代数入門：演習問題　解答

演習問題 1

1. (1) 4. (2) 10. (3) 5.

2. (1) 15. (2) 19. (3) 22.

3. $a = 0.3.6, 9.$

4. $a = 0, 8.$

5. $1 + 2 + \cdots + 10 = \dfrac{10 \cdot 11}{2} = 5 \cdot 11 \equiv 0 \ \ (mod\, 11).$

6. (1) 5. (2) 0. (3) 4.

7. $1 + 2 + 3 + \cdots + (n-1) \equiv \begin{cases} 0 \ \ (n \text{ が奇数のとき}) \\ \dfrac{n}{2} (n \text{ が偶数のとき}) \end{cases} \qquad (mod\, n).$

   （証明）公式より, $1+2+3+\cdots+(n-1) = \dfrac{(n-1)n}{2}$. もし n が奇数ならば, $n-1$ は偶数なので $\dfrac{n-1}{2}$ は整数. よって, $\dfrac{(n-1)n}{2}$ は n の倍数である. もし n が偶数ならば, $\dfrac{n}{2}$ は整数. $\dfrac{n}{2} - \dfrac{(n-1)n}{2} = n - \dfrac{n^2}{2} = n\left(1 - \dfrac{n}{2}\right)$ は n の倍数だから, $\dfrac{n}{2} \equiv \dfrac{(n-1)n}{2} \ \ (mod\, n).$

8. (1) 4. (2) 6. (3) 10.

9. p が素数のとき，$(p-1)! =_p p-1$ である．

   p が素数 $\Longleftrightarrow (p-1)! \equiv p-1 \, (\equiv -1) \ \ (mod\, p)$. は「ウィルソンの定理」と呼ばれるものである．

   証明：7 章のフェルマーの小定理の章の始めに，p が素数ならば，$a \neq 0$ は必ず $a \times_p x = 1$ の解を持つことを示す: $x = a^{-1}$ としるす．まず，$1^{-1} = 1, (p-1)^{-1} = p-1$ である．後者は $(p-1) \times_p (p-1) = (-1) \times_p (-1) = 1$ より従う．次に，$2 \times_p 3 \times_p 4 \times_p \cdots \times_p (p-2) = 1$ である．ゆえに，$(p-1)! =_p p-1$ である．p が素数でないならば，$p = ab, 1 < a, b < p$ と分解できて $(p-1)!$ に $a \times_p b$ が出てくるので，$(p-1)! = 0$ である．

演習問題 2

1. (1) $45 = 18 \times 2 + 9$
   $18 = 9 \times 2 + 0$ より，$(18, 45) = 9.$

(2) $182 = 143 + 39$
$143 = 39 \times 3 + 26$
$39 = 26 + 13$
$26 = 13 \times 2 + 0$. $\therefore (182, 143) = 13$.

(3) $102 = 84 + 18$
$84 = 18 \times 4 + 12$
$18 = 12 + 6$
$12 = 6 \times 2 + 0$. $\therefore (102, 84) = 6$.

2. (1) $45 - 18 \times 2 = 9$ だから，$x = -2, y = 1$ は $18x + 45y = (18, 45)$ の１つの解である．

(2) $a = 182, b = 143$ とおく．$182 = 143+39$ より $39 = 182-143 = a-b$.
$143 = 39 \times 3 + 26$ より $26 = 143 - 39 \times 3 = b - 3(a - b) = -3a + 4b$.
$39 = 26 + 13$ より $13 = 39 - 26 = (a - b) - (-3a + 4b) = 4a - 5b$ なので，$x = 4, y = -5$ は $182x + 143y = (182, 143) = 13$ の１つの解である．

(3) $a = 102, b = 84$ とおく．$102 = 84 + 18$ より $18 = 102 - 84 = a - b$.
$84 = 18 \times 4 + 12$ より $12 = 84 - 18 \times 4 = b - 4(a - b) = -4a + 5b$.
$18 = 12 + 6$ より $6 = 18 - 12 = (a - b) - (-4a + 5b) = 5a - 6b$ なので，$x = 5, y = -6$ は $102x + 84y = (102, 84) = 6$ の１つの解である．

3. (1) 1, 5, 7, 10 (2) 2, 10, (3) 3, 9 (4) 4, 8 (6) 6

4. 省略.

5. 省略.

