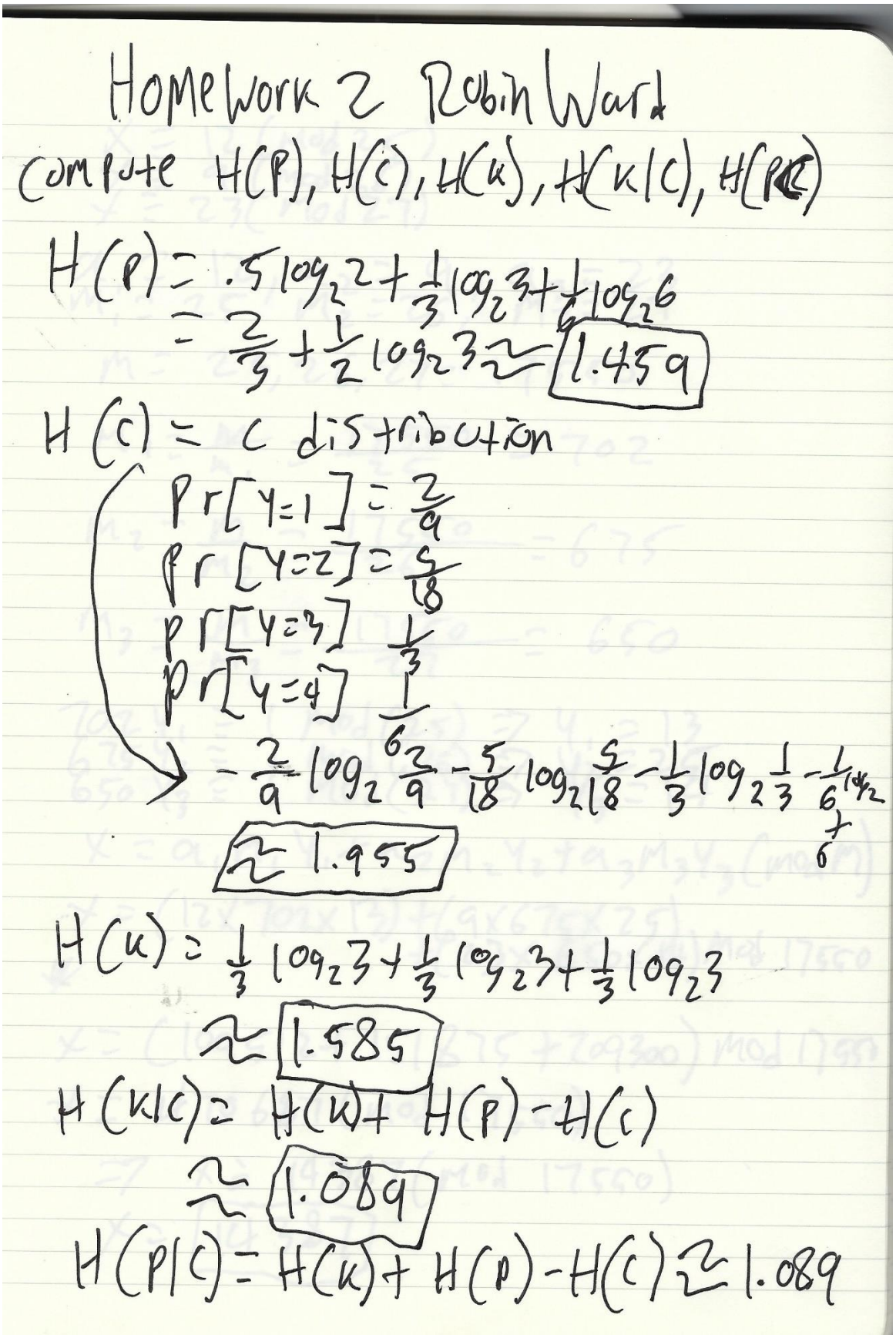
HOMEWORK 2

ROBIN WARD

COMP 7376

3/11/2020

1.


Homework 2 Robin Ward
compute H(P), H(C), H(K), H(K|C), H(P|C)
H(P) = .5 log2 2 + 1/3 log2 3 + 1/6 log2 6
= 2/3 + 1/2 log2 3 ≈ 1.459
H(C) = C distribution
Pr[Y=1] = 2/9
Pr[Y=2] = 5/18
Pr[Y=3] 1/3
Pr[Y=4] 1/6
- 2/9 log2 2/9 - 5/18 log2 5/18 - 1/3 log2 1/3 - 1/6 log2 1/6
≈ 1.955
H(K) = 1/3 log2 3 + 1/3 log2 3 + 1/3 log2 3
≈ 1.585
H(K|C) = H(K) + H(P) - H(C)
≈ 1.089
H(P|C) = H(K) + H(P) - H(C) ≈ 1.089

2.

