Number theory

$a \mid b \quad b = k_1 a \quad k \in \mathbb{Z}$

$b \mid d \quad d = k_2 b$

$19 \nmid 7 \quad 7 = \square\, 19$ ✗

19 is divisible by 7 $\quad 7 \mid 19 \quad 19 \neq \square\, 7$

$19 = \underset{q}{2} \times 7 + \underset{r}{5}$

✗ $19 = 1 \times 7 + 12$

$a = d\,q + r$

divisor, divider, quotient, remainder

$789 = \overset{34}{\square}\,23 + 7 \qquad 0 \leq r < d$

$1001 = (77)13 + 0$

-0.333

$-1 = (-1)3 + (\;) \qquad -1 = (-1)3 + 2$

$-1 + 3 \quad -3$

$-1 = -3 + 2 \qquad 0 \leq r = 2 < 3$

$-765432 = (-21)38271 + (38259)$

$a \equiv b \mod m \qquad m \mid a-b$

$a - b = k_1 m$

$a = b + k_1 m$

$a \equiv b \bmod m \qquad c \equiv d \bmod m$

$$a + c \equiv b + d \pmod m$$

$$ac \equiv bd \pmod m$$

$$(a \bmod m + b \bmod m) \bmod m = (a+b) \pmod m$$

$$[(a \bmod m)(b \bmod m)] \bmod m = ab \bmod m$$

$a = dq + r \qquad q = a \text{ div } d$

$r = a \bmod d$

$$19 = 2 \times 7 + 5$$

$19 \text{ div } 7 = 2$

$19 \bmod 7 = 5$

$a \equiv 4 \pmod{13} \qquad b \equiv 9 \bmod 13 \qquad 0 \leq c \leq 12$

a) $c \equiv 9a \pmod{13}$

$\equiv 36 \pmod{13}$

$\equiv 10 \bmod 13 \qquad c = 10$

b) $c \equiv 11b \pmod{13}$

$\equiv 99 \pmod{13}$

$\equiv 8 \pmod{13} \qquad c = 8$

e) $c \equiv (a^2 + b^2) \bmod 13$

$\equiv 97 \pmod{13} \equiv 6 \bmod 13$

$c =$

$(-133 \bmod 23 + 261 \bmod 23) \bmod 23$

$= (-133 + 261) \bmod 23$

$= 128 \bmod 23 = 13$

$128 = 5(23) + 13$

$\gcd(a, b) = d$

$d \mid a \wedge d \mid b$

$a = k_1 d \qquad b = k_2 d$

$\gcd(88, 1001)$

$88 = 2 \cdot 44 = 2 \cdot 4 \cdot 11 = 2^3 \cdot 11$

$1001 = 11 \cdot 91 = 11 \cdot 7 \cdot 13$

$\gcd(2^3 \cdot 11, 11 \cdot 7 \cdot 13) =$

$\underset{\min(3,0)}{2} \quad \underset{\min(1,1)}{11} \quad \underset{\min(0,7)}{7} \quad \underset{\min(0,1)}{13} =$

$2^0 \quad 11^{\cancel{0}} \quad 7^0 \quad 13^0 = 11$

$\operatorname{Lcm}(a, b) = \underset{\max(3,0)}{2} \quad \underset{\max(1,1)}{11} \quad \underset{\max(0,7)}{7} \quad \underset{\max(0,1)}{13}$

$=$

$lcm(a,b) = 2^3 \; 7^1 \; 11^1 \; 13^1$ $\qquad lcm(a,b) = d$

$a \mid d \qquad b \mid d$

$ab = lcm(a,b)\, gcd(a,b)$

$\gcd(a,b) = d$ $\quad \boxed{d = sa + tb}$

$\gcd(0,a) = a \qquad \gcd(1,a) = 1$

$a|0 \quad a|a \qquad 1|a \quad 1|1$

$0 = 0 \cdot a \qquad \cancel{a = a \cdot 1}$

$\gcd(10^3, 625) = \gcd(125, 0) = 125$

$10^3 = (1)\,625 + 375$

$625 = (1)\,375 + 250$

$375 = (1)\,250 + 125$

$250 = (2)\,125 + 0$

$125 = 375 - 250$

$= 375 - 625 + 375$

$= 2(375) - 625$

$= 2(10^3 - 625) - 625$

$\boxed{125 = (2)\,10^3 - 3(625)}$

$s = 2 \qquad t = -3 \qquad d = sa + tb$