１４．体の例とまとめ1

代数Ⅱ

$$\begin{cases} x \equiv 1 (\mathrm{mod}\, 3) \\ x \equiv 2 (\mathrm{mod}\, 5) \\ x \equiv 6 (\mathrm{mod}\, 11) \end{cases}$$

$x \equiv 1 (\mathrm{mod}\, 3)$

$x = 3k + 1 (k \in Z)$

2式に代入

$3k + 1 \equiv 2 (\mathrm{mod}\, 5)$

$3k \equiv 1 (\mathrm{mod}\, 5)$

両辺を2倍する

$6k \equiv k \equiv 2 (\mathrm{mod}\, 5)$

$k = 5l + 2 (l \in Z)$

$x = 3(5l + 2) + 1 = 15l + 7$

3式に代入

$15l + 7 \equiv 6 (\mathrm{mod}\, 11)$

$4l \equiv -1 \equiv 10 (\mathrm{mod}\, 11)$

両辺を3倍する

$12l \equiv l \equiv 30 \equiv 8 (\mathrm{mod}\, 11)$

$l = 11m + 8 (m \in Z)$

代入して

$x = 15(11m + 8) + 7$

$x = 165m + 127$

$x \equiv 127 (\mathrm{mod}\, 165)$

(検算)

$127 \equiv 1 (\mathrm{mod}\, 3)$

$127 \equiv 2 (\mathrm{mod}\, 5)$

$127 \equiv 6 (\mathrm{mod}\, 11)$

試験対策１

連立合同式

$$\begin{cases} x \equiv 1 (\mathrm{mod}\, 3) \\ x \equiv 2 (\mathrm{mod}\, 5) \\ x \equiv 6 (\mathrm{mod}\, 11) \end{cases}$$

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

複素数体や体の乗法においての
逆元の計算

連分数表示

$$\sqrt{3} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + (\sqrt{3} - 1)}} = <1,1,2,1,2,\cdots> = <1,\dot{1},\dot{2}>$$

試験対策2

合同式で割った余りを求める

$15^{143}(mod\ 16) \equiv$

フェルマーの(小)定理

pが素数，$(a,p)=1$ならば

$a^{p-1} \equiv 1(mod\ p)$

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

環と体の定義，分類

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を奇数とするとき，$1^k + 2^k + \cdots + n^k$ は$1 + 2 + \cdots + n$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を奇数とするとき，$1^k + 2^k + \cdots + n^k$ は$1 + 2 + \cdots + n$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

$$(a+b)^p = \sum_{k=0}^{p} {}_pC_k a^{p-k} b^k = a^p + {}_pC_1 a^{p-1} b + {}_pC_2 a^{p-2} b^2 + \cdots + {}_pC_{p-1} a b^{p-1} + b^p$$

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