

15. まとめ

代数Ⅱ

試験対策1

連立合同式

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 6 \pmod{11} \end{cases}$$

ユークリッドの互除法

1. $m \geq n$ に対して
2. $n=0$ なら m を出力 終了
3. n を m とし, m を n で割った余りを n とし, ②に戻る

$$(4368, 315) = (315, 273) = (273, 42) = (42, 21) = (21, 0)$$

法5の剰余類の演算表

$$Z_5 = \{0, 1, 2, 3, 4\}$$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

p^α (p は素数)の約数の和は

$$1 + p + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}$$

連分数表示

$$\sqrt{3} = 1 + \frac{1}{1 + \frac{1}{2 + (\sqrt{3} - 1)}} = \langle 1, 1, 2, 1, 2, \dots \rangle = \langle 1, \dot{1}, \dot{2} \rangle$$

$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 6 \pmod{11} \end{cases}$	<p>両辺を3倍する</p> $12l \equiv l \equiv 30 \equiv 8 \pmod{11}$ $l = 11m + 8 (m \in \mathbb{Z})$ <p>代入して</p> $x = 15(11m + 8) + 7$ $x = 165m + 127$ $x \equiv 127 \pmod{165}$
$x \equiv 1 \pmod{3}$ $x = 3k + 1 (k \in \mathbb{Z})$ <p>2式に代入</p> $3k + 1 \equiv 2 \pmod{5}$ $3k \equiv 1 \pmod{5}$ <p>両辺を2倍する</p> $6k \equiv k \equiv 2 \pmod{5}$ $k = 5l + 2 (l \in \mathbb{Z})$ $x = 3(5l + 2) + 1 = 15l + 7$ <p>3式に代入</p> $15l + 7 \equiv 6 \pmod{11}$ $4l \equiv -1 \equiv 10 \pmod{11}$	<p>(検算)</p> $127 \equiv 1 \pmod{3}$ $127 \equiv 2 \pmod{5}$ $127 \equiv 6 \pmod{11}$

試験対策2

合同式で割った余りを求める
 $15^{143} \pmod{16} \equiv$

フェルマーの(小)定理
 p が素数, $(a, p) = 1$ ならば
 $a^{p-1} \equiv 1 \pmod{p}$

最大公約数(G.C.D.)greatest common divisor
 $(a, b) = g$

最小公倍数(L.C.M.)least common multiple
 $[a, b] = l$

群

• 空でない集合Gに対して, ある演算*が定義

- (1) 閉鎖律
 (2) 結合律 $(x * y) * z = x * (y * z)$
 (3) 単位元 e の存在 $e * x = x * e = x$
 (4) 逆元 x' の存在 $x' * x = x * x' = e$

(5) 可換律 $x * y = y * x$

可換群

模擬試験

- (1) 剰余環 Z_{12} の可逆元, 零因子を全て求めよ
 (2) 8^{103} を 13 で割ったときの余りを求めよ
 (3) k を奇数とすると, $1^k + 2^k + \dots + n^k$ は $1 + 2 + \dots + n$ で割り切れることを示せ
 (4) $(a + b)^p \equiv a^p + b^p \pmod{p}$ p は素数のとき示せ

模擬試験ヒント

- (1) 剰余環 Z_{12} の可逆元, 零因子を全て求めよ
 演算表をつくる
 (2) 8^{103} を 13 で割ったときの余りを求めよ
 この場合は, フェルマーの定理を使ってあげてもいい
 (3) k を奇数とすると, $1^k + 2^k + \dots + n^k$ は $1 + 2 + \dots + n$ で割り切れることを示せ
 1 から n の和は和の公式で表せるから, そこから考える
 (4) $(a + b)^p \equiv a^p + b^p \pmod{p}$ p は素数のとき示せ
 2項定理を用いて

$$(a + b)^p = \sum_{k=0}^p {}_p C_k a^{p-k} b^k = a^p + {}_p C_1 a^{p-1} b + {}_p C_2 a^{p-2} b^2 + \dots + {}_p C_{p-1} a b^{p-1} + b^p$$

$${}_p C_r = \frac{p!}{r!(p-r)!} = \frac{p(p-1)\cdots(p-r+1)}{r!}$$