講義ノートの訂正

以下の 2 つの誤植がありました．お詫びして訂正させて頂くとともに，指摘して頂いた学生の方に感謝いたします．

- p.6 例 2.12 の表にある q の項は $q_0, q_1, q_2, \ldots$ とリストするのでひとつ上にずらす．

i	a	x	y	q
0	520	1	0	2
1	221	0	1	2
2	78	1	-2	1
3	65	-2	5	5
4	13	3	-7	
5	0			

- p.17 定理 5.1 の証明の 2 行目，最後の項の指数部分の k の前にある (は不要．
  $(m^e)^d = n^{ed} = m^{kM+1} = m^{k(p-1)(q-1)} \times m$.

RSA 暗号の数学的基礎 練習問題 解答例

練習問題 1

$$
\begin{array}{rcll}
 & & & (x_0, y_0) = (1, 0), \\
 & & & (x_1, y_1) = (0, 1), \\
a = a_0 = 3107 & = & 975 \times 3 + 182, & q_0 = 3, \quad (x_2, y_2) = (1, -3) \\
b = a_1 = 975 & = & 182 \times 5 + 65, & q_1 = 5, \quad (x_3, y_3) = (-5, 16) \\
a_2 = 182 & = & 65 \times 2 + 52, & q_2 = 2, \quad (x_4, y_4) = (11, -35) \\
a_3 = 65 & = & 52 \times 1 + 13, & q_3 = 1, \quad (x_5, y_5) = (-16, 51) \\
a_4 = 52 & = & 13 \times 4 &
\end{array}
$$

より，最大公約数 $d = 13$ であり，$(x, y) = (-16, 51)$.

練習問題 2

(1) 23 を法として考える．$7^2 \equiv 3$，$7^4 \equiv 9$，$7^8 \equiv 81 \equiv 12$．また，フェルマーの小定理から $7^{22} \equiv 1$ であることに注意すると，

$$7^{430} = (7^{22})^{19} \cdot 7^{12} \equiv 7^{8+4} \equiv 12 \cdot 9 \equiv 16 \pmod{23}.$$

(2) $173 = 2 \times 86 + 1$ より，$2 \times (-86) \equiv 1 \mod 173$．よって $2^{-1} \equiv -86 \equiv 87$.

$$
\begin{array}{lll}
 & & (x_0, y_0) = (1, 0) \\
 & & (x_1, y_1) = (0, 1) \\
173 = 17 \times 10 + 3 & q_0 = 10, & (x_2, y_2) = (1, -10) \\
17 = 3 \times 5 + 2 & q_1 = 5, & (x_3, y_3) = (-5, 51) \\
3 = 2 \times 1 + 1 & q_2 = 1, & (x_4, y_4) = (6, -61)
\end{array}
$$

より，$173 \times 6 + 17 \times (-61) = 1$ が成り立つから，$17 \times (-61) \equiv 1 \mod 173$．よって $17^{-1} \equiv -61 \equiv 112$.
(3) 41 を法として 16 の逆数 16^{-1} を求めればよい.

$$
\begin{array}{lll}
 & & (x_0, y_0) = (1, 0) \\
 & & (x_1, y_1) = (0, 1) \\
41 = 16 \times 2 + 9 & q_0 = 2, & (x_2, y_2) = (1, -2) \\
16 = 9 \times 1 + 7 & q_1 = 1, & (x_3, y_3) = (-1, 3) \\
9 = 7 \times 1 + 2 & q_2 = 1, & (x_4, y_4) = (2, -5) \\
7 = 2 \times 3 + 1 & q_3 = 3, & (x_5, y_5) = (-7, 18)
\end{array}
$$

より，$41 \times (-7) + 16 \times 18 = 1$ が成り立つので，$16^{-1} \equiv 18 \mod 41$．よって，$16x \equiv 19 \mod 41 \Leftrightarrow x \equiv 16^{-1}19 \equiv 18 \times 19 = 342 = 41 \times 8 + 14 \equiv 14 \mod 41$．よって解は $x \equiv 14 \mod 41$ となる．

練習問題 3

(1)

$$
\begin{array}{lll}
 & & (x_0, y_0) = (1, 0) \\
 & & (x_1, y_1) = (0, 1) \\
12 = 5 \times 2 + 2 & q_0 = 2, & (x_2, y_2) = (1, -2) \\
5 = 2 \times 2 + 1 & q_1 = 2, & (x_3, y_3) = (-2, 5)
\end{array}
$$

より，$12 \times (-2) + 5 \times 5 = 1$ だから，$x \equiv 2 \times 12 \times (-2) + 5 \times 5 \times 5 \equiv 77 \equiv 17 \pmod{60}$ と解ける．
(2) まず $20 \times 21 \times 23 = 9660$.