6.

$$67890 = 12345 \times 5 + 6165$$

$$12345 = 6165 \times 2 + 15$$

$$6165 = 15 \times 411 + 0$$

したがって，互除法により，求める最大公約数は 15 である．

$67890 = a, 12345 = b$ とおくと，

$$67890 = 12345 \times 5 + 6165 \rightarrow 6165 = a - 5b.$$

$12345 = 6165 \times 2 + 15 \rightarrow 15 = b - 6165 \times 2 = b - 2(a - 5b) = -2a + 11b$.

ゆえに，$x = 11, y = -2$ とおけば，これは $12345x + 67890y = 15$ の解となっている．

演習問題 3

1. (1) 4 (2) 1, 3 (3) 2

2. (1) 2 (2) 2, 5 (3) なし

3.

a	1	2	3	4	5	6	7	8	9	10
a^{-1}	1	6	4	3	9	2	8	7	5	10

4. (1) 9 (2) 1 (3) 5

5.

a	1	2	3	4	5	6	7	8	9	10	11	12
a^{-1}	1	7	9	10	8	11	2	5	3	4	6	12

6. (1) 3 (2) 4 (3) 3

7. $ka = 0, (k+1)a = 0$ とすると，$ka = n\ell, (k+1)a = nt$ となる整数 ℓ, t がある．これより，$a = (k+1)a - ka = (t-\ell)n = 0$ である．

演習問題 4

1. 特殊解の取りかたは一意的でない．他にもいくらでも別の特殊解の取りかたはあるので，それらも正解である．

   (1) $\begin{cases} x = 2 + 5t \\ y = -1 - 3t \end{cases}$ (t は任意の整数)．

   (2) $\begin{cases} x = 4 + 5t \\ y = -1 - 2t \end{cases}$ (t は任意の整数)．

   (3) $\begin{cases} x = 4 - 5t \\ y = 1 - 2t \end{cases}$ (t は任意の整数)．

2. (1) 一般解は $\begin{cases} x = 5 - 7t \\ y = 1 - 2t \end{cases}$ (t は任意の整数) の形なので，$t = 0$ のとき，$1 \leq x \leq 10$ で，$(x, y) = (5, 1)$.

   (2) 一般解は $\begin{cases} x = 2 - 3t \\ y = 4 - 7t \end{cases}$ (t は任意の整数) の形なので，$t = -2, -1, 0$ のとき，$1 \leq x \leq 10$ で，$(x, y) = (2, 4), (5, 11), (8, 18)$.

   (3) 一般解は $\begin{cases} x = 2 + 2t \\ y = -1 - 3t \end{cases}$ (t は任意の整数) の形なので，$t = 0, 1, 2, 3, 4$ のとき，$1 \leq x \leq 10$ で，$(x, y) = (2, -1), (4, -4), (6, -7), (8, -10), (10, -13)$.

3. (1) 一般解は $\begin{cases} x = 4 + 2t \\ y = 4 - 3t \end{cases}$ (t は任意の整数）の形なので，$t = -1, 0, 1$ のとき，$x, y > 0$ で，$(x, y) = (2, 7), (4, 4), (6, 1)$.

   (2) 一般解は $\begin{cases} x = 7 + 3t \\ y = -5t \end{cases}$ (t は任意の整数）の形なので，$t = -1, -2$ のとき，$x, y > 0$ で，$(x, y) = (4, 5), (1, 10)$.

   (3) $7x + 4y = 1$ は解 $(x, y) = 3, y = -5$ を解に持つので．$7x + 4y = 40$ は $x = 120, -200$ を解に持つ．

   一般解は $\begin{cases} x = 120 + 4t \\ y = -200 - 7t \end{cases}$ (t は任意の整数）の形なので，$t = -29$ のとき，$x, y > 0$ で，$(x, y) = (4, 3)$.

4. (1)　亀が 1 匹で鶴が 2 羽か，亀が 3 匹で鶴が 1 羽.

   (2) $8x + 10y = 72$ を解いて，$x = 4, y = 4$ なので，両方とも 4 匹.

5. $2x + 4y = a$ が解を持ち，しかも $x, y > 0$ となる解は一意的ならば，$a = 6$ または $a = 8$ である．

6. $b = 5, 4, 3, 2, 1$ とそれぞれ見ていくと（ただし，$1 \leq a \leq b \leq 6$），$x + 5y = 6, x + 4y = 6, 2x + 4y = 6, x + 3y = 6, 3x + 3y = 6$ の 5 個.

