問6.3

$\mathbb{Z} \ni a, b$, $a < b$ に対し $b = aq + r$ なる $\mathbb{Z} \ni q, r$, $0 \leq r < |a|$ は除法の原理より一意的に存在する。このとき、r は平均的に $\frac{|a|}{2}$ に等しくなる。拡張ユークリッドの互除法が終了するのは $r = 1$ となったときであるから、拡張ユークリッドの互除法の計算量は $\log_2 |a|$ 程度である。

また、中国剰余定理を用いて法演算を行う場合には、予め元の法を2つ(以上)の互いに素な法に分けた際の剰余演算をしておく必要がある。整数に対する法演算は、バイナリ法を用いると $\log_2 |n|$ 程度の計算量である。

(1) $p_1 = 2^3 \times 7 = 56$, $q_1 = 3^4 = 81$ とする。

まず、法 p_1, q_1 に対する法演算をする必要がある。

その計算量は p_1, q_1 あわせて $2\log_2 293^{13}$ である。

次に、拡張ECDにより $p_1 x + q_1 y = 1$ を満たす $\mathbb{Z} \ni x, y$ をおめる。

このときの計算量は、$\log_2 q_1 = \log_2 3^4$ である。

この後、この結果を用い「$293^{13} \bmod p_1 q_1$ を計算するが、この計算量は、上述の計算と比べて小さいため無視する。」・・・①

以上より、求める計算量は、

$2\log_2 293^{13} + \log_2 3^4 = 26 \times 8.195 + 4 \times 1.585 = 219.41$

(2) $p_2 = 2^3 = 8$, $q_2 = 3^4 \times 7 = 567$

(1)と同様にして計算量をおめると、

$2\log_2 293^{13} + \log_2 (3^4 \cdot 7) = 222.22$

(3) $p_3=7,\ q_3=2^3=8,\ r_3=3^4=81$

まず、p_3, q_3に対し、(1),(2)と同様の計算をし、293^{13}のp_3q_3による剰余を得る。

その後、p_3q_3, r_3に対し、計算を行い、$p_3q_3r_3$による剰余を得ることができる。全体の計算量は、

$3\times\log_2 293^{13}+\log_2 2^3+\log_2 3^4=325.945$

(4) 計算量の大きさは、

(1) < (2) < (3) となった。

ゆえに、今回の場合では、同程度の互いに素な二数に分割するのが好ましいと考えられる。