MA 1301 / 6301

TALLTEORI 7. VI. 2010

J. Lindqvist

---

① $13 \mid 13 + 1002!$ Hence $13 + 1002!$ is not a prime number.

---

② Antithesis: $6n^2 = m^2$, $\gcd(m, n) = 1$

$$3 \cdot 2n^2 = m^2 \Rightarrow 3 \mid m^2 \Rightarrow 3 \mid m \Rightarrow$$

$$m = 3\mu$$

$$\cancel{3} \cdot 2n^2 = \cancel{3} \cdot 3\mu^2 \Rightarrow 3 \mid n^2 \Rightarrow 3 \mid n$$

Thus $\gcd(m, n) \geq 3$. This is a ↯ contradiction. Hence the antithesis is false.

---

③ $x^{65} \equiv 6 \ (133)$, $133 = 7 \cdot 19$

$$\varphi(133) = 6 \cdot 18 = 108$$

$65 \cdot e \equiv 1 \ (\underline{108})$ has the solution $\underline{e = 5}$

(Use Euclid's algorithm to find it.)

$$x \equiv 6^e \ (133) \equiv 6^5 \ (133) \equiv 62 \ (133)$$

Answer: $x \equiv \underline{62} \ (133)$.

(4) Wilson: $(p-1)! \equiv -1 \pmod{p}$

103 is a prime number.

$102! \equiv \underline{-1} \pmod{103}$

$\underbrace{102}_{\equiv -1} \cdot 101! \equiv -1 \implies 101! \equiv \underline{1}$

$101 \cdot 100! \equiv 1, \quad -2 \cdot 100! \equiv 1$

$(-2)(51) \cdot 100! \equiv 51, \quad 102 \cdot 101! \equiv -51$

$(-1) \cdot 101! \equiv -51 \implies 101! \equiv \underline{\underline{51}}$

---

(5) $m^n - 1 = (m-1)(m^{n-1} + m^{n-2} + \cdots + m + 1)$

If $m > 2$, $m - 1 \geq 2$ and we have a factorization. (When $m = 2$, $m - 1 = 1$ so that there is no "first factor".)

---

(6) $\sqrt{23} = [4; \overline{1, 3, 1, 8}]$ length of the period is $m = 4$. Use p_3, q_3.

0	1	2	3		
4	1	3	1	8	1
$\frac{4}{1}$	$\frac{5}{1}$	$\frac{19}{4}$	$\frac{24}{5}$		

$x^2 - 23y^2 = 1$

Take

$x = \underline{\underline{24}}, \; y = \underline{\underline{5}}.$

(7) Claim $a^{4n+1} \equiv a \pmod{10}$

$\varphi(10) = 4$, $a^4 \equiv 1 \pmod{10}$ when
EULER–FERMAT
$2, 5 \nmid a$

In this case

$$a^{4n}+1 = (a^4)^n a \equiv 1^n a \equiv a.$$

Special cases.

- $\underline{10 \mid a}$ The last digit is clearly 0
- $5 \mid a$, $2 \nmid a$ The last digit is 5
- $2 \mid a$, $5 \nmid a$ Modulo 5 we have $a^{4n+1} \equiv a \pmod{\underline{\underline{5}}}$. Only $\underline{\text{one}}$ of the numbers $\alpha, \alpha+5$ is even. Now a is even, so is a^{4n+1}. Thus $a^{4n+1} \equiv a \pmod{\underline{\underline{10}}}$.

---

(8) $\underline{\text{Claim}}$ $2^{2^k} - 1$ has at least k different prime factors, $k = 1, 2, 3, \ldots$.

$\underline{\text{Proof by induction}}$ 1°) $\underline{k=1}$ $2^2 - 1 = 3$ %.

2°) Ind. Hypothesis: $2^{2^k} - 1$ has at least k diff. prime factors.

3°) $$2^{2^{k+1}} - 1 = 2^{2^k \cdot 2} - 1 = (2^{2^k})^2 - 1$$

$$= \underbrace{(2^{2^k} - 1)}_{\substack{\geq k \text{ different} \\ \text{prime factors} \\ \text{by Ind. Hyp.}}}(2^{2^k} + 1)$$

Now $2^{2^k} + 1$ contains a $\underline{\text{new}}$ prime factor, since

$\gcd(2^{2^k}+1, 2^{2^k}-1) = 1$

(A common factor is both odd and even!)

Thus we have at least $k+1$ different prime factors.