Peter Lindqvist

MA 1301 TALLTEORI

30. XI. 2007 SOLUTIONS

---

① Assume that

$$7m^3 = n^3, \quad \gcd(m,n) = 1$$

(Common factors are divided out in advance.) Now

$$7 \mid n^3 \Rightarrow 7 \mid n \quad \text{by Euclid's lemma}$$

Hence $n = 7\nu$ and $7m^3 = 7 \cdot 49\nu^3$. Thus

$$m^3 = 7 \cdot 7\nu^3$$

It follows that $7 \mid m^3$ and, again, $7 \mid m$. But then both m and n have the factor 7, so that $\gcd(m,n) \geq 7$, a contradiction. We have proved that $\sqrt[3]{7}$ is not a rational number.

---

③ $n = 57482 = 2pq$ (Notice "2".)

$$\phi(n) = 28000 = n\left(1-\frac{1}{2}\right)\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)$$

$$= (p-1)(q-1)$$

$$28000 = pq - (p+q) + 1 = 28741 - (p+q) + 1$$

$$\begin{cases} p+q = 742 \\ pq = 28741 \end{cases}$$

Now <u>p and q are the roots of the quadratic equation</u>

$$(X-p)(X-q) = 0$$

$$X^2 - (p+q)X + pq = 0$$

$$X^2 - 742X + 28741 = 0 \quad *)$$

*) The roots are

$$\begin{cases} p = \underline{41} \\ q = \underline{701} \end{cases}$$

(2) $\begin{cases} x \equiv 1 \pmod 5 \\ x \equiv 2 \pmod 6 \\ x \equiv 3 \pmod 7 \end{cases}$ $M = 5\cdot 6\cdot 7 = 210$

According to the Chinese Remainder Theorem the solution is unique modulo 210. The auxiliary system of equations is

$$\begin{cases} 42x_1 \equiv 1 \pmod 5, & x_1 = 3 \\ 35x_2 \equiv 1 \pmod 6, & x_2 = -1 \\ \underline{30x_3 \equiv 1} \pmod 7, & x_3 = 4 \end{cases}$$

For example, $\underline{30x_3 \equiv 1} \pmod 7 \iff 2x_3 \equiv 1 \pmod 7$ $\iff 8x_3 \equiv 4 \pmod 7 \iff x_3 \equiv 4 \pmod 7$. – The solution is

$$x = 1\cdot 42\cdot 3 + 2\cdot 35(-1) + 3\cdot 30\cdot 4 = 416$$
$$\equiv 206 \pmod{210}$$

Answer $x \equiv 206 \pmod{210}$ or $206 + 210\cdot n$

---

(4) $(p-1)! \equiv -1 \pmod p$ Wilson's Theorem

$p = 101$ is a prime number.

(1°) $\underline{100!} \underline{\equiv -1} \pmod{101}$.

(2°) $100! \equiv -1$, $100\cdot 99! \equiv -1$, $-1\cdot 99! \equiv -1$

since $100 \equiv -1$. Thus $\underline{99! \equiv 1}$.

(3°) $99\cdot 98! \equiv 1$, $(-2)\cdot 98! \equiv 1$, $-100\cdot 98! \equiv 50$,

$\underline{98! \equiv 50}$. $(99 \equiv -2,\ -100 \equiv 1)$

2

(5) Assume that $a^2 \equiv -1 \pmod{p}$.

$$\underbrace{+1 \equiv a^{p-1}}_{\text{FERMAT's theorem}} \;\underset{\substack{\uparrow\\ \frac{p-1}{2} \text{ is an integer}}}{=}\; (a^2)^{\frac{p-1}{2}} \;\underset{\substack{\uparrow\\ \text{Assumption}}}{\equiv}\; (-1)^{\frac{p-1}{2}}$$

If $p = 4k+3$, $\frac{p-1}{2} = 2k+1$, and

$$+1 \equiv (-1)^{2k+1} = -1 \quad ↯$$

This is a contradiction. Hence $p = 4k+1$.

---

(6) $$\sqrt{D} = 6 + \cfrac{1}{12 + \cfrac{1}{12 + \cfrac{1}{12 + \cdots}}} = [6; \overline{12}]$$

Period of length $m = 1$. $\quad (2m-1 = 2\cdot 1 - 1 = 1)$

n	0	1	2	3
a_n	6	12	12	12
$\frac{p_n}{q_n}$	$\frac{6}{1}$	$\frac{73}{12}$		

$$x^2 - Dy^2 = 1$$

The fundamental solution is $x = p_1 = 73$, $y = q_1 = 12$ so that

$$73^2 - D \cdot 12^2 = 1$$

We can find $D = 37$ from this. A second solution

One may also calculate $\sqrt{D}$ directly by first solving

$$z = 12 + \cfrac{1}{12 + \cfrac{1}{\ddots}} = 12 + \frac{1}{z}$$

continues

comes from

$$x_2 + \sqrt{37}\, y_2 = (73 + \sqrt{37}\cdot 12)^2$$

$$= 10657 + 1752\sqrt{37}$$

Thus

$$x_2 = 10657, \quad y_2 = 1752$$

---

(7) $x^{65} \equiv 210 \pmod{299} \iff 210^{d} \equiv x \pmod{299}$

provided that $65 \cdot d \equiv 1 \pmod{\phi(299)}$.

$$\phi(299) = (13-1)(23-1) = 12\cdot 22 = 264$$

Using, for example, Euclid's Algorithm to solve $65d \equiv 1 \pmod{264}$ one finds that

$$65\cdot 65 - 16\cdot 264 = 1, \quad d = 65$$

Hence

$$x \equiv 210^{65} \pmod{299}$$

See, example 4.5

A calculation via $x, x^2, x^4, x^8, \ldots, x^{64}$ (modular exponentiation) yields the answer $x \equiv 123 \pmod{299}$.

---

(8) For the first part, see the proof of Theorem 8.1 in the book. Then consider

$$a^{101} \equiv 1 \pmod{71}, \quad \varphi(71) = 71 - 1 = 70$$

Thus

$$a^{70} \equiv 1 \pmod{71} \quad \text{Fermat's theorem.}$$

The order of a must be among the divisors of 70, i.e. $2, 5, 7, 10, 14, 35, 70$. But 101 is a prime, so that the order of a is not a factor of 101. Thus NO SOLUTION!