AC

Worksheet 2

1) a) $69 \cdot 73$

$69 = (1000101)_2$

1	$2^0 \cdot 73 = 73$	mod 1000
0	$2^1 \cdot 73 = 146$	mod 1000
1	$2^2 \cdot 73 = 256$	
0	$2^3 \cdot 73 = 584$	
0	$2^4 \cdot 73 = 168$	
0	$2^5 \cdot 73 = 338$	
1	$2^6 \cdot 73 = 672$	

mod 1000

How many additions?

$672 + 292 + 73 = 37 \mod 1000$

b) $2047 \cdot 7873$

$2048 = 2^{11}$

so we double 7873 11 times

then subtract 7879

(1)

2) a) yes

b) no

c) yes

d) yes → Does 2 mod 4 have an inverse?

e) yes

f) yes $\forall a \in F_p^* \quad a^{p-1} \equiv 1 \iff a \cdot a^{p-2} \equiv 1 \iff a^{-1} = a^{p-2}$

3) a) 4 is not a generator

$4^2 = 1 \mod 5$

b) 2 is a generator

$2^1 = 2$
$2^2 = 4$
$2^3 = 8$
$2^4 = 5$
$2^5 = 10$
$2^6 = 9$
$2^7 = 7$
$2^8 = 3$
$2^9 = 6$
$2^{10} = 1$

mod 11

c) $g = 5$ because it is a generator for F_{54}^* so it ~~tells the best about~~ gives the best information

A g/c

$7^a \equiv 1004 \mod 2593$

$g = 7$

$p = 2593$

$p-1 = 2592 = 2^5 \cdot 3^4$ ✓

$g_1 = 2 \quad e_1 = 5$

$g_2 = 3 \quad e_2 = 4$

$i = 1$

$a = a_0 + a_1 \cdot 2 + a_2 \cdot 4 + a_3 \cdot 8 + a_4 \cdot 16$

$(g^a)^{\frac{p-1}{g_1}} \equiv \left(g^{\frac{p-1}{g_1}}\right)^{a_0} \mod p$

$(7^a)^{\frac{2592}{2}} = \left(7^{\frac{2592}{2}}\right)^{a_0} \mod 2593$

$1 = \left(7^{\frac{2592}{2}}\right)^{a_0} \mod 2593$

$\Rightarrow a_0 = 0$ ✓ $\Leftrightarrow a \bmod 2 = 0$

$k = 1, 2, 3, 4 \qquad l_1 = 5$

$(g^a)^{\frac{p-1}{g_1^2}} = \left(g^{\frac{p-1}{g_1}}\right)^{a_0 + a_1} \cdot \left(g^{\frac{p-1}{g_1}}\right)^{a_1} \mod p$

$(7^a)^{\frac{2592}{4}} \equiv \left(7^{\frac{2592}{4}}\right)^{a_0} \cdot \left(7^{\frac{2592}{2}}\right)^{a_1} \mod 2593$

$1004^{648} \equiv 7^{1296 a_1}$

$1 \Rightarrow a_1 = 0$ ✓

$i = 2$

$(g^a)^{\frac{p-1}{g_2^3}} \equiv \left(g^{\frac{p-1}{g_2}}\right)^{a_0 + 2a_1} \cdot \left(g^{\frac{p-1}{g_2}}\right)^{a_2} \mod p$

$(7^a)^{\frac{2592}{9}} \equiv \left(7^{\frac{2592}{3}}\right)^{a_0 + 2a_1} \cdot \left(g^{\frac{2592}{3}}\right)^{a_2} \mod 2593$

$1004^{324} \equiv \left(7^{324}\right)^{a_0} \cdot 7^{1296 a_2} \mod 2593$

$1 \equiv 1 \cdot 7^{1296 a_2}$

$a_0 = 0$ ✓
$a_1 = 0$ ✓
$a_2 = 0$ ✓
$a_3 = 0$ ✓
$a_4 = 0$

$a = 0 \mod 32$

because 1004^{81} is 1 and each a_i is 0

$a = 0 \mod 32$

$a_0 \bmod 3 = ?$

$a = a_0 + a_1 \cdot 3 + a_2 \cdot 3^2 + a_3 \cdot 3^3$

$\left(7^9\right)^{\frac{2592}{3}} \equiv \left(7^{\frac{2592}{3}}\right)^{a_0} \bmod 25$

$1004^{864} \equiv 7^{864\, a_0} \bmod 25$

$1455 \equiv 1137^{a_0} \bmod 25$

$\Rightarrow a_0 = 2$ ✓ $\quad a \bmod 3 = 2$

$k = 1, 2, 3 \qquad a_2 = 4$

$k=1$

$\left(g^a\right)^{\frac{p-1}{3^2}} \equiv \left(g^{\frac{p-1}{3^2}}\right)^{a_0} \cdot \left(g^{\frac{p-1}{3}}\right)^{a_1}$

$(1004)^{288} \equiv 7^{288 \cdot 2} \cdot 7^{864\, a_1}$ (576)

$512 \equiv 7^{576 + 864\, a_1}$

$a_1 = 0 \quad 576$

$a_1 = 1 \quad 1440$ ✓ $\Rightarrow$ $a_1 = 1$ ✓

~~$a \bmod 3 = 1$~~

$k = 2$

$(1004)^{\frac{2592}{27}} \equiv \left(7^{\frac{2592}{27}}\right)^{a_0 + 3a_1} \cdot \left(7^{\frac{2592}{3}}\right)^{a_2}$

$1004^{96} \equiv 7^{96 a_0 + 3 \cdot 36 a_1 + 864 a_2} \bmod 25$

$1317 = 7^{96 \cdot 2 + 3 \cdot 96 + 864 a_2}$

$a_2 = 0 \quad 480$

$a_2 = 1 \quad 480 + 864 = 1344$

$a_2 = 2 \quad 480 + 864 + 864$

$\Rightarrow a_2 = 1$ ✓

$\Rightarrow$ ~~$a \bmod 27 = 4$~~

$k = 3$

$(1004)^{\frac{2592}{81}} \equiv \left(7^{\frac{2592}{81}}\right)^{a_0 + 3a_1 + 9a_2} \cdot \left(7^{\frac{2592}{3}}\right)^{a_3} \bmod 25$

$1004^{32} \equiv \left(7^{32}\right)^{2 + 3 + 9} \cdot 7^{864 a_3} \bmod 25$

$314 \equiv 7^{32 \cdot 14 + 864 a_3}$

$a_3 = 0 \quad 448$

$a_3 = 1 \quad 448 + 864 = 1312$

$a_3 = 2 \quad 2176$

$a_3 = 2$ ✓

$\Rightarrow$ ~~$a \bmod 81 = 71$~~

$7^a = 1004 \mod 2533$

$a \mod 32 = 0$

$a \mod 81 = 68$

$32y + 81x = 1$

$x = -15$

$y = 38$

$\Rightarrow \quad a = 32 \cdot 68 \cdot 38 + (-15) \cdot 0 \cdot 81 \mod 2532$

$a = 2336$

Really good stuff!

5) $g * f = f * g$ cause G is a group

$f(g * h, s) = f(g, f(h, s))$

$f(h * g, s) = f(h, f(g, s))$

$\Rightarrow$