$x \equiv 12 \pmod{25}$
$x \equiv 9 \pmod{26}$
$x \equiv 23 \pmod{27}$

$a_1 = 12, a_2 = 9, a_3 = 23$
$m_1 = 25, m_2 = 26, m_3 = 27$

$m = 25, 26, 27 = 17550$

$M_1 = \frac{m}{m_1} = \frac{17550}{25} = 702$

$M_2 = \frac{m}{m_2} = \frac{17550}{26} = 675$

$M_3 = \frac{m}{m_3} = \frac{17550}{27} = 650$

$702 y_1 \equiv 1 \pmod{25} \Rightarrow y_1 = 13$
$675 y_2 \equiv 1 \pmod{26} \Rightarrow y_2 = 25$
$650 y_3 \equiv 1 \pmod{27} \Rightarrow y_3 = 14$

$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod{m}$

$x = (12 \times 702 \times 13) + (9 \times 675 \times 25) + (23 \times 650 \times 14) \bmod 17550$

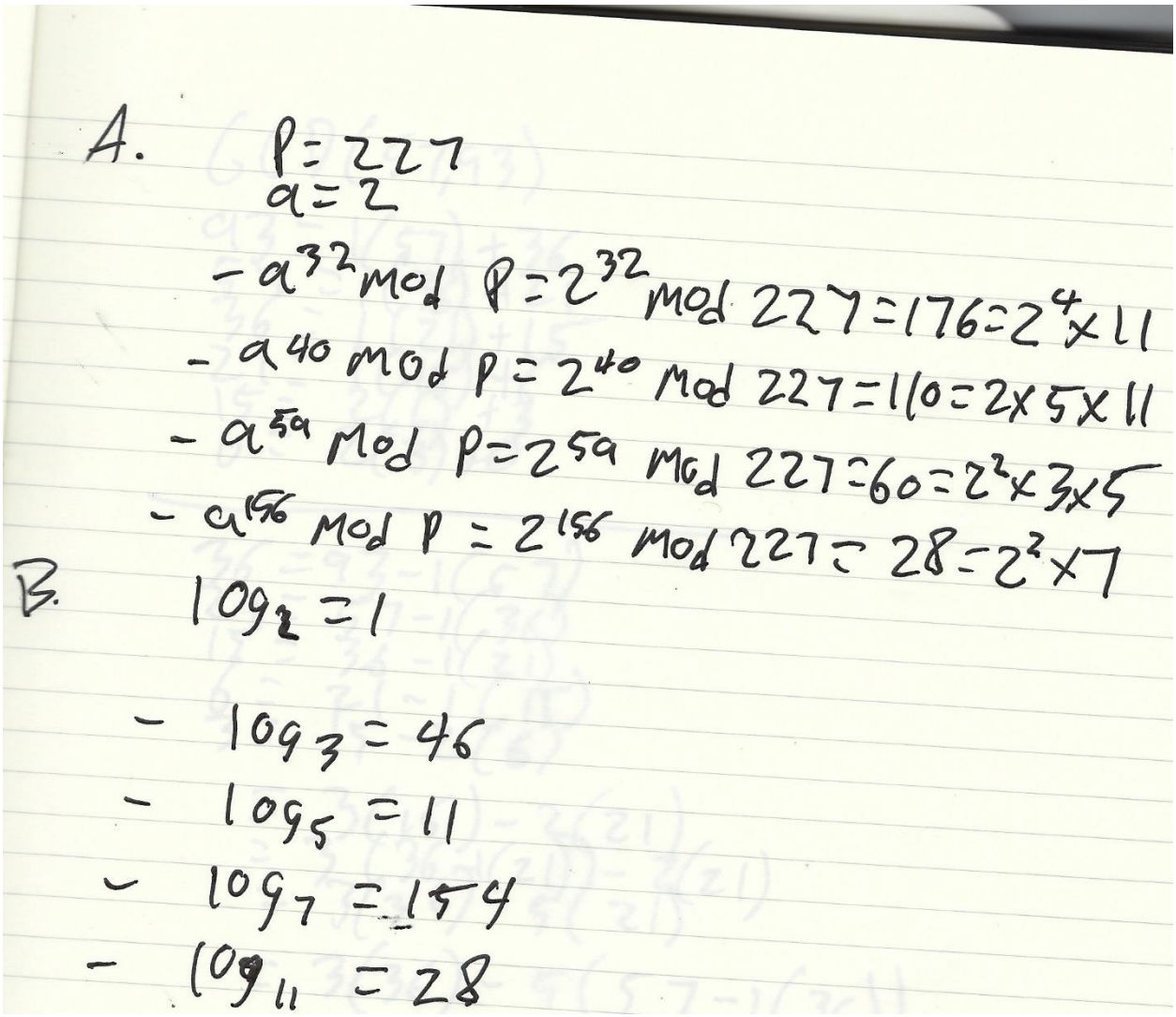
$x = (109512 + 151875 + 209300) \bmod 17550$

