NNTDM 11 (2005) 1, 1-6

ON FOUR SMARANDACHE'S PROBLEMS

Krassimir T. Atanassov

CLBME - Bulg. Academy of Sci., and MRL, P.O.Box 12, Sofia-1113, Bulgaria
e-mail: krat@bgcict.acad.bg

In [1] F. Smarandache formulates the following four problems:
Problem 1. *Let p be an integer ≥ 3. Then:*

p is prime if and only if

$$(p-3)! \text{ is congruent to } \frac{p-1}{2} (\text{mod } p). \tag{1}$$

Problem 2. *Let p be an integer ≥ 4. Then:*

p is prime if and only if

$$(p-4)! \text{ is congruent to } (-1)^{\lfloor \frac{p}{3} \rfloor + 1} \lfloor \frac{p+1}{6} \rfloor (\text{mod } p). \tag{2}$$

Problem 3. *Let p be an integer ≥ 5. Then:*

p is prime if and only if

$$(p-5)! \text{ is congruent to } rh + \frac{r^2-1}{24} (\text{mod } p), \tag{3}$$

with $h = \lfloor \frac{p}{24} \rfloor$ and $r = p - 24h$.

Problem 4. *Let $p = (k-1)!h + 1$ be a positive integer $k > 5$, h natural number. Then:*

p is prime if and only if

$$(p-k)! \text{ is congruent to } (-1)^t h (\text{mod } p), \tag{4}$$

with $t = h + \lfloor \frac{p}{h} \rfloor + 1$.

Everywhere above $\lfloor x \rfloor$ means the inferior integer part of x, i.e., the smallest integer greater than or equal to x.

Here we shall discuss these four problems.

Problem 1. admits the following representation:
Let $p \geq 3$ be an odd number. Then:

$$p \text{ is prime if and only if } (p-3)! \equiv \frac{p-1}{2} (\text{mod } p). \tag{1'}$$

First, we assume that p is a composite number. Therefore, $p \geq 9$. For p there are two possibilities:

(a) $p = \prod_{i=1}^{s} p_i^{a_i}$, where p_i are different prime numbers and $a_i \geq 1$ are natural numbers $(1 \leq i \leq s)$;
(b) $p = q^k$, where q is a prime number and $k \geq 2$ is a natural number.

Let (a) hold. Then there exist odd numbers a and b such that

$$2 < a < b < \frac{p}{2};\ (a,b) = 1;\ a.b = p.$$

The case when $a = 2$ and $b = \frac{p}{2}$ is impossible, because p is an odd number. Hence a and b are two different multipliers of $(p-3)!$ because $\frac{p}{2} < p-3$. Therefore, the number $a.b = p$ divides $(p-3)!$, i.e.,

$$(p-3)! \equiv 0 (\text{mod } p).$$

Hence in case (a) the congruence in the right hand-side of (1') is impossible.

Let (b) hold. Then $q \geq 3$ and we have to consider only two different cases:
(b_1) $k \geq 3$;
(b_2) $k = 2$.

Let (b_1) hold. Then

$$3 \leq q < q^{k-1} < q^k - 3 = p - 3.$$

Hence q and q^{k-1} are two different multipliers of $(p-3)!$. Therefore, the number $q.q^{k-1} = q^k = p$ divides $(p-3)!$, i.e.,

$$(p-3)! \equiv 0 (\text{mod } p).$$

Hence in case (b_1) the congruence in the right hand-side of (1') is impossible.

Let (b_2) hold. Then

$$p - 3 = q^2 - 3 \geq 2q.$$

Hence q and $2q$ are two different multipliers of $(p-3)!$. Therefore, the number $q^2 = p$ divides $(p-3)!$, i.e.,

$$(p-3)! \equiv 0 (\text{mod } p).$$

Hence in case (b_2) the congruence in the right hand-side of (1') is also impossible.

