1a product of three 4-cycles has sign $(-1)^3$, so is not even.

b $\sigma = (124356)$, so order 6

c 28102014 is divisible by 2 and by 3 (because of sum of decimal digits),
hence $28102019 \equiv 5 \bmod 6$,
so $\sigma^{28102014} = \sigma^5 = \sigma^{-1} = (165342)$

2a since $p \mid (2n)^4 + 1$, $p \nmid 2n$, so $\gcd(2n, p) = 1$,
so $2n \bmod p$ is a unit.

$(2n)^4 \equiv -1 \bmod p$,
hence $(2n)^8 \equiv 1 \bmod p$, so order divides 8,
and it does not divide 4 (as $(2n)^4 \equiv -1 \bmod p \neq 1 \bmod p$ (since p is odd))
so order $= 8$

2b $\#(\mathbb{Z}/p\mathbb{Z})^\times = p-1$,
so since we have an element of order 8,
$8 \mid p-1$ which means $p \equiv 1 \bmod 8$

2c There is one such prime, namely 17.
If $p_1, \dots, p_t$ are such primes,
consider $(2p_1 \cdots p_t)^2 + 1$,
and a prime divisor of it p
then $p \neq p_j$ $(1 \leq j \leq t)$
since $\gcd(p, 2p_1 \cdots p_t) = 1$ (see (a))
and $p \equiv 1 \bmod 8$ by (b)
So there are at least $t+1$ such primes, $\forall t$.
hence ∞ many ☺

3a

* $id = f_{1,0} \in N$ ✓
* for $f_{1,b} \in N$, its inverse is $f_{1,-b}$ which is also in N ✓
* $f_{1,b_1} \circ f_{1,b_2} = f_{1,b_1+b_2}$ hence the composition of elements in N is also in N

Hence $N \subset G$ is a subgroup ✓

normal:

the inverse of $f_{a,c} = f_{1,c} \circ f_{a,0}$ is

$$f_{a^{-1},0} \circ f_{1,-c},$$

and

$$f_{a,c} \circ f_{1,b} \circ f_{a^{-1},0} \circ f_{1,-c}$$

sends x to

$$x \mapsto x-c \mapsto a^{-1}x - a^{-1}c \mapsto a^{-1}x - a^{-1}c + b$$
$$\downarrow$$
$$x - c + ab + c$$

so this conjugation equals $f_{1,ab}$.

which shows $f_{a,c} N f_{a,c}^{-1} = N$

b. of course $HN \subset G$.

vice versa,

$f_{a,b} = f_{a,0} \circ f_{1,a^{-1}b}$ because $ax+b = a(x+a^{-1}b)$

so $G \subset HN$, hence $G = HN$

c. one of the isomorphism thms states $HN/N \simeq H/_{H \cap N}$.

in our case $H \cap N = \{id\}$ because if $f_{1,b} \in H$, then $b = f_{1,b}(0) = 0$.

Hence $G/N = HN/N \cong H/_{\{id\}} \cong H$. $H \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$, $f_{a,0} \mapsto a$ is evident.

4 a ⇒ : the algorithm transforms $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ to $\begin{pmatrix} d_1 & \\ & d_2 \end{pmatrix}$

"generated by only one element" means

either $r=1$ and no elementary divisors

so matrix $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

or $r=0$ and one (a zero) elementary divisor,

so matrix $\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$, $d>1$ or $d=1$

in both cases $\gcd(\text{entries}) = 1$,

and this gcd doesn't change during the algorithm.

⇐ : again, the gcd remains the same during the algorithm

so we must end with $\begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}$,

which results in a cyclic group $(\mathbb{Z}/*\mathbb{Z})$

b we look for the smallest $m>0$ with $m\cdot(1,0)+H = H$,

in other words, with $(m,0) \in H$.

$H = \{ (2a+4b,\ 2a+12b) \}$.

to have 2nd coord $=0$, must have $-6b=a$

that gives $\{(-8b, 0)\}$

we conclude: smallest $m>0$ is $\underline{\underline{m=8}}$.

c. $\begin{pmatrix} 2 & 4 \\ 2 & 12 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 \\ 0 & 8 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 \\ 0 & 8 \end{pmatrix}$

hence $r=0$ and elementary divisors $2, 8$.

5a 2 is prime and $2 \mid \#G$,

so Cauchy's thm says $\exists$ element of order 2.

b $g_1 \in G$ gives $\lambda_g(g_1) = gg_1$, $\lambda_g^2(gg_1) = g^2 g_1 = g_1$,

so 2-cycle $(g_1\ gg_1)$

continuing for all elements in G.

one obtains a product of m (disjoint) 2-cycles.

hence sign $(-1)^m = -1$ since m is odd

c $G \longrightarrow S_G \xrightarrow{\text{sign}} \{\pm 1\}$

$h \longmapsto \lambda_h = \text{mult by } h$ $(\tilde{g} \mapsto h\tilde{g})$

φ

the composition is a homomorphism φ,

and $\varphi(g) = -1$, so φ is surjective

$G = \underset{\downarrow 1}{\text{Ker}(\varphi)} \cup \underset{\text{disjoint}}{} g.\underset{\downarrow -1}{\text{Ker}(\varphi)}$

so $\text{Ker}(\varphi)$ is the desired subgp of index 2