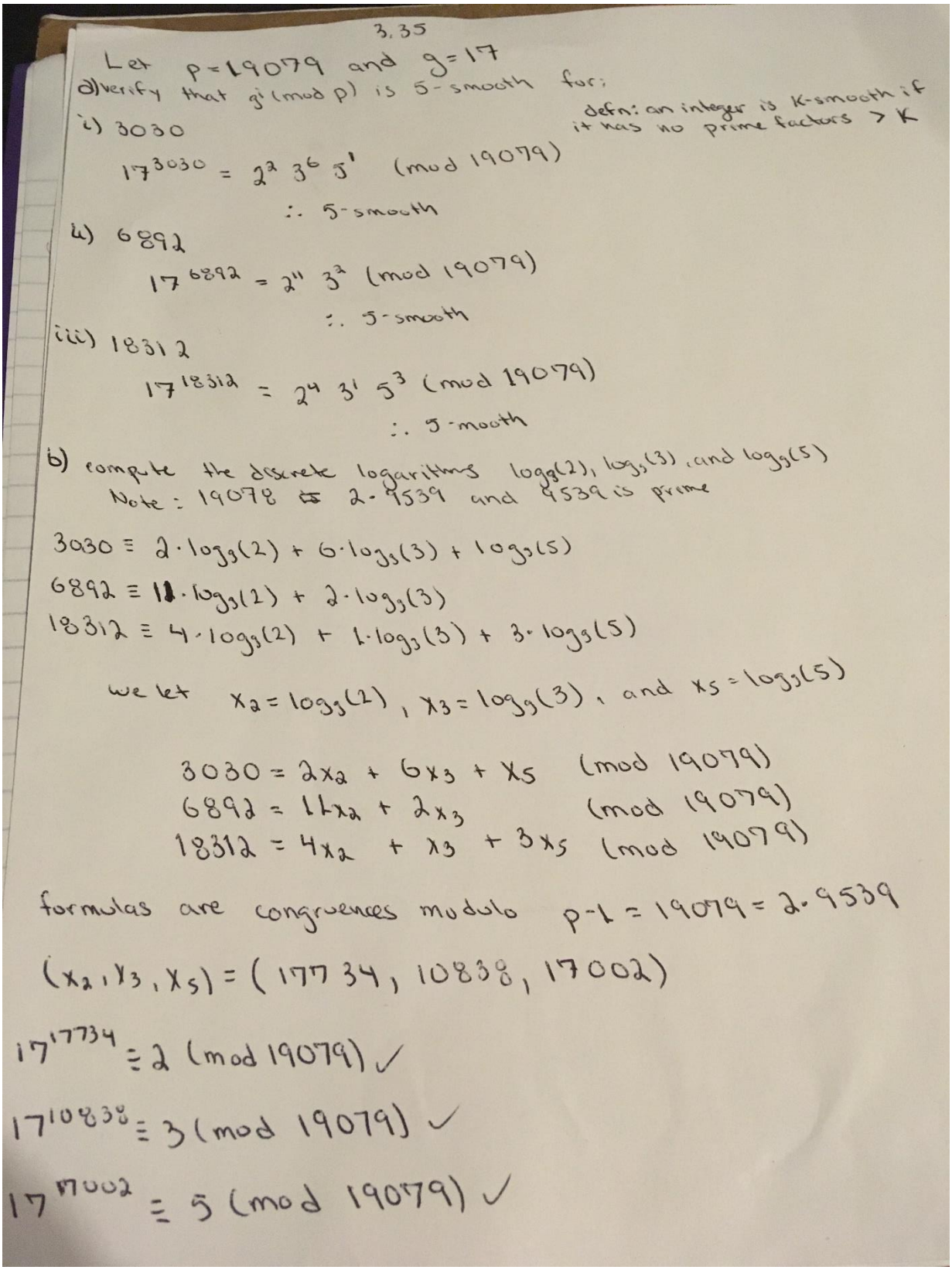
Group 2: Kyle, Jesus, Mason, Ying, Adam, Gage, Connor

