問5.1

わかりませんでした。

H_nに対し、$\langle a_1, \cdots, a_k \rangle$が生成する群の要素数は、
$a_1, \cdots, a_k$の位数を$l_1, \cdots, l_k$としたとき、高々$l_1 \cdots l_k$個である。
$H_n \ni a_1$に対し、$|\langle a_1 \rangle| < |H_n|$ならば、生成群に$a_2$を追加する。
この操作を繰り返すと、$\langle a_1, \cdots, a_m \rangle = H_n$となる$a_1, \cdots, a_m$が存在する。この操作をすべての元の組み合わせ、$(a_1, a_2, \cdots)$で繰り返すと、目当てのnを求めることができる。
これにかかる時間は、$O(n \cdot {}_nC_4) = O(n^5)$程度である。
目当てのnが$n \sim 100$程度であるとすると、
$100^5 = 10^{10}$程度の計算量で決定できる。

問5-3

(1)

$(a_0+a_1x+a_2x^2+\cdots)^p$ を展開したとき、$x^{1\cdot e_1}x^{2\cdot e_2}\cdots x^{k\cdot e_k}$ の係数は、$e_1+\cdots+e_k=p$ なるば、$\dfrac{p!}{e_1!e_2!\cdots e_k!}$ となり、p が素数であれば、この値は、p の倍数もしくは1となる。係数が1となるのは、$\sum a_ix^i$ のある1つの項のみを p 乗したときであり、それ以外の場合は、$\mathbb{F}_p$ 上で0と等しくなる。また、フェルマーの小定理より $a^p\equiv a \pmod p$ となるから、

$\phi(f(x))=(\sum a_ix^i)^p=\sum a_i^px^{ip}=\sum a_ix^{ip}$

(2) $\mathbb{F}_p[x]\ni f(x)=\sum a_ix^i$, $g(x)=\sum b_ix^i$ とする。

(加法) $\phi(f(x)+g(x))=\phi(\sum a_ix^i+\sum b_ix^i)=\phi(\sum(a_i+b_i)x^i)$

$=\sum(a_i+b_i)^px^{ip}$

$=\sum a_i^px^{ip}+\sum b_i^px^{ip}$ ($\because$ 素数 p に対し、$p\mid {}_pC_k$ $(k=1,\cdots,p-1)$)

$=\sum a_ix^{ip}+\sum b_ix^{ip}$

$=\phi(f(x))+\phi(g(x))$

(乗法) $\phi(f(x))\phi(g(x))=(\sum a_ix^i)^p(\sum b_ix^i)^p$

$=(\sum a_ix^{ip})(\sum b_ix^{ip})$

$=\sum_{i=0}\left(\sum_{j+k=i}(a_jb_k \pmod p)\right)x^{ip}$

$=\sum_{i=0}\left(\sum_{j+k=i}(a_jb_k \pmod p)x^i\right)^p$

$=\left(\sum_{i=0}\left(\sum_{j+k=i}(a_jb_k \pmod p)x^i\right)^p\right)$

$=\phi(f(x)g(x))$ ■

(3) $\mathbb{F}_p[x]\ni f(x)=\sum a_ix^i$ に対し、$\exists a_i>0$ $(i\geq 1)$ なるば、x^p $(k\geq 1)$ の項が $\phi(f(x))=(\sum a_ix^i)^p$ に現れるから、$\forall a_i=0$ $(i\geq 1)$ である必要がある。よって、$\phi(f(x))=a_0^p=a_0$ であるから、$a_0=1$ である。

以上より、$\{f(x)\in\mathbb{F}_p[x]\mid\phi(f(x))=1\}=\{1\}$ である。

問5.4

(1) a_i, a_{i-1} は奇数だから k, l $(k>l\geq 0)$ を用いて,

$a_i = 2k+1$, $a_{i-1} = 2l+1$ と表せる.

$a_i - a_{i-1} = (2k+1) - (2l+1) = 2(k-l)$ となり, これは偶数である.

(2) a_{i-1} は奇数であるため, 素因数2をもたない.

$\therefore GCD(a_{i+1}, a_{i-1}) = GCD(a_{i+1}, a_{i-1})$

$= GCD(a_i - a_{i-1}, a_{i-1})$

$= GCD(a_i, a_{i-1})$ ■