Thus we conclude that if $p > 1$ is an odd composite number, then the congruence

$$(p-3)! \equiv \frac{p-1}{2} (\text{mod } p)$$

is impossible.

Let $p \geq 3$ be prime. In this case we shall prove the above congruence using the well-known Wilson's Theorem (see, e.g. [2]):

$$p \text{ is prime if and only if } (p-1)! \equiv -1(\text{mod } p). \tag{5}$$

If we rewrite the congruence from (5) in the form

$$(p-1)(p-2)(p-3)! \equiv p-1(\text{mod } p)$$

and using that

$$(p-2) \equiv -2(\text{mod } p)$$

and

$$(p-1) \equiv -1(\text{mod } p)$$

we obtain

$$2(p-3)! \equiv p-1(\text{mod } p).$$

Hence the congruence

$$(p-3)! \equiv \frac{p-1}{2}(\text{mod } p)$$

is proved, i.e., Problem 1 is solved.

Problem 2. is false, because, for example, if $p = 7$, then (2) obtains the form

$$6 \equiv (-1)^4 2(\text{mod } 7),$$

where

$$6 = (7-4)!$$

and

$$(-1)^4 2 = (-1)^{\lfloor \frac{7}{3} \rfloor + 1} \lfloor \frac{8}{6} \rfloor,$$

i.e.,

$$6 \equiv 2(\text{mod } 7),$$

which is impossible.

Problem 3. can be modified, having in mind that from $r = p - 24h$ it follows:

$$rh + \frac{r^2-1}{24} = (p-24h).h + \frac{p^2 - 48ph + 24^2h^2 - 1}{24}$$

$$= ph - 24h^2 + \frac{p^2-1}{24} - 2ph + 24h^2 = \frac{p^2-1}{24} - ph,$$

i.e., (3) has the form

p is prime if and only if

$$(p-5)! \text{ is congruent to } \frac{p^2-1}{24}(\text{mod } p), \tag{3'}$$

Let $p \geq 5$ be prime. It is easy to see that $\frac{p^2-1}{24}$ is an integer (because every prime number p has one of the two forms $6k+1$ or $6k+5$ for some natural number k).

From Wilson's Theorem (see, e.g. [2]) and from

$$p^2 \equiv 0(\text{mod } p)$$

we may write

$$(p-5)!.(p-4).(p-3).(p-2).(p-1) \equiv p^2 - 1(\text{mod } p).$$

Since

$$(p-i) \equiv -i(\text{mod } p),$$

for $i = 1, 2, 3, 4$, we finally obtain

$$24(p-5)! \equiv p^2 - 1(\text{mod } p).$$

Hence, the congruence

$$(p-5)! \equiv \frac{p^2-1}{24}(\text{mod } p)$$

is proved.

When p is a composite number and the number $\frac{p^2-1}{24}$ is not integer, the congruence

$$(p-5)! \equiv \frac{p^2-1}{24}(\text{mod } p)$$

is impossible. That is why we consider below only the composite odd numbers $p \geq 5$ for which $\frac{p^2-1}{24}$ is an integer.

Like in the proof of Problem 1, for p we have only the two possibilities (a) and (b).

Let (a) hold. Then $p \geq 15$ and there exist odd numbers a and b such that

$$2 < a < b < \frac{p}{2};\ (a,b) = 1;\ a.b = p.$$

Hence a and b are two different multipliers of $(p-5)!$ since $\frac{p}{2} < p-5$. Therefore, the number $a.b = p$ divides $(p-5)!$, i.e.,

$$(p-5)! \equiv 0(\text{mod } p).$$

If we suppose that the congruence from (3') holds too, then we obtain that

$$\frac{p^2-1}{24} \equiv 0(\text{mod } p),$$

i.e.,

$$p^2 - 1 \equiv 0(\text{mod } p),$$

i.e.,

$$-1 \equiv 0(\text{mod } p),$$

which is impossible. Therefore, the congruence in the right hand-side of (3') is impossible.