Homework 7 – Group 2



3.35

Let $p = 19079$ and $g = 17$

a) Verify that $g^i \pmod p$ is 5-smooth for:

defn: an integer is K-smooth if it has no prime factors $> K$

i) 3030

$17^{3030} = 2^2 3^6 5^1 \pmod{19079}$

$\therefore$ 5-smooth

ii) 6892

$17^{6892} = 2^{11} 3^3 \pmod{19079}$

$\therefore$ 5-smooth

iii) 18312

$17^{18312} = 2^4 3^1 5^3 \pmod{19079}$

$\therefore$ 5-smooth

b) compute the discrete logarithms $\log_3(2)$, $\log_3(3)$, and $\log_3(5)$

Note: $19078 = 2 \cdot 9539$ and 9539 is prime

$3030 \equiv 2 \cdot \log_3(2) + 6 \cdot \log_3(3) + 1 \log_3(5)$

$6892 \equiv 11 \cdot \log_3(2) + 2 \cdot \log_3(3)$

$18312 \equiv 4 \cdot \log_3(2) + 1 \cdot \log_3(3) + 3 \cdot \log_3(5)$

we let $x_2 = \log_3(2)$, $x_3 = \log_3(3)$, and $x_5 = \log_3(5)$

$3030 = 2x_2 + 6x_3 + x_5 \pmod{19079}$

$6892 = 11x_2 + 2x_3 \pmod{19079}$

$18312 = 4x_2 + x_3 + 3x_5 \pmod{19079}$

formulas are congruences modulo $p - 1 = 19079 = 2 \cdot 9539$

$(x_2, x_3, x_5) = (17734, 10838, 17002)$

$17^{17734} \equiv 2 \pmod{19079}$ ✓

$17^{10838} \equiv 3 \pmod{19079}$ ✓

$17^{17002} \equiv 5 \pmod{19079}$ ✓

Group 2: Kyle, Jesus, Mason, Ying, Adam, Gage, Connor

c) verify that $19 \cdot 17^{-12400}$ is 5-smooth

$19 \cdot 17^{-12400} \equiv 2^{7} \cdot 3^{1} \pmod{19079}$

384

d) solve the logarithm problem $17^{\lambda} \equiv 19 \pmod{19079}$ using the values of the discrete logs of 2, 3, and 5 this yields

[redacted] $17^{13830} \equiv$ [redacted] $19 \pmod{19079}$ ✓

Group 2: Kyle, Jesus, Mason, Ying, Adam, Gage, Connor

3.38

a.) $b^2 \equiv a^{\frac{p+1}{2}} \equiv a^{1+\left(\frac{p-1}{2}\right)} \equiv a * \left(\frac{a}{p}\right)$ $\left(since\ a\ is\ a\ quadratic\ residue\ it\ means \frac{a}{p} = 1\right)$

this means that it would be ≡ a mod p which satisfies the proof.

b.) i.) a = 116 , p = 587

$116^{\left(\frac{587+1}{4}\right)} \equiv 116^{147} \equiv 65\ mod\ 587. So\ we\ check\ 65^2 mod\ 587\ which\ is\ in\ fact\ \equiv to\ 116\ mod\ 587$

ii.) a = 3217, p = 8672

$3217^{\left(\frac{8672+1}{4}\right)} \equiv 3217^{2157} \equiv 2980\ mod\ 8627. So\ we\ check\ 2980^2 mod\ 8672\ which\ is\ in\ fact$
$\equiv to\ 3217\ mod\ 8672$

III.) a = 9109, p = 10663

$9109^{\left(\frac{10663+1}{4}\right)} \equiv 9109^{2666} \equiv 3502\ mod\ 10663.$

So we check 3502^2 mod 587 actually equals 1554 mod 10663.This means that this is not a quadratic residue modulo of 10663. However you can see that 3502^2 mod 10663 is actually equal to -9109 mod 10663.

3.41

a) N = 1842338473, a = 1532411781

$$\left(\frac{1794677960}{32411}\right) = \left(\frac{16068}{32411}\right) = \left(\frac{2}{32411}\right)^2 \left(\frac{3}{32411}\right)\left(\frac{13}{32411}\right)\left(\frac{103}{32411}\right)$$
$$= (-1)^2 \left(\frac{3}{32411}\right)\left(\frac{13}{32411}\right)\left(\frac{103}{32411}\right) = -\left(\frac{32411}{3}\right)\left(\frac{32411}{13}\right) * -\left(\frac{32411}{103}\right)$$
$$= -\left(\frac{2}{3}\right)\left(\frac{2}{13}\right) * -\left(\frac{69}{103}\right) = -(-1)(-1) * -\left(\left(\frac{3}{103}\right)\left(\frac{23}{103}\right)\right)$$
$$= -(-1)(-1) * -\left(-\left(\frac{103}{3}\right) * -\left(\frac{103}{23}\right)\right) = -(-1)(-1) * -\left(\left(\frac{-1}{3}\right) * -\left(\frac{11}{23}\right)\right)$$
$$= -(-1)(-1) * -\left((-1) * -\left(-\left(\frac{23}{11}\right)\right)\right) = -(-1)(-1) * -\left((-1) * -\left(\frac{-1}{11}\right)\right)$$
$$= -(-1)(-1) * -\big((-1) * -(-1)\big) = \mathbf{-1}$$

