解答 (2013.10.24 出題)

1. $2^{35}-1$ と $2^{21}-1$ の最大公約数を求めよ.

   $a-b=2^{35}-2^{21}=2^{21}(2^{14}-1)\to 2^{14}-1$

   $b-(2^{14}-1)=2^{21}-2^{14}=2^{14}(2^7-1)\to 2^7-1$

   $(2^{14}-1)-(2^7-1)=2^{14}-2^7=2^7(2^7-1)\to 2^7-1$

   $(2^7-1)-(2^7-1)=0$ より

   $\mathrm{GCD}(2^{35}-1,2^{21}-1)=2^7-1=127.$

   一般に $\mathrm{GCD}(2^m-1,2^n-1)=2^{\mathrm{GCD}(m,n)}-1$ が成り立つ. (途中現れる数を 2 進表示したときの 1 の個数がちょうど m, n に対する互除法に対応する.)

2. $a=55$, $b=23$ に対し拡張ユークリッド互除法を実行し, $55x+23y=1$ をみたす整数 x, y を一組もとめよ.

   $v_1=\begin{pmatrix}55\\1\\0\end{pmatrix}$, $v_2=\begin{pmatrix}23\\0\\1\end{pmatrix}$, $v_3=v_1-2v_2=\begin{pmatrix}9\\1\\-2\end{pmatrix}$,

   $v_4=v_2-2v_3=\begin{pmatrix}5\\-2\\5\end{pmatrix}$, $v_5=v_3-v_4=\begin{pmatrix}4\\3\\-7\end{pmatrix}$, $v_6=v_4-v_5=\begin{pmatrix}1\\-5\\12\end{pmatrix}$

   1 が 4 を割り切るのでこれで終了し, $x=-5$, $y=12$ を得る. 実際 $(-5)\cdot 55+12\cdot 23=1$ である.

3. $a=1,\ldots,12$ に対し, $(ax) \bmod 13=1$ をみたす整数 x $(1\le x\le 12)$ を求めよ.

a	1	2	3	4	5	6	7	8	9	10	11	12
x	1	7	9	10	8	11	2	5	3	4	6	12

   $13k+1$ $(k=1,2,\ldots)$ をあらかじめ計算しておくと便利であろう.