演習問題 5

1. (1) $x = 3$. (2) $x = 4$. (3) $x = 4, 10$.

2. (1) 与式は，移項して $3x \equiv 4 \pmod 7$ と同じである．ゆえに,$x = 6$.

   (2) 与式は，移項して $6x \equiv -9 \equiv 6 \pmod{15}$ と同じである．$6x - 15y = 6$ を解くと，特殊解として $x = 6, y = 2$ がある．一般解は $(6, 15) = 3$ より，$\begin{cases} x = 6 - 5t \\ y = 2 - 2t \end{cases}$ ($t \in \mathbf{Z}$) と言う形なので,$0 \leq x \leq 14$ の範囲の x は $x = 1, 6, 11$ で，これが求める解である．

   (3) 与式は，移項して $4x \equiv -2 \equiv 16 \pmod{18}$ と同じである．$4x - 18y = 16$ を解くと，特殊解として $x = 4, y = 0$ がある．一般解は $(4, 18) = 2$ より，$\begin{cases} x = 4 - 9t \\ y = -2t \end{cases}$ ($t \in \mathbf{Z}$) と言う形なので,$0 \leq x \leq 17$ の範囲の x は $x = 4, 13$ で，これが求める解である．

3. $4x - 10y = a$ が解を持つ $\Longleftrightarrow$ 最大公約数 $(4, 10) = 2$ が a を割る．これより，$4x - 10y = a$ が解を持たないような a は $a = 1, 3, 5, 7, 9$ である．

4. もち金は 109 円．x 個買ったときの料金は $13x$ だが，1 円玉はすべて使うので，合同式 $13x \equiv 4 \pmod 5$ で $0 < 13x \leq 109$ の範囲で最大のものは $x = 8$. よって，8 個.

演習問題 6

1. $12 = 5+7, 14 = 3+11 (= 7+7), 16 = 3+13 (= 5+11), 18 = 7+11, 20 = 7+13, 22 = 3+19, 24 = 5+19, 26 = 3+23, 28 = 5+23, 30 = 7+23$

2. (1) 2 (2) 4 (3) 0 (4) 3

3. $m = p^k a, n = p^t b$ で a, b は p で割れないとする：$v_p(m) = k, v_p(n) = t$ である．(1) $mn = p^{k+t}ab$ で ab は p で割れないので，$v_p(mn) = k+t = v_p(m) + v_p(n)$.

   (2) $t \leq k$ とすると，$m + n = p^t(p^{k-t}a + b)$ なので，$v_p(m+n) \geq t = \min(v_p(m), v_p(n))$.

演習問題 7

1. (1) 1. (2) 5. (3) 3.

2. (1) $\displaystyle\sum_{k=0}^{32}((3k+1)^2(3k+1)^2 + (3k+3)^2) \equiv \sum_{k=0}^{32} 2 = 2 \times 33 \equiv 0 \pmod 3.$

   (2) $\displaystyle\sum_{k=0}^{19}((5k+1)^4 + (5k+1)^4 + (5k+3)^4 + (5k+4)^4 + (5k+5)^4) \equiv \sum_{k=0}^{19} 4 = 4 \times 20 \equiv 0 \pmod 5.$

   (3) $\displaystyle\sum_{k=0}^{14}((7k+1)^6 + (7k+1)^6 + (7k+3)^6 + (7k+4)^6 + (7k+5)^6 + (7k+6)^6 + (7k+7)^6) \equiv \sum_{k=0}^{13} 6 = 6 \times 14 \equiv 0 \pmod 7.$

3. $1^{10} - 2^{10} + 3^{10} - 4^{10} + \cdots + 99^{10} = \displaystyle\sum_{k=0}^{8}\left(\sum_{i=1}^{9}\left\{(11k+i)^{10} - (11k+i+1)^{10})\right\} + (11k+11)^{10}\right).$

   ここで，$\displaystyle\sum_{i=1}^{9}\left((11k+i)^{10} - (11k+i+1)^{10}\right) + (11k+11)^{10} \equiv 0 \pmod{11}$

   なので，結局 11 で割り切れることが分かる.

