(10pt total) # HW 6

(2pt) 1. Prop: If $g \in G$, $n = |G|$, then $g^n = e$.

Pf: Lagrange Thm: Subgroup $H \subset G$ has $|G| = |H|\ell$ for $\ell \in \mathbb{N}$.

For $H = \langle g \rangle$ cyclic subgroup, $k = |H|$, have $g^k = e$. But $n = |G| = |H|\ell = k\ell$, so $g^n = (g^k)^\ell = e^\ell = e$. QED

2a. Extended Eucl. Algor for 3 & 11 $\Rightarrow$ Bezout formula

$4(3) + (-1)(11) = 1$

(2pt) b. Isomorphism $T: C_3 \times C_{11} \longrightarrow C_{33}$

$\langle b \rangle$ $\quad$ $\langle c \rangle$ $\quad$ $\langle d \rangle$

$b^3 = e$ $\quad$ $c^{11} = e$ $\quad$ $d^{33} = e$

$T(b, e) = d^{11}$, $\quad$ $T(e, c) = d^3$ $\quad$ $T(b^i, c^j) = d^{11i + 3j}$

$(d^{11})^3 = e$ $\quad$ $(d^3)^{11} = e$

By Bezout $d^1 = d^{11(-1) + 3(4)} = T(b^{-1}, c^4) = T(b^2, c^4)$

Thus $d^k = T(b^2, c^4)^k = T(b^{2k}, c^{4k})$.

$T^{-1}(d^k) = (b^{2k}, c^{4k})$.

Alternative: $\tilde{T}^{-1}(d) = (b, c)$, $\tilde{T}^{-1}(d^k) = (b^k, c^k)$

Then $1 - 4(3) = (-1)(11) = -11$, $\quad 1 + 11 = 4(3) = 12$

so $\tilde{T}^{-1}(d^{-11}) = (b^{-11}, c^{-11}) = (b^{1 - 4(3)}, c^{(-1)11}) = (b, e)$

$\tilde{T}^{-1}(d^{12}) = (b^{12}, c^{12}) = (b^{4(3)}, c^{1+11}) = (e, c)$

$\tilde{T}(b, e) = d^{-11} = d^{22}$, $\quad \tilde{T}(e, c) = d^{12}$

$\tilde{T}(b^i, c^j) = d^{-11i + 12j} = d^{22i + 12j}$

(1pt) c. Generator $T^{-1}(d) = (b^2, c^4)$

(e, e), (b^2, c^4), $(b^4, c^8) = (b, c^8)$, ... 33 different powers.

or $\tilde{T}^{-1}(d) = (b, c) \Rightarrow (e, e), (b, c), (b^2, c^2), (b^3, c^4) = (b, c^4)$

Number of possible generators is $\varphi(33) = (3-1)(11-1) =$ 20

3a. $\mathbb{Z}_{11}^\times = \{1, 2, \ldots, 10\} \cong C_{10}$

(1pt) E.g. $\langle 2\rangle = \{1, 2, 4, 8, 16=5, 10, 20=9, 18=7, 14=3, 6\}$

Number of pass generators $\varphi(10) = (2-1)(5-1) = 4$.

i.e. $g = 2, 8, 7, 6$

b. $\mathbb{Z}_{15}^\times \cong C_2 \times C_4$ not C_8

(1pt) since: $\langle 2\rangle = \{1, 2, 4, 8\}$

$\langle 13\rangle = \langle -2\rangle = \{1, -2=13, 4, -8=7\}$

$\langle 11\rangle = \langle -4\rangle = \{1, -4=11\}$

$\langle 14\rangle = \langle -1\rangle = \{1, -1=14\}$

} elements of order 2, 4; no elements of order 8

In fact: $T: C_2 \times C_4 \to \mathbb{Z}_{15}^\times$

$(b, e) \mapsto -1 = 14$

$(e, c) \mapsto 2$

$(b^i, c^j) \mapsto (-1)^i 2^j$

4.a $n = 1147$, if not prime, must have prime factor $p \le \lfloor \sqrt{1147} \rfloor = 33$

(1pt) Try factors $p = \cancel{2}, \cancel{3}, \cancel{5}, \cancel{7}, \cancel{11}, \cancel{13}, \cancel{17}, \cancel{19}, \cancel{23}, \cancel{29}, 31$

$1147 = (31)(37)$

b. $\varphi(1147) = \varphi((31)(37)) = (30)(36) = 1080$

so $|\mathbb{Z}_{1147}^\times| = 1080$

(2pt) c. Euclidean Algor: $(491)(11) - (5)(1080) = 1$

$b \quad a$

d. $m = 2$, $m^a = 2^{11} = 2048 \equiv 901 \equiv -246 \pmod{1147}$

$(m^a)^b = (-246)^{491} \equiv 2 \pmod{1147}$

Wolfram Alpha: (-246)^491 mod 1147

For arithmetic computation techniques, see Terras p. 125-6