TALLTEORI MA 1301/6301

EXAM. 9. $\overline{\text{XII}}$. 2009 4 pages P. Lindqvist

① The number

$$N = 1 + p_1 p_2 \cdots p_n$$

is not divisible by any of the prime numbers $p_1, p_2, \ldots, p_n$. Hence its prime factor(s) is (are) not any of these. Thus there exists at least one "new" prime. This proves that there are infinitely many prime numbers.

---

② $\begin{cases} x \equiv 5 \pmod 6 \\ x \equiv 5 \pmod{13} \\ x \equiv 4 \pmod 5 \end{cases}$

CHINESE REMAINDER THEOREM

$\Longleftrightarrow \quad x \equiv 239 \pmod{390}$

Calculations omitted

$\begin{cases} x \equiv 5 \pmod 6 \\ 10x \equiv 11 \pmod{13} \\ x \equiv 4 \pmod 5 \end{cases}$

$10x \equiv 11 \pmod{13} \Longleftrightarrow$

$40x \equiv 44 \equiv 5 \Longleftrightarrow$

$x \equiv 5$

The systems are equivalent and the answer is $x \equiv 239 \pmod{390}$ in both cases

---

③ $x^{147} \equiv 232 \pmod{253}$, $x = ?$

RSA

$\varphi(253) = 10 \cdot 22 = 220$,

$147 \cdot e \equiv 1 \pmod{220}$. Euclid's algorithm for the Diophantine equation

$$147e + 220f = 1$$

yields $e = 3$. We know that

$$x \equiv 232^e \equiv 232^3 \equiv 100 \pmod{253}.$$

4

- $$\sqrt{18} = 4 + (\sqrt{18}-4) = 4 + \cfrac{1}{\underbrace{\cfrac{1}{\sqrt{18}-4}}_{}} \quad \frac{1}{\sqrt{18}-4} = \frac{\sqrt{18}+4}{2}$$

$$= 4 + \cfrac{1}{4 + \cfrac{\sqrt{18}-4}{2}} = 4 + \cfrac{1}{4 + \cfrac{1}{\cfrac{2}{\sqrt{18}-4}}}$$

$$= 4 + \cfrac{1}{4 + \cfrac{1}{\sqrt{18}+4}} \quad \sqrt{18}+4 = 8 + (\sqrt{18}-4)$$

$$= 4 + \cfrac{1}{4 + \cfrac{1}{8 + \cfrac{1}{4 + \cfrac{1}{8 \cdots}}}} = [4; \overline{4, 8}]$$

"$m=2$"

0	1	2	3
$\frac{4}{1}$	$\frac{17}{4}$		

- A solution of

$$\boxed{x^2 - 18y^2 = 1}$$

is $x = p_1 = 17$, $y = q_1 = 4$,

i.e. $17^2 - 18 \cdot 4^2 = 1$. * A second solution is found from

$$x_2 + \sqrt{18}\, y_2 = (17 + \sqrt{18} \cdot 4)^2 = 577 + \sqrt{18} \cdot 136,$$

$x_2 = 577, \quad y_2 = 136$

* There are infinitely many solutions.

---

(5) $9^n - n^2 = 3^{2n} - n^2 = (3^n)^2 - n^2$

$$= (3^n - n)(3^n + n)$$

Thus we have a factorization, when $n = 1, 2, 3, \ldots$ Indeed, $3^n - n \neq 1$ since

$$3^n = (1+2)^n = 1^n + n \cdot 2^{n-1} + \cdots \geq 1 + n.$$

This exhibits that $9^n - n$ is not a prime.

---

(6) $49 \mid \frac{10^n - 1}{9} = \underbrace{111\ldots\ldots111}_{n\ 1\text{'s}}$ "REPUNITS"

Always $9 \mid 10^n - 1$. Hence the problem is the same as

$$49 \mid 10^n - 1 \iff 10^n \equiv 1 \pmod{49}.$$

According to the Euler-Fermat theorem

$$10^{\varphi(49)} \equiv 1 \pmod{49}.$$

Now $\varphi(49) = 7^2 - 7 = 42$. Hence

$$R_{42} = \underbrace{11\ldots111}_{42}$$

will do. So does R_{252}, where $252 = \varphi(9 \cdot 49)$.

Remark: R_{12} is wrong. The smallest possible number is R_{42}.

(7) By Fermat's Theorem

$$a^{p-1} \equiv 1 \pmod{p}.$$

In other words

$$p \mid a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right)$$

and $\frac{p-1}{2}$ is an integer ($p \geq 3$, $p =$ odd).

By Euclid's lemma*)

$$p \mid a^{\frac{p-1}{2}} - 1 \quad \underline{\text{or}} \quad p \mid a^{\frac{p-1}{2}} + 1,$$

i.e.,

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad \underline{\text{or}} \quad a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

This proves that at least one of the congruences hold. They cannot both be valid simultaneously, because that would lead to

$$1 \equiv -1 \pmod{p},$$

which is impossible for $p > 2$.

---

*) $p \mid bc \Rightarrow p \mid b$ or $p \mid c$ ($p =$ prime)

None of the numbers $2, 3, 4, \ldots, n$ divide $n! + 1$. Thus the factors of $n! + 1$ are all $> n$. So are the <u>prime</u> factors of $n! + 1$. Thus there exists a prime number $p > n$. It follows that there exists infinitely many prime numbers.