Since the ciphertext is not a quadratic residue to p then **plaintext = 1**

Group 2: Kyle, Jesus, Mason, Ying, Adam, Gage, Connor

$$\left(\frac{5257334818}{32411}\right) = \left(\frac{28398}{32411}\right) = \left(\frac{2}{32411}\right)\left(\frac{3}{32411}\right)\left(\frac{4733}{32411}\right) = (-1) * -\left(\frac{32411}{3}\right)\left(\frac{32411}{4733}\right)$$
$$= (-1) * -\left(\frac{2}{3}\right)\left(\frac{4013}{4733}\right) = (-1) * -(-1)\left(\frac{4733}{4013}\right) = (-1) * -(-1)\left(\frac{720}{4013}\right)$$
$$= (-1) * -(-1)\left(\left(\frac{2}{4013}\right)^4\left(\frac{3}{4013}\right)^2\left(\frac{5}{4013}\right)\right)$$
$$= (-1) * -(-1)\left((-1)^4\left(\frac{4013}{3}\right)^2\left(\frac{4013}{5}\right)\right) = (-1) * -(-1)\left((-1)^4\left(\frac{2}{3}\right)^2\left(\frac{3}{5}\right)\right)$$
$$= (-1) * -(-1)\left((-1)^4(-1)^2\left(\frac{5}{3}\right)\right) = (-1) * -(-1)\left((-1)^4(-1)^2\left(\frac{2}{3}\right)\right)$$
$$= (-1) * -(-1)\left((-1)^4(-1)^2(-1)\right) = \mathbf{1}$$

The ciphertext is a quadratic residue to p so **plaintext = 0**

$$\left(\frac{420526487}{32411}\right) = \left(\frac{23173}{32411}\right) = \left(\frac{7}{32411}\right)\left(\frac{3739}{32411}\right) = -\left(\frac{32411}{7}\right) * -\left(\frac{32411}{3739}\right) = \left(-\frac{1}{7}\right) * -\left(\frac{2499}{3739}\right)$$
$$= (-1) * \left(\left(\frac{3}{3739}\right)\left(\frac{7}{3739}\right)^2\left(\frac{17}{3739}\right)\right) = (-1) * \left(-\left(\frac{3739}{3}\right)\left(\frac{-3739}{7}\right)^2\left(\frac{3739}{17}\right)\right)$$
$$= (-1) * \left(\left(\frac{-1}{3}\right)\left(\frac{-1}{7}\right)^2\left(\frac{16}{17}\right)\right) = (-1) * \left((-1)(-1)^2\left(\frac{2}{17}\right)^4\right)$$
$$= (-1) * \left(\left(\frac{-1}{3}\right)\left(\frac{-1}{7}\right)^2(1)^4\right) = -\mathbf{1}$$

The cipher text is not a quadratic residue to p so **plaintext = 1**

b) N = 3149, a = 2013

N = pq = 47*67

$$\left(\frac{2322}{47}\right) = \left(\frac{19}{47}\right) = -\left(\frac{47}{19}\right) = -\left(\frac{9}{19}\right) = -\left(\frac{3}{19}\right)^2 = -\left(-\frac{19}{3}\right)^2 = -\left(-\frac{1}{3}\right)^2 = -(-1)^2 = -\mathbf{1}$$

The cipher text is not a quadratic residue to p so **plaintext = 1**

$$\left(\frac{719}{47}\right) = \left(\frac{14}{47}\right) = \left(\frac{2}{47}\right)\left(\frac{7}{47}\right) = (1) * -\left(\frac{47}{7}\right) = (1) * -\left(\frac{5}{7}\right) = (1) * -\left(\frac{7}{5}\right) = (1) * -\left(\frac{2}{5}\right)$$
$$= (1) * -(-1) = \mathbf{1}$$

The ciphertext is a quadratic residue to p so **plaintext = 0**

$$\left(\frac{202}{47}\right) = \left(\frac{14}{47}\right) = 1$$

The ciphertext is a quadratic residue to p so **plaintext = 0**

Group 2: Kyle, Jesus, Mason, Ying, Adam, Gage, Connor

c) N = 781044643, a = 568980706

r =705130839, m = 1

$$c = 568980706 * 705130839^2 \equiv 517254876 \bmod N$$

C = 517254876

r = 631364468, m = 1

$$c = 568980706 * 631364468^2 \equiv 4308279 \bmod N$$

C = 4308279

r = 67651321, m = 0

$$c = 67651321^2 \equiv 660699010 \bmod N$$

C =660699010