4. $p = 11$ として，$10 = p - 1$ に注意すると，フェルマーの小定理より，$1^{p-1} - 2^{p-1} + 3^{p-1} - 4^{p-1} + 5^{p-1} - 6^{p-1} + 7^{p-1} - 8^{p-1} + 9^{p-1} - 10^{p-1} + 11^{p-1} \equiv (1-1) + (1-1) + \cdots + (1-1) + 0 \equiv 0 \pmod{11}$ である．

5. $p = 7$ のとき，$a^5 = a^{-1}$ である．したがって，$\mathbf{F}_7$ において，$1^5 + 2^5 + 3^5 + 4^5 + 5^5 + 6^5 + 7^5 = 1 + 4 + 5 + 2 + 3 + 6 + 0 = 0$ である．

6. n が奇数のとき，$\mathbf{F}_7$ において，$1^n + 2^n + 3^n + 4^n + 5^n + 6^n + 7^n = 1^n + 2^n + 3^n + (-3)^n + (-2)^n + (-1)^n + 7^n = 1 + 2^n + 3^n - 3^n - 2^n - 1 + 0 = 0$ である．

   n が偶数のとき，$1^n + 2^n + 3^n + 4^n + 5^n + 6^n + 7^n = 2(1 + 2^n + 3^n)$ である．$n = 2, 4$ の場合のみこれが 0 になることを確認すればよい．

   $n = 2$ のとき，$2(1 + 4 + 9) = 28 = 0$ である．$n = 4$ のとき，$2(1 + 16 + 81) = 2 \times 98 = 0$ である．

7. 略．

演習問題 8

1. (1) $x^2 + 1$. (2) $x^3 + 1$. (3) $x^5 + 1$.

2. $x^p + 1$.

3. (1) 商は $2x + 4$, 余りは $x + 1$.

   (2) 商は $4x^2 + 6x + 6$, 余りは 6.

   (3) 商は $x + 10$, 余りは 0.

4. (1) $(x + 2)(x + 1)$.

   (2) $(x + 1)(x + 4)$.

   (3) $(x + 3)(x + 4)$.

演習問題 9

1. (1) $2, 4$. (2) $1, 5$. (3) $2, 4, 6$.

2. (1) $x^2 + 4 = x^2 - 9 = (x - 3)(x + 3)$ より，$x = 3, -3 = 3, 10$. (2) $8x^2 + 4x + 1 = 8(x^2 + 7x + 5) = 8(x - 1)(x - 5)$ より，$x = 1, 5$. (3) $x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x - 8)(x + 8)$ より，$x = 1, -1, 8, -8 = 1, 12, 8, 5$.

3. フェルマの小定理より，$\forall x \in \mathbf{F}_p - \{0\}) x^{p-1} = 1)$ なので，$\mathbf{F}_p$ の 0 でない $p - 1$ この元は方程式 $x^{p-1} - 1 = 0$ の根である．あとは因数定理（定理 9.3）を繰り返し用いる．

4. 上で証明した等式 $x^{p-1}-1=(x-1)(x-2)\cdots(x-(p-1))$ に $x=0$ を代入すればよい.

5. $\mathbf{F}_{17}$ で $2^8=2^4 2^4=(-1)\times(-1)=1$ なので，$2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8$ は $x^8-1=0$ の根である.

演習問題 10

1. (1) $\mathbf{F}_{11}$ の各元 $a\neq 0$ の位数は a^n を計算して行って初めて 1 となる n だが，位数は $p-1=11-1=10$ の約数であることが分かっているので，1 以外の元の位数は $n=2,5,10$ のどれかである．フェルマの定理より，$a^{10}=1$ は分かっているから，したがって，$a^2\neq 1, a^5\neq 1$ が確認できれば，a は原始根である.

   $2^2=4\neq 1, 2^5=4\cdot 8=10\neq 1$ なので，2 は $\mathbf{F}_{11}$ の原始根である.

   (2) $\mathbf{F}_{13}^*$ の各元 a の位数は a^n を計算して行って初めて 1 となる n だが，位数は $p-1=13-1=12$ の約数であることが分かっているので，1 以外の元の位数は $n=2,3,4,6,12$ のどれかである．フェルマの定理より，$a^{12}=1$ は分かっているから，したがって，$a^2\neq 1, a^3\neq 1, a^4\neq 1, a^6\neq 1$ が確認できれば，a は原始根である.