$$
\begin{array}{llllll}
21 \times 23 = 483 & 483u_1 \equiv 1 & \mod 20 & 3u_1 \equiv 1 & \mod 20 & \therefore u_1 = 7 \\
20 \times 21 = 460 & 460u_2 \equiv 1 & \mod 21 & 19u_2 \equiv 1 & \mod 21 & \therefore u_2 = 10 \\
20 \times 23 = 420 & 420u_3 \equiv 1 & \mod 23 & 6u_3 \equiv 1 & \mod 23 & \therefore u_3 = 4
\end{array}
$$

より

$$13u_1 \times 483 - 12u_2 \times 460 - 7u_3 \times 420 = 43953 - 55200 - 11760 = -23007 = 9660 \times (-3) + 5973$$

を得るので，$x \equiv 5973 \mod 9660$.
(3) まず $21 = 3 \times 7$ と互いに素な 1 より大きく 20 以下の自然数は，$2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20$.

a	2	4	5	8	10	11	13	16	17	19	20
$a \bmod 3$	2	1	2	2	1	2	1	1	2	1	2
$a \bmod 7$	2	4	5	1	3	4	6	2	3	5	6

ここで，$2^{20} \equiv (-1)^{20} \equiv 1 \pmod 3$．またフェルマーの小定理から，7 と互いに素な b に対して $b^6 \equiv 1 \pmod 7$ だから，$b^{20} \equiv (b^6)^3 \cdot b^2 \equiv b^2 \pmod 7$．これより，7 を法として，$2^{20} \equiv 4$, $3^{20} \equiv 9 \equiv 2$，$4^{20} \equiv 16 \equiv 2$，$5^{20} \equiv 25 \equiv 4$，$6^{20} \equiv 36 \equiv 1$ となる．上の表から

a	2	4	5	8	10	11	13	16	17	19	20
$a^{20} \bmod 3$	1	1	1	1	1	1	1	1	1	1	1
$a^{20} \bmod 7$	4	2	4	1	2	2	1	4	2	4	1

とわかる．中国剰余定理から，$a^{20} \equiv 1 \pmod{21}$ となる a は，$a^{20} \equiv 1 \pmod{3}$ かつ $a^{20} \equiv 1 \pmod{7}$ を満たすものだから，$a = 8, 13, 20$ である．これが $n = 21$ にフェルマー・テストを行った場合に,「素数の可能性がある」と出力するものである．

練習問題 4

(1) $M = (p-1)(q-1) = 28 \cdot 30 = 840$ である．$ed \equiv 1 \pmod{840}$ となる d を求める．

$$
\begin{array}{lll}
 & & (x_0, y_0) = (1, 0) \\
 & & (x_1, y_1) = (0, 1) \\
840 = 11 \times 76 + 4 & q_0 = 76, & (x_2, y_2) = (1, -76) \\
11 = 4 \times 2 + 3 & q_1 = 2, & (x_3, y_3) = (-2, 153) \\
4 = 3 \times 1 + 1 & q_2 = 1, & (x_4, y_4) = (3, -229)
\end{array}
$$

より，$840 \cdot 3 + 11 \cdot (-229) = 1$ となるので，$d \equiv -229 \equiv 611 \pmod{840}$.

(2) $c = 15^{11} \pmod{899}$.

まず 29 を法として，$15^2 = 225 \equiv 22 \equiv -7$，$15^4 \equiv 49 \equiv 20 \equiv -9$，$15^8 \equiv 81 \equiv 23 \equiv -6$ より，$15^{11} \equiv 15^{8+2+1} \equiv (-6) \cdot (-7) \cdot 15 \equiv 13 \cdot 15 \equiv 21 \equiv -8$.

次に 31 を法として，$15^2 = 225 \equiv 8$，$15^4 \equiv 64 \equiv 2$，$15^8 \equiv 4$ より，$15^{11} \equiv 15^{8+2+1} \equiv 4 \cdot 8 \cdot 15 \equiv 15$.

そこで，連立合同式 $x \equiv -8 \pmod{29}$，$x \equiv 15 \pmod{31}$ を解く．

$$
\begin{array}{lll}
 & & (x_0, y_0) = (1, 0) \\
 & & (x_1, y_1) = (0, 1) \\
31 = 29 \times 1 + 2 & q_0 = 1, & (x_2, y_2) = (1, -1) \\
29 = 2 \times 14 + 1 & q_1 = 14, & (x_3, y_3) = (-14, 15)
\end{array}
$$

より，$31 \cdot (-14) + 29 \cdot 15 = 1$ となる．従って，$x \equiv (-8) \cdot 31 \cdot (-14) + 15 \cdot 29 \cdot 15 = 9997 \equiv 108 \pmod{899}$ と解ける．よって暗号文 $c = 108$.

