

## 0.1 Minimum prime divisors

1 A14 Let  $n > 1$  be an integer. Show that  $n$  does not divide  
PEN A14  
A71

$$2^n - 1 \tag{1}$$

A71 Determine all integers  $n > 1$  such that

$$\frac{2^n + 1}{n^2} \tag{2}$$

is an integer.

First we will introduce some definitions and we will provide the proof of an elementary fact. Let  $d$  be the least natural number that satisfies

$$a^d \equiv 1 \pmod{p} \tag{3}$$

Then we write

$$\text{ord}_p a = d \tag{4}$$

Lemma 1:

$$a^k \equiv 1 \pmod{p} \tag{5}$$

if and only if

$$k \equiv 0 \pmod{\text{ord}_p a} \tag{6}$$

Proof:

Suppose

$$\text{ord}_p a = d \tag{7}$$

Let  $k = dt + r$ ,  $d > r \geq 0$  (which is valid by the division algorithm)

So we get that

$$2^{dt+r} \equiv 1 \pmod{p} \tag{8}$$

Since  $2^d \equiv 1 \pmod{p}$ ,  $2^{dt} \equiv 1 \pmod{p}$  then

$$2^r \equiv 1 \pmod{p} \tag{9}$$

but

$$d > r \tag{10}$$

If  $r = 0$  the claim follows and if  $r > 0$  we are contradicting the minimality of  $d$ , absurd.

If

$$k \equiv 0 \pmod{d} \tag{11}$$

is trivial to see that it works.

It is worthy to stop here and analyze the importance of the definition we have just introduced. It not only uses elementary number theory but also relies on a very powerful principle that states that every set of natural numbers has an element which is less than the others. Clearly the idea

of a least-element allows us to find contradictions about minimality after supposing a number satisfies a given condition and is the smallest of the sort. This is a key concept in mathematics; especially in number theory.

Now we are ready to begin our proof of A14:

Since  $n > 1$ ,  $n$  has a prime divisor, then we can choose it so that it is minimal. Clearly if  $n$  is even we get that  $2^n - 1$  is odd. And even cannot divide and odd number so  $n$  is odd. Let  $p$  be the minimal prime that divides  $n$  ( $p > 2$ ) We can write  $n = pk$

$$2^{pk} \equiv 1 \pmod{p} \tag{12}$$

Because  $2^p \equiv 2 \pmod{p}$  by Fermats little theorem, we get that

$$2^k \equiv 1 \pmod{p} \tag{13}$$

Let

$$d = \text{ord}_p 2 \tag{14}$$

So  $k = dt$  for some integer  $t$

Clearly  $d > 1$

Since  $2^{p-1} \equiv 1 \pmod{p}$  by Fermat little theorem , we obtain

$$p - 1 \equiv 0 \pmod{d} \tag{15}$$

so

$$p > p - 1 > d \tag{16}$$

We obtain that  $d$  is a divisor of  $k$ ,and it follows it is also a divisor of  $n$ . Because  $p > d$ , we are contradicting the minimality of  $p$ . Absurd.

Thus the statment is proved and we conclude that there are no solutions for  $n > 1$

A71 Clearly  $n$  is odd Again we define  $p$  as the least prime divisor of  $n$  We have that

$$2^n \equiv -1 \pmod{p} \tag{17}$$

squaring both sides

$$2^{2n} \equiv 1 \pmod{p} \tag{18}$$

Again we put  $n = pk$  and we have, reasoning in the same way as the previous problem, that

$$2^{2k} \equiv 1 \pmod{p} \tag{19}$$

Let

$$d = \text{ord}_p 2 \tag{20}$$

Then  $2k \equiv 0 \pmod{d}$  and  $p - 1 \equiv 0 \pmod{d}$  If  $\text{gcd}(k, d) > 1$  , as exposed before,  $d$  divides  $n$  and is smaller than  $p$ . So the only possibility is that  $d$  divides 2

$d = 1$  is not possible

$d = 2$  we have that

$$2^2 \equiv 1 \pmod{p} \quad (21)$$

So

$$p = 3 \quad (22)$$

Hensel Lemma (Lifting the exponent): Let  $p$  be an odd prime. Suppose that  $a \equiv b \pmod{p}$  Lets define  $X$  as the maximum exponent of  $p$  dividing  $a - b$  and  $Y$  the maximum exponent of  $p$  dividing the positive number  $m$ . Then

$$X + Y \quad (23)$$

is the maximum exponent of  $p$  dividing

$$a^m - b^m \quad (24)$$

Now,back to the problem let  $X$  be the exponent of 3 in  $n$  Since  $n^2$  divides  $2^{2^n} - 1$  Then we get:  $2X$  is the exponent of 3 in  $n^2$  Since the exponent of 3 in  $2^2 - 1$  is 1 we have that the exponent of 3 in  $2^{2^n} - 1$  is  $X + 1$  So we must have

$$X + 1 \geq 2X \quad (25)$$

implying

$$X = 1 \quad (26)$$

Then we may write  $n = 3t$  with  $\gcd(3, t) = 1$

Now we will continue with our reasoning, as shown before. Let  $q$  be the least prime divisor of  $t$

$$t = ql \quad (27)$$

Again we get that

$$2^{6l} \equiv 1 \pmod{q} \quad (28)$$

Then if

$$c = \text{ord}_q 2 \quad (29)$$

Easily we conclude that  $c$  divides  $6l$  and if  $\gcd(l, c) > 1$  we will get a similar contradiction as in previous lines.

So  $c$  divides 6

The cases  $c = 1$  and  $c = 2$  lead to  $q = 1$  implying  $n = 3$  which works and  $q = 3$  which does not make any sense.

If  $d = 3$  or  $d = 6$  replacing in

$$2^d \equiv 1 \pmod{p} \quad (30)$$

we get 7 as the desired prime We must have

$$2^n \equiv -1 \pmod{7} \quad (31)$$

It is easy to check that  $2^1 \equiv 2 \pmod{7}$   $2^2 \equiv 4 \pmod{7}$   $2^3 \equiv 1 \pmod{7}$  But  $2^{k+3} \equiv 2^3 2^k \equiv 2^k \pmod{7}$  So for all  $k$ ,  $2^k \not\equiv -1 \pmod{7}$  As a corollary the only possibility is that  $n = 3$  which indeed satisfies the equation. The proof is finished.

## REFERENCES

1 *PEN Problem A14*, <http://www.mathlinks.ro/Forum/viewtopic.php?t=150382>

2 *PEN Problem A71*, <http://www.mathlinks.ro/Forum/viewtopic.php?t=150439>