Linear diophantine equations

$$ax+by=c$$

解法：① 算 $d=\gcd(a,b)$，if $d\mid c$，那么有解

② 找特解 (x_0,y_0). FindInstance[ax+by==c,{x,y},Integers]

③ 通解：$x=x_0+\frac{b}{d}t$，$y=y_0-\frac{a}{d}t$

验证：Reduce[ax+by==c ,{x,y}, Integers]

☆ $a+b\equiv(a \bmod m+b \bmod m)\ (\bmod\ d)$

$ab\equiv((a \bmod m)(b \bmod m))\ (\bmod\ d)$ } 用于化简

例：证 $41\mid 2^{20}-1$

证：即证 $2^{20}-1\equiv 0\ (\bmod\ 41)$

$\because 2^{20}=(2^5)^4$　$2^5=32\equiv -9\ (\bmod\ 41)$　$2^{20}=(-9)^4\ (\bmod\ 41)$

$=81\cdot 81\ (\bmod\ 41)$

$81\equiv(-1) \bmod 41$

$2^{20}\equiv 81^2\equiv 1\ (\bmod\ 41)$

☆ $ac\equiv bc\ (\bmod\ m)\Rightarrow a\equiv b\ (\bmod\ m/d)$　$d=\gcd(c,m)$

Linear Congruence

$$ax\equiv b\ (\bmod\ m)$$

解：该式写成 $ax-my=b$（变成 linear diophatine equation）

① 算 $d=\gcd(a,m)$　则有 d 个解

② 算特解 x_0，$x=x_0+\frac{m}{d}t$

例：$18x\equiv 30\ (\bmod\ 42)$

$\gcd(18,42)=6\Rightarrow$ 有 6 个解

$3x \equiv 5 \pmod 7$ $x_0 = 4,\ x_1 = 11,\ x_2 = 18,\ x_3 = 25,\ x_4 = 32,\ x_5 = 39$

The Chinese Remainder Theorem

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots \qquad \vdots$$
$$x \equiv a_n \pmod{m_n}$$

解 ① 算 $m = m_1 m_2 \cdots m_n$

$M_1 = \frac{m}{m_1}$ $M_2 = \frac{m}{m_2}$ ……

Find the inverse of M_k.

$M_1 y_1 \equiv 1 \pmod{m_1}$ $M_2 y_2 \equiv 1 \pmod{m_2}$ ……

$\Rightarrow y_1$ $\Rightarrow y_2$

$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots a_n M_n y_n$

最后: $x \equiv$ smallest $\pmod m$ (取最小的)

例: $x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

$m = 3 \cdot 5 \cdot 7 = 105$. $M_1 = 35$ $M_2 = 21$ $M_3 = 15$

$35 y_1 \equiv 1 \bmod 3$ $21 y_2 \equiv 1 \bmod 5$ $15 y_3 \equiv 1 \bmod 7$

$2 y_1 \equiv 1 \bmod 3$ $y_2 \equiv 1 \bmod 5$ $y_3 = 1 \bmod 7$

$y_1 = 2$ $y_2 = 1$ $y_3 = 1$

$\Rightarrow x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$

化简: $233 \equiv 23 \pmod{105}$ √

解复杂mod的congruency

例：$17x \equiv 9 \pmod{276}$ ① 分解276：$276 = 3\cdot4\cdot23$

$17x \equiv 9 \pmod 3$ $17x \equiv 9 \pmod 4$ $17x \equiv 9 \pmod{23}$

$x \equiv 0 \pmod 3$ $x \equiv 1 \pmod 4$ $17x \equiv 9 \pmod{23}$

$x = 3k \rightarrow 3k \equiv 1 \pmod 4$ modular inverse of $a=3$ is $\tilde{a}=3$

$\Rightarrow k \equiv 3 \pmod 4$

then, $x = 3(3+4j) = 9+12j$

$17(9+12j) \equiv 9 \pmod{23}$

$204j \equiv -144 \pmod{23}$

$\Rightarrow 3j \equiv 6 \pmod{23} \Rightarrow j = 2+23t$

$\Rightarrow x = 33+276t$ $x \equiv 33 \pmod{276}$

Fermat's Factorization Method

例：分解 $n = 119143$ ： $345^2 < 119143 < 346^2$

从346开始，$346^2 - n$，$347^2 - n$ ⋯ 直到某项 $(346+m)^2 - n$ 为完全平方数

$\Rightarrow 352^2 - 119143 = 4761 = 69^2$

$119143 = (352+69)(352-69) = 421\cdot283$

Mathematica：FactorInteger[n]

Fermat's Little Theorem

例：$5^{38} \bmod 11$ ，$\because 5^{10} \equiv 1 \pmod{11}$

$\Rightarrow 5^{38} = (5^{10})^3\cdot5^8 \equiv 5^8 \bmod 11$

$5^2 \equiv 3 \bmod 11$

$5^8 = (5^2)^4 \equiv 3^4 \pmod{11}$

$\equiv 81 \equiv 4 \bmod 11$

Mathematica: PowerMod[5, 38, 11]

Fermat Pseudoprimes

$a^p \equiv a \pmod q$ and $a^q \equiv a \pmod p$

then $a^{pq} \equiv a \pmod{pq}$

例: show that $2^{340} \equiv 1 \pmod{341}$: $341 = 11 \cdot 31$

$2^{10} = 1024 = 31 \cdot 33 + 1$

$\Rightarrow 2^{11} = 2 \cdot 2^{10} = 2 \cdot 1 \equiv 2 \pmod{31}$

$2^{31} = 2(2^{10})^3 = 2 \cdot 1^3 \equiv 2 \pmod{11}$ $\quad 2^{341} = 2^{11 \cdot 31} \equiv 2 \pmod{341}$

cancelling the factor 2 $\Rightarrow$ $2^{340} \equiv 1 \pmod{341}$