Let (b) hold. As in the proof of Problem 1, here we have to consider two different cases (b_1) and (b_2).

Let (b_1) hold. Then

$$3 \leq q < q^{k-1} < q^k - 5 = p - 5.$$

Hence q and q^{k-1} are two different multipliers of $(p-5)!$. Therefore, the number $q.q^{k-1} = q^k = p$ divides $(p-5)!$, i.e.,

$$(p-5)! \equiv 0(\text{mod } p).$$

Therefore, just as in the case (a) we conclude that the congruence in the right hand-side of (3') is impossible.

Let (b_2) hold. If $q \geq 7$, then we have

$$p - 5 = q^2 - 5 \geq 2q.$$

Hence q and $2q$ are two different multipliers of $(p-5)!$. Hence, the number $q^2 = p$ divides $(p-5)!$, i.e.,

$$(p-5)! \equiv 0(\text{mod } p).$$

Just as in case (a) we conclude that the congruence in the right hand-side of (3') is impossible.

It remains only to consider the cases:

$$p = 3^2 = 9, \ p = 5^2 = 25$$

and to finish with (b_2).

If $p = 9$, then $\dfrac{p^2-1}{24}$ is not an integer and as we noted before, the congruence in the right hand of (3') fails.

When $p = 25$ the above congruence yields

$$20! \equiv 26(\text{mod } 25),$$

i.e.,

$$20! \equiv 1(\text{mod } 25).$$

On the other hand, 25 divides 20! and therefore,

$$20! \equiv 0(\text{mod } 25).$$

Hence, the congruence in the right hand of (3') is impossible in the case $p = 25$, too.

Thus the same congruence is impossible for the case (b).

Finally we proved

If $p > 1$ is an odd composite number, then the congruence

$$(p-5)! \equiv \frac{p^2-1}{24}(\text{mod } p)$$

is impossible and Problem 3 is completely solved.

Problem 4. also can be simplified, because

$$t = h + \lfloor \frac{p}{h} \rfloor + 1$$

$$= h + \lfloor \frac{(k-1)!h+1}{h} \rfloor + 1$$

$$= h + (k-1)! + 1 + 1 = h + (k-1)! + 2,$$

i.e.,

$$(-1)^t = (-1)^h,$$

because for $k > 2 : (k-1)! + 2$ is an even number. Therefore, (4) obtains the form

$$p \textit{ is prime if and only if}$$

$$(p-k)! \textit{ is congruent to } (-1)^h h (\text{mod } p). \tag{4'}$$

Let us assume that (4') is valid. We use again the congruences

$$(p-1) \equiv -1 (\text{mod } p)$$

$$(p-2) \equiv -2 (\text{mod } p)$$

$$\cdot \quad \cdot \quad \cdot$$

$$(p-(k-1)) \equiv -(k-1) (\text{mod } p)$$

and obtain the next form of (4')

$$p \textit{ is prime if and only if}$$

$$(p-1)! \equiv (-1)^h.(-1)^{k-1}.(k-1)!.h (\text{mod } p)$$

or

$$p \textit{ is prime if and only if}$$

$$(p-1)! \equiv (-1)^{h+k-1}.(p-1) (\text{mod } p).$$

But the last congruence is not valid, because, e.g., for $k = 5, h = 3, p = 73 = (5-1)!3!+1$ holds

$$72! \equiv (-1)^9.72 (\text{mod } 73),$$

i.e.,

$$72! \equiv 1 (\text{mod } 73),$$

while from Wilson's Theorem it follows that

$$72! \equiv -1 (\text{mod } 73).$$

REFERENCES:

[1] F. Smarandache, Collected Papers, Vol. 1, Ed. Tempus, Bucharest, 1996, 94-98.

[2] T. Nagell, Introduction to Number Theory. John Wiley & Sons, Inc., New York, 1950.