   $2^2=4\neq 1, 2^3=8\neq 1, 2^4=3\neq 1, 2^6=4\cdot 3=12\neq 1$ なので，2 は $\mathbf{F}_{13}$ の原始根である.

   (3) $\mathbf{F}_{17}^*$ の各元 a の位数は a^n を計算して行って初めて 1 となる n だが，位数は $p-1=17-1=16$ の約数であることが分かっているので，1 以外の元の位数は $n=2,4,8,16$ のどれかである．フェルマの定理より，$a^{16}=1$ は分かっているから，したがって，$a^2\neq 1, a^4\neq 1, a^8\neq 1$ が確認できれば，a は原始根である.

   $3^2=9\neq 1, 3^4=13\neq 1, 3^8=16\neq 1$ なので，3 は $\mathbf{F}_{17}$ の原始根である

   $2^8=2^4 2^4=(-1)^2$ なので，2 の位数は 8 であり 16 でないので，2 は $\mathbf{F}_{17}$ の原始根ではない.

2. (1) 2 は $\mathbf{F}_{11}$ の原始根なので，$\{1,2,\cdots,10\}=\{2^0,2^1,2^2,\cdots,2^9\}$ であるから，$1+2+2^2+\cdots+2^9=1+2+3+\cdots+10=\dfrac{10\times 11}{2}=5\times 11=0$ である．これを利用するか，次のようにやってもよい.

   $1+2+2^2+2^3+\cdots+2^{100}=\dfrac{2^{101}-1}{2-1}=2^{101}-1\equiv 2-1=1 \pmod{11}$ なので，1.

   (2) $1+2+2^2+2^3+\cdots+2^{100}=\dfrac{2^{101}-1}{2-1}=2^{101}-1\equiv 2^5-1=5 \pmod{13}$ なので，5.

(3) $1+3+3^2+3^3+\cdots+3^{100} = \sum_{k=0}^{5}\{3^{16k}+3^{16k+1}+3^{16k+2}+\cdots+3^{16k+15}\}+$ $3^{96}+3^{97}+3^{98}+3^{99}+3^{100} \equiv 6(1+2+3+\cdots+16)+1+3+3^2+3^3+3^4 = 6\dfrac{16\cdot 17}{2}+\dfrac{3^5-1}{2} \equiv 0+2=2 \pmod{17}$ なので，2.

3. 略.

4. 是非やってみてください．$\dfrac{2}{7}, \dfrac{3}{7}, \cdots, \dfrac{6}{7}$ の少数展開の循環節も見てみましょう.

5. 略.

演習問題 11

1. (1) $\bmod 11$ で 2 のべき乗 2^k を計算して，$2^2=4, 2^3=8, 2^4=5, 2^5=10, 2^6=9, 2^7=7, 2^8=3, 2^9=6, 2^{10}=1$ より，$\mathrm{ind}_2(a)$ が求まる.

   また，各元 a の位数は a^n を計算して行って初めて 1 となる n だが，位数は $p-1=11-1=10$ の約数であることが分かっているので，1 以外の元の位数は $n=2,5,10$ のどれかである．$\bmod 11$ で計算して，$3^5=12=1$ より，3 の位数は 5 である．$4^2=5, 4^3=9, 4^5=1$ なので，$\mathrm{ord}(4)=5$. $5^2=3, 5^3=4, 5^5=1$ なので，$\mathrm{ord}(5)=5$. $6^2=3, 6^3=7, 6^5=10$ なので，6 の位数は 10（つまり，6 も $\mathbf{F}_{11}$ の原始根）である．$7=-4$ なので，$7^2=4^2\neq 1, 7^5=(-4)^5=-1\neq 1$ なので，7 の位数は 10（つまり，7 も $\mathbf{F}_{11}$ の原始根）である．$8=-3$ より，$8^5=(-3)^5=-3^5=-1$ なので，$\mathrm{ord}(8)=10$（つまり，8 も $\mathbf{F}_{11}$ の原始根）．$9=-2$ なので，同様に，$8^5=(-2)^5=-2^5=-(-1)=1$ なので，$\mathrm{ord}(9)=5$. 最後に，$10=-1$ より $10^2=1$ だから，$\mathrm{ord}(10)=2$.

