MA 1301/6301 TALLTEORI Peter Lindqvist

SOLUTIONS TO EXAM. 3.XII.2008

① $496 = 1\cdot 2\cdot 2\cdot 2\cdot 2\cdot 31$ The sum of the proper divisors is

$$1+2+4+8+16+31+62+124+248 = 496,$$

as it should. (One can also use Euclid's theorem about perfect numbers.)

---

② We have the factors

$$2 \mid 1001!+2,\quad 3\mid 1001!+3,\quad 4\mid 1001!+4,\ \ldots,\ 1001\mid 1001!+1001$$

and hence none of the numbers is a prime.

---

③ ASSUMPTION $3^{2009} \equiv 3 \pmod{m}$

CLAIM $3^{n\cdot 2008+1} \equiv 3 \pmod{m}$, when

$n = 1, 2, 3, \ldots$

<u>Proof by Induction:</u>

i) <u>$n=1$</u> This is the assumption above.

ii) <u>$n=k$</u> Induction hypothesis $3^{k\cdot 2008+1} \equiv 3$

iii) <u>$n=k+1$</u> $3^{(k+1)2008+1} = 3^{k\cdot 2008+1}\cdot 3^{2008}$

$$\underset{\text{ii}}{\equiv} 3\cdot 3^{2008} = 3^{2009} \underset{\text{i}}{\equiv} 3$$

<u>Comment:</u> It may happen that $3^{2008} \not\equiv 1 \pmod{m}$. For example, $m=3$.

(4) $[5;\overline{10}] = [5;10,10,\dots]$

$$x = 10 + \cfrac{1}{10+\cfrac{1}{10+\dots}} = 10 + \frac{1}{x},$$

$$x^2 - 10x - 1 = 0, \quad x = 5 \pm \sqrt{26} = 5 + \sqrt{26}$$
(since $x > 0$)

$$\frac{1}{x} = x - 10 = \sqrt{26} - 5. \quad \text{Hence } \underline{[5;\overline{10}] = \sqrt{26}}$$

0	1	2	3
5	10	10	10
$\frac{5}{1}$	$\frac{51}{10}$	$\frac{515}{101}$	$\frac{5201}{1020}$

Period length $m = 1$ (odd)

Hence
$$\begin{cases} x = p_{2m-1} = p_1 = 51 \\ y = q_{2m-1} = q_1 = 10 \end{cases}$$
solves Pell's equation.
(There are infinitely many of them.)

Pell's eqn. $\boxed{x^2 - 26y^2 = 1}$

$$51^2 - 26 \cdot 10^2 = 1$$

---

(5) $x^{173} \equiv 291 \pmod{323}, \quad x = ?$

$$\varphi(323) = \varphi(17)\varphi(19) = 16 \cdot 18 = 288$$

First we solve the eqn

$$173e \equiv 1 \pmod{\underline{288}}.$$

Euclid's algorithm yields $e = 5$. Then

$$x \equiv 291^5 \equiv 100 \pmod{323}.$$

(6) $x^2 \equiv -1 \pmod{2038}$. Is this possible?

$2038 = 2 \cdot 1019$, $\varphi(2038) = 1018$ (we know that 1019 is a prime number). Modulo 2038,

$$1 \equiv x^{\varphi(n)} = x^{1018} = (x^2)^{509} \quad \text{Euler – Fermat}$$

holds for each x, $\gcd(x, 2038) = 1$.

<u>If</u> $x^2 \equiv -1 \pmod{2038}$, then $\gcd(x, 2038) = 1$ ($x^2+1 = k \cdot 2038$ for some integer), and

$$1 \equiv (-1)^{509} = -1,$$

but $1 \not\equiv -1$. This is a contradiction. It follows that the equation $x^2 \equiv -1$ does not have a solution.

<u>Comment</u>: One can reduce the problem to the fact that 1019 is a prime of the type
$$p = 4k+3.$$