数学通論 レポート 5, 解答.

問 5.1 1. 同値関係による完全代表系の定義を書きなさい.

2. p を素数とするとき $\equiv$ についての一次方程式 $ax \equiv b \bmod p$ をどのようにして解けばよいか例をあげて説明しなさい.

3. p を素数、a を p と互いに素な自然数とする時、次を証明しなさい.

$$a^{p-1} \equiv 1 \pmod{p} \tag{1}$$

解答 1. 完全代表系とは各同値類からとってきた代表元. R を完全代表系, S を全体集合とすると次の性質をもつ. (a) $R \ni a, b$ が $a \neq b$ なら $a \not\sim b$. (b) 任意の $a \in S$ に対して, $b \sim a$ となる R の元 b が存在.

2. (x, y) についての不定方程式 $ax + py = b$ を解けばよい. これは (ユークリッドの) 互除法でたとえば次のように解くことができる.
例: $4x + 11y = 4$ を考える.

$$\begin{aligned} 11 &= 2 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \end{aligned}$$

よって, $4 - 1 \cdot (11 - 2 \cdot 4) = 1$, 計算して, $-1 \cdot 11 + 3 \cdot 4 = 1$. 全体を 4 倍 すると, $-4 \cdot 11 + 12 \cdot 4 = 4$ となり $(x, y) = (12, -4)$ となる. よって, $4x \equiv 4 \bmod 11$ の解として, 12 が得られる. (見ただけで 1 が解であるが, $12 \equiv 1$.)
3. a は p と互いに素なので, $a^{p-1} \not\equiv 0 \bmod p$.
$a^{p-1} \equiv r \bmod p$ となる代表元 $r \in \{1, 2, \ldots, p-1\}$ をとってくると, $r, 2r, \ldots, (p-1)r$ はすべて異なる同値類に入るので, $a^{p-1}, 2a^{p-1}, \ldots (p-1)a^{p-1}$ はすべて異なる同値類に入る. これらをすべてかけることにより,

$$(p-1)!a^{p-1} \equiv (p-1)! \bmod p, \quad \therefore (p-1)!(a^{p-1} - 1) \equiv 0 \text{ modp}$$

となる. 明らかに $(p-1)! \not\equiv 0 \bmod p$ だから,

$$a^{p-1} - 1 \equiv 0 \bmod p \quad \therefore a^{p-1} \equiv 1 \bmod p.$$

[**別解**] $a \equiv 1 \bmod p$ のときは明らかに成立. a と p は互いに素だから同値類で考えて, $2 \leq a \leq p-1$ として良い. p が素数なので, 2 項係数 $\binom{p}{k}$ は $k \neq 0, p$ のとき p の倍数となるので,

$$a^p = (a - 1 + 1)^p \equiv (a-1)^p + 1 \mod p$$

これを繰り返すと $a^p \equiv a \bmod p$ がいえ,

$$a(a^{p-1} - 1) \equiv 0 \bmod p$$

p が素数なので, $a \not\equiv 0 \bmod p$ から, $a^{p-1} \equiv 1 \bmod p$ がわかる.

問 5.2 p を素数とする.

1. 集合 $\mathbf{Z} \setminus p\mathbf{Z} = \{x \in \mathbf{Z} \,|\, x \notin p\mathbf{Z}\}$ に関係 $x \sim y$ を $x \equiv y \bmod p$ で定義する. $\sim$ は同値関係であることを示せ. ($p\mathbf{Z}$ は p の (負の数も含む) 倍数.)

2. $\{1, 2, \ldots, p-1\}$ は $G = (\mathbf{Z} \setminus p\mathbf{Z})/\sim$ の完全代表系であることを示せ.

3. $x \in \mathbf{Z} \setminus p\mathbf{Z}$ のとき
$$[x] = \{z \in \mathbf{Z} \setminus p\mathbf{Z} \mid z \sim x\}$$
と定義した. $[x]$ は G の元であるとみなせる. (参考: $[x]$ の集合としての G は考えにくいので普通は完全代表系の集合と G を同一視する.)
さて G の元 $[x]$, $[y]$ の積を $\mathbf{Z}$ のかけ算を用いて $[xy]$ で定義する. $\mathbf{Z}$ のかけ算が G の積を矛盾なく定義すること (well-defined) を示せ.

4. $p = 5$ の時に G の掛け算表を作成せよ.

1. (1) $x \sim x$ は明らか. (2) $x \sim y$ なら $y \sim z$ も明らか. (3) $x \sim y$, $y \sim z$ と仮定する. $x - y \in p\mathbf{Z}$, $y - z \in p\mathbf{Z}$ なので $x - z \in p\mathbf{Z}$ である. したがって $x \sim z$.

2. $i, j \in \{1, 2, \ldots, p-1\}$ に対して $i \neq j$ なら $i - j \notin p\mathbf{Z}$. つまり $i \not\sim j$. 次に $i \in \mathbf{Z} \setminus p\mathbf{Z}$ をとる. i を p でわった余りを i' とする. このとき $i \sim i'$ である. さらに i' は $\{1, 2, \ldots, p-1\}$ に属する. よって完全代表系の条件をみたす.

3. well-defined であることをいうには $x \sim x'$, $y \sim y'$ のとき $xy \sim x'y'$ をいえばよい. $x' = x + np$, $y' = y + mp$ と書けるので $x'y' = xy + (ny + mx + nm)p$. つまり $xy \sim x'y'$ である. よって well-defined.

4.

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1