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{ind}_2(a)$	10	1	8	2	4	9	7	3	6	5
$\mathrm{ord}(a)$	1	10	5	5	5	10	10	10	5	2

   (2) $\bmod 13$ で計算していって，次の結果を得る.

a	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ind}_2(a)$	12	1	4	2	9	5	11	3	8	10	7	6
$\mathrm{ord}(a)$	1	12	3	6	4	12	12	4	3	6	12	2

2. (1) $\mathbf{F}_{11}$ の原始根として 2 をとり，$p-1=10=5\cdot 2$ なので，$1, 2^2=4, 2^4=5, 2^6=9, 2^8=3$ が，つまり $3,4,5,9$ が $x^5-1=0$ の解である.

   (2) $\mathbf{F}_{13}$ の原始根として 2 をとり，$p-1=12=4\cdot 3$ なので，$1, 2^3=8, 2^6=12, 2^9=5$ が，つまり $1,5,8,12$ が $x^4-1=0$ の解である.

   (3) $\mathbf{F}_{17}$ の原始根として 3 をとり，$p-1=16=8\cdot 2$ なので，$3^2=9, 3^4=13, 3^6=15, 3^8=16, 3^{10}=8, 3^{12}=4, 3^{14}=2, 3^{16}=1$ が，つまり $1,2,4,8,9,13,15,16$ が $x^8-1=0$ の解である.

3. $1 \leq a \leq 12$ なる整数 a に対して，$a^{12} \equiv 1 \pmod{13}$ である（フェルマーの小定理）．したがって，$a^{100} \equiv (a^{12})^8 a^4 \equiv a^4 \pmod{13}$ である．そこで，$a^4 \equiv 1\mathrm{ind}_2(5) \pmod{13}$ となる a を求めればよいが，それは，$x^4 - 1 = 0$ の解であるから，上の問題の (2) より，$1, 5, 8, 12$ がそうである．

演習問題 12

$\mathbf{F}_p$ における方程式 $x^n = a$ の解法：

1. $\mathbf{F}_p$ の原始根 r を一つ選ぶ（どれでもよい）
2. $x^n = a$ より，合同式 $\mathrm{ind}_r(x^n) \equiv n \times \mathrm{ind}_r(x) \equiv \mathrm{ind}_r(a) \pmod{\textbf{p-1}}$ がなりたつ．$X = \mathrm{ind}_r(x)$ とおく．$\mathrm{ind}_r(a) = m$ を求める．
3. 1 次合同式 $n \times X \equiv m \pmod{\textbf{p-1}}$ を解く（$\bmod\ p$ ではない）．解の個数は $(n, p-1)$ 個である．
4. 1 次合同式 $nX \equiv m \pmod{\textbf{p-1}}$ の解を $k_1, k_2, \cdots, k_s$ とするとき，$x = r^{k_1}, r^{k_2}, \cdots, r^{k_s}$ が方程式 $x^n = a$ の解である．

問 1. (1) $\mathbf{F}_{11}$ の原始根として 2 がとれる（練習問題 10 の 1 (1). その他の $\mathbf{F}_{11}$ の原始根として $6, 7, 8$ があるが，2 が計算がラクそうである）．$2^4 = 5$ なので，$\mathrm{ind}_2(5) = 4$ である．したがって，$X = \mathrm{ind}_2(x)$ とおいて，1 次合同式 $6X \equiv 4 \pmod{p-1 = 11-1 = 10}$ を解く. 解の個数は $(6, 10) = 2$ 個である．解は不定方程式 $6X - 10Y = 4$ を解いて，$X = 4, 9$ である．ゆえに，求める方程式の解は $x = 2^4, 2^9 (= 2^{-1}) = 5, 6$ である．

(2) $\mathbf{F}_{13}$ の原始根として 2 がとれる（練習問題 10 の 1 (2)）．$2^4 = 16 = 3$ なので，$\mathrm{ind}_2(3) = 4$ である．したがって，$X = \mathrm{ind}_2(x)$ とおいて，1 次合同式 $8X \equiv 4 \pmod{p-1 = 13-1 = 12}$ を解く．解の個数は $(8, 12) = 4$ 個である．解は不定方程式 $8X - 12Y = 4$ を解いて，$X = 2, 5, 8, 11$ である．ゆえに，求める方程式の解は $x = 2^2, 2^5, 2^8, 2^{11} (= 2^{-1}) = 4, 6, 9, 7$ である．