(3) $m = 467^{611} \pmod{899}$.

まず 29 を法として，$467 \equiv 3$．フェルマーの小定理から $3^{28} \equiv 1$ であることに注意する．さらに，$3^4 \equiv 9^2 \equiv 23 \equiv -6$，$3^8 \equiv 36 \equiv 7$，$3^{16} \equiv 49 \equiv -9$ であるから，

$$467^{611} \equiv 3^{611} \equiv (3^{28})^{21} \cdot 3^{23} \equiv 3^{16+4+2+1} \equiv (-9) \cdot (-6) \cdot 9 \cdot 3 \equiv -21 \equiv 8.$$

次に 31 を法として，$467 \equiv 2$．フェルマーの小定理から $2^{30} \equiv 1$ であることに注意する．さらに，$2^8 = 256 \equiv 8$ であるから，

$$467^{611} \equiv 2^{611} \equiv (2^{30})^{20} \cdot 2^{11} \equiv 2^{8+2+1} \equiv 8 \cdot 4 \cdot 2 \equiv 2.$$

そこで，連立合同式 $x \equiv 8 \pmod{29}$，$x \equiv 2 \pmod{31}$ を解く．(2) と同様に，$x \equiv 8 \cdot 31 \cdot (-14) + 2 \cdot 29 \cdot 15 = -2602 \equiv 95 \pmod{899}$ と解ける．よってもとのメッセージ $m = 95$.

練習問題 5

連立合同式 $x \equiv 60 \pmod{143}$，$x \equiv 203 \pmod{391}$，$x \equiv 711 \pmod{899}$ を解く．

$391 \cdot 899 u_1 \equiv \pmod{143} \Leftrightarrow 15 u_1 \equiv 1 \pmod{143}$.

$$
\begin{array}{lll}
 & & (x_0, y_0) = (1, 0) \\
 & & (x_1, y_1) = (0, 1) \\
143 = 15 \times 9 + 8 & q_0 = 9, & (x_2, y_2) = (1, -9) \\
15 = 8 \times 1 + 7 & q_1 = 1, & (x_3, y_3) = (-1, 10) \\
8 = 7 \times 1 + 1 & q_2 = 1, & (x_4, y_4) = (2, -19)
\end{array}
$$

より，$u_1 = -19$ が取れる．

$143 \cdot 899 u_2 \equiv \pmod{391} \Leftrightarrow 309 u_2 \equiv 1 \pmod{391}$.

$$
\begin{array}{lll}
 & & (x_0, y_0) = (1, 0) \\
 & & (x_1, y_1) = (0, 1) \\
391 = 309 \times 1 + 82 & q_0 = 1, & (x_2, y_2) = (1, -1) \\
309 = 82 \times 3 + 63 & q_1 = 3, & (x_3, y_3) = (-3, 4) \\
82 = 63 \times 1 + 19 & q_2 = 1, & (x_4, y_4) = (4, -5) \\
63 = 19 \times 3 + 6 & q_3 = 3, & (x_5, y_5) = (-15, 19) \\
19 = 6 \times 3 + 1 & q_4 = 3, & (x_6, y_6) = (49, -62)
\end{array}
$$

より，$u_2 = -62$ が取れる．

$143 \cdot 391 u_3 \equiv \pmod{899} \Leftrightarrow 175 u_3 \equiv 1 \pmod{899}$.

$$
\begin{array}{lll}
 & & (x_0, y_0) = (1, 0) \\
 & & (x_1, y_1) = (0, 1) \\
899 = 175 \times 5 + 24 & q_0 = 5, & (x_2, y_2) = (1, -5) \\
75 = 24 \times 7 + 7 & q_1 = 7, & (x_3, y_3) = (-7, 36) \\
24 = 7 \times 3 + 3 & q_2 = 3, & (x_4, y_4) = (22, -113) \\
7 = 3 \times 2 + 1 & q_3 = 2, & (x_5, y_5) = (-51, 262)
\end{array}
$$

より，$u_3 = 262$ が取れる．

以上から

$$
\begin{aligned}
x &\equiv 60 \times 391 \cdot 899 \times (-19) + 203 \times 143 \cdot 899 \times (-62) + 711 \times 143 \cdot 391 \times 262 \\
&\equiv 2460375 \pmod{143 \cdot 391 \cdot 899 = 50265787}
\end{aligned}
$$

と解ける．これが m^3 になるので，($130^3 = 2197000$ と $140^3 = 2744000$ から見当を付ければ）$m = 135$ とわかる．