sufficient for anyone who has thought hard about the problem.

31st IMO 1990
(C) John Scholes
jscholes@kalva.demon.co.uk
7 Sep 1999

[2] http://www.cs.cornell.edu/~asdas/imo/imo/isoln/isoln903.html