

$3^2 + 4^2 = 5^2$
 $9 + 16 = 25$
 $b = a \cdot x$
 $c = a \cdot y$
 $c = b \cdot x \Rightarrow c = (a \cdot x) \cdot y$
 $b + c = a \cdot b + a \cdot x = a \cdot (b + x)$
 $(b \cdot c) = a \cdot b \cdot c = (a \cdot c) \cdot b$

2 17-14:02

$m^2 + 1$ je delitelci $m+1$.
 $m+1 \mid m^2 - 1$
 $m+1 \mid 2$

$a = q_1 m + r_1 = q_2 m + r_2$
 $0 = (q_1 - q_2) m + (r_1 - r_2)$

$a \equiv r_1 \pmod{m}$
 $b \equiv r_2 \pmod{m}$

$a \cdot b \equiv r_1 \cdot r_2 \pmod{m}$

$a = q_1 m + r_1$
 $b = q_2 m + r_2$

$a \cdot b = q_1 q_2 m + q_1 m r_2 + q_2 m r_1 + r_1 r_2 \equiv r_1 r_2 \pmod{m}$

2 17-14:29

$a = a_1^{c_1} \dots a_k^{c_k}$
 $b = b_1^{d_1} \dots b_l^{d_l}$

$(= 2^7 \cdot 5^2 \cdot 11^3)$
 $(= 3^{14} \cdot 5 \cdot 13)$

a, b, \dots, d **Euclid:**

$a = 10175$ $b = 2277$

$10175 = 4 \cdot 2277 + 1067$
 $2277 = 2 \cdot 1067 + 143$
 $1067 = 7 \cdot 143 + 66$
 $143 = 2 \cdot 66 + 11$
 $66 = 6 \cdot 11 + 0$

$11 = 143 - 2 \cdot 66$
 $= 143 - 2(1067 - 7 \cdot 143)$
 $= -2 \cdot 1067 + 15 \cdot 143$
 $= -2 \cdot 1067 + 15(2277 - 2 \cdot 1067)$
 $= -32 \cdot 1067 + 15 \cdot 2277$
 $= 15 \cdot 2277 - 32(10175 - 4 \cdot 2277)$
 $= -32 \cdot 10175 + 143 \cdot 2277$

2 17-14:58

$(a_1, a_2) \mid (a_1, a_2) = a_1 a_2$
 $\Rightarrow (a_1, a_2) = \frac{a_1 a_2}{(a_1, a_2)} = q$

$2^{49} - 3 = a$ $b = 2^{35} - 1$

$2^{49} - 1 = 2^{14}(2^{35} - 1) + 2^{14} - 1$
 $2^{35} - 1 = (2^{21} + 2^7)(2^{14} - 1) + 2^7 - 1$
 $2^{14} - 1 = (2^7 + 1)(2^7 - 1) + 0$
 $= 127$

$2^7 - 1 = (2^{49} - 1) \dots$
 $= (2^{35} + 2^{21} + 1)(2^{14} - 1)$
 $= (2^{21} + 2^7)(2^{14} - 1)$

2 17-15:31