(3) $\mathbf{F}_{17}$ の原始根として 3 がとれる（練習問題 10 の 1 (3)）．$3^3 = 10, 3^4 = 30 = 13$ なので，$\mathrm{ind}_3(14) = 4$ である．したがって，$X = \mathrm{ind}_3(x)$ とおいて，1 次合同式 $10X \equiv 4 \pmod{p-1 = 17-1 = 16}$ を解く. 解の個数は $(10, 16) = 2$ 個である．解は不定方程式 $10X - 16Y = 4$ を解いて，$X = 2, 10$ である．ゆえに，求める方程式の解は $x = 3^2, 3^{10} = 9, 8$ である．$3^8 = -1$ なので（$3^{16} = 1$ で 3 は原始根だから），$3^{10} = -9 = 8$ である．

問 2. (1) $\mathbf{F}_{11}$ の原始根として 2 がとれる．$2^8 = 3$ なので，$\mathrm{ind}_2(3) = 8$ である．したがって，$X = \mathrm{ind}_2(x)$ とおいて，1 次合同式 $2X \equiv 8 \pmod{p-1 =}$

$11-1=10$) を解く. 解の個数は $(2,10)=2$ 個である．解は不定方程式 $2X-10Y=8$ を解いて，$X=4,9$ である．ゆえに，求める方程式の解は $x=2^4, 2^9(=2^{-1})=5,6$ である．

(2) $\mathbf{F}_{11}$ の原始根として 2 がとれる．$2^7=7$ なので，$\mathrm{ind}_2(7)=7$ である．したがって，$X=\mathrm{ind}_2(x)$ とおいて，1 次合同式 $2X\equiv 7 \pmod{p-1=11-1=10}$ を解く．しかし，$(2,10)=2$ は 7 を割らないので，不定方程式 $2X-10Y=7$ に解は無い．

(3) $\mathbf{F}_{13}$ の原始根として 2 がとれる（練習問題 10 の 1 (2)）．$2^{10}=10$ なので，$\mathrm{ind}_2(10)=10$ である．したがって，$X=\mathrm{ind}_2(x)$ とおいて，1 次合同式 $2X\equiv 10 \pmod{p-1=13-1=12}$ を解く．解の個数は $(2,12)=2$ 個である．解は不定方程式 $2X-12Y=10$ を解いて，$X=5,11$ である．ゆえに，求める方程式の解は $x=2^5, 2^{11}(=2^{-1})=6,7$ である．

問 3. $\mathbf{F}_{13}$ において方程式 $x^2=-1=12$ は解をもつ．実際，$\mathbf{F}_{13}$ の原始根として 2 をとる．$2^6=-1$ なので，$\mathrm{ind}_2(-1)=6$ である．したがって，$X=\mathrm{ind}_2(x)$ とおいて，1 次合同式 $2X\equiv 6 \pmod{p-1=13-1=12}$ を解く．解の個数は $(2,12)=2$ 個である．解は不定方程式 $2X-12Y=6$ を解いて，$X=3,9$ である．ゆえに，求める方程式の解は $x=2^3=8$ と，$2^9=2^6 2^3=-1\times 8=5$ である．

問 4. (1) $x^2+2x+4=(x+1)^2+3=0$ より，$(x+1)^2=-3=4$ であるから，$x+1=\pm 2=2,5$. $\therefore x=1,4$.

(2) $x^2+4x+2=x^2+4x+4-2=(x+2)^2-2=0$ より，$(x+2)^2=2$. $\mathbf{F}_7$ において $3^2=2, 4^2=2$ なので，$x+2=3,4$. $\therefore x=1,2$.

(3)

平方完成すると，$\left(x+\dfrac{9}{2}\right)^2+7-\dfrac{81}{4}=0$ である．$\mathbf{F}_{11}$ において，$\dfrac{1}{2}=6, 9\times 6=54=-1, \dfrac{1}{4}=36=3, 81=4$ なので，方程式は，$\left(x+\dfrac{9}{2}\right)^2+7-\dfrac{81}{4}=0$ は $(x-1)^2=5$ となる．$\mathbf{F}_{11}$ において，$t^2=5$ を解くと，$t=4,7$ だから，$t=x-1$ のとき，$x-1=4,7$ より，$x=5,8$ が求める解である．