問1.2

(0) $42 = 2 \times 3 \times 7$

(1) $\frac{6}{42} = \frac{1}{7}$　(2) $\frac{6}{42} = \frac{1}{7}$　(4) $\frac{12}{42} = \frac{2}{7}$　(6) $\frac{12}{42} = \frac{2}{7}$　(8) $\frac{2}{42} = \frac{1}{21}$

(3) $\mathrm{ord}(a) = 14$ であるから、$|\langle a \rangle| = 14$ となる。

$\langle a \rangle$ の部分群が存在するときラグランジュの定理より、その位数は、1, 2, 7, 14である。

よって、位数7の元は、存在するならば、$\langle a \rangle$ の中に含まれるため、$\langle a \rangle$ を探索すればよい。

(5), (7)　(3)と同様。

(9) $\mathrm{ord}(a) = 6$ であるから、$|\langle a \rangle| = 6$ である。

よって、ラグランジュの定理より、$\langle a \rangle$ の任意の部分群Gの位数は、6の約数であるから、$G \Rightarrow \forall b$ の位数は、6以下である。■

(10) 1. $U(\mathbb{Z}/42\mathbb{Z})$ より、元aをランダムにとる。

2. $\langle a \rangle$ を計算し、$7 \nmid |\langle a \rangle|$ であれば、1.へ。

3. $\mathrm{ord}(b) = 7$ なる $\langle a \rangle$ の b が見つかれば、bを出力する。

2.において、$\langle a \rangle$ の計算量は、

$\frac{1}{7} \times 6 + \frac{1}{7} \times 13 + \frac{2}{7} \times 20 + \frac{2}{7} \times 41 + \frac{1}{21} \times 5 + \frac{1}{21} \times 2 + \frac{1}{21} \times 1 + \frac{1}{21} \times 0 = \frac{431}{21}$

aを取りなおす確率は、$\frac{1}{7}$ だから、2.の計算量は、おおよそ、

$\frac{431}{21} \times \frac{7}{6} = \frac{431}{18}$　(2回以上同じ値をとるパターンは無視)

3.における計算量は、

aが取られる確率	$\lvert\langle a \rangle\rvert$	$\mathrm{ord}(b)=7$ なる $b \in \langle a \rangle$ が選ばれる確率	左列1bが見つかるまでの計算量
$\frac{2}{7}$	42	$\frac{1}{7}$	$\frac{431}{21} \times (42 \times \frac{1}{6})$
$\frac{2}{7}$	21	$\frac{1}{4}$	$(\frac{1}{4} \times 6 + \frac{1}{4} \times 13 + \frac{2}{4} \times 20) \times (42 \times \frac{1}{6})$
$\frac{1}{7}$	14	$\frac{1}{2}$	$(\frac{1}{2} \times 6 + \frac{1}{2} \times 13) \times (42 \times \frac{1}{2})$
$\frac{1}{7}$	7	1	0

であるから、

$$\frac{2}{7}\times\frac{431}{21}\times 42\times\frac{1}{6}+\frac{2}{7}\times\left(\frac{1}{4}\times 6+\frac{1}{4}\times 13+\frac{2}{4}\times 20\right)\times\left(42\times\frac{1}{4}\right)+\frac{1}{7}\times\left(\frac{1}{2}\times 6+\frac{1}{2}\times 13\right)\times\left(42\times\frac{1}{2}\right)+\frac{1}{7}\times 0$$

$$=\frac{862}{21}+\frac{1717}{4}+\frac{517}{2}$$

$$=\frac{3448}{84}+\frac{37117}{84}+\frac{2394}{84}$$

$$=\frac{9559}{84}$$

よって、合計の計算量は

$$\frac{431}{18}+\frac{9559}{84}=\frac{34711}{252}\simeq 137.7\ \text{回}\ //$$