$x = 470687 \pmod{17550}$

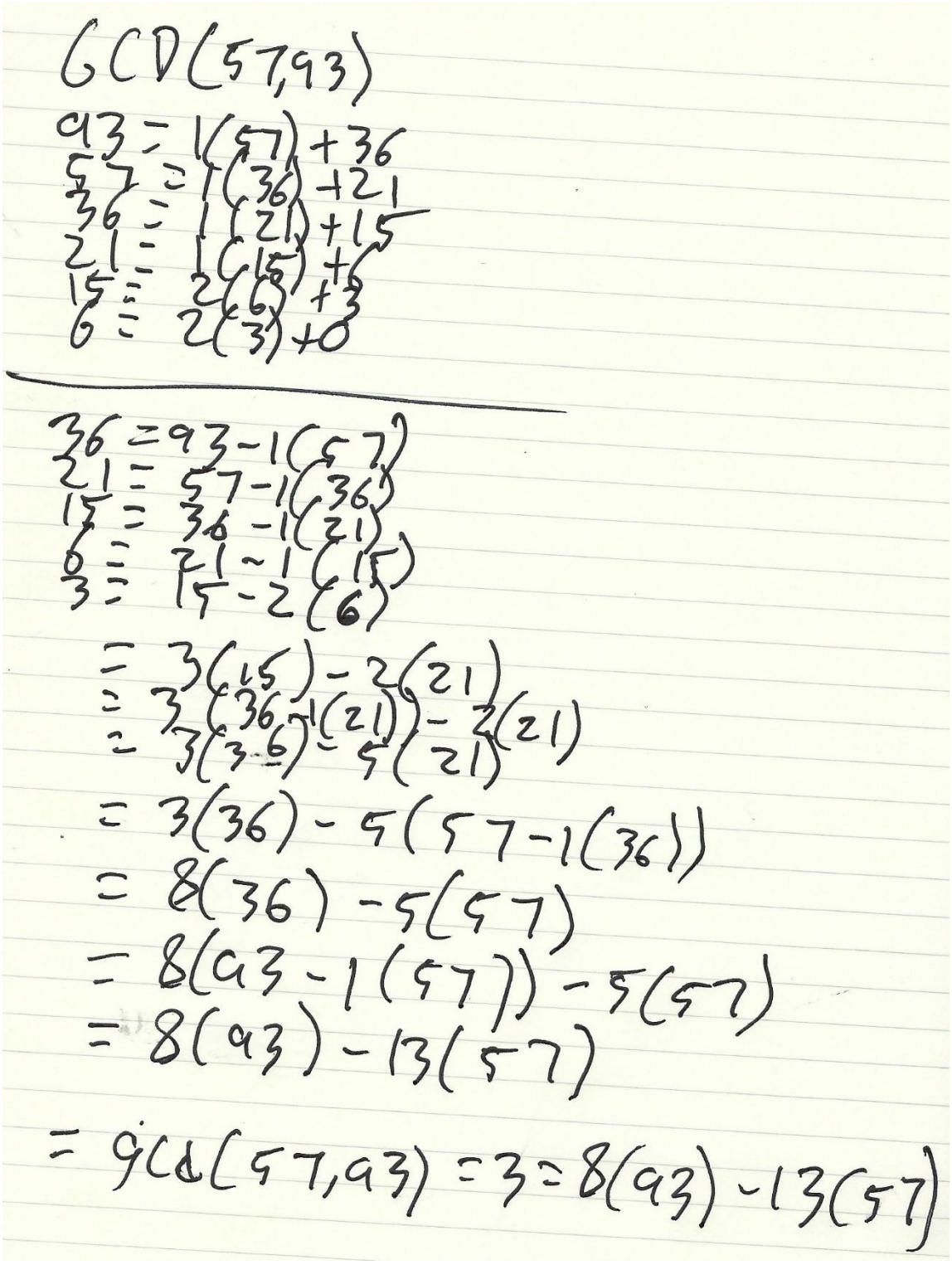
$\Rightarrow x \equiv 14387 \pmod{17550}$

$x = \boxed{14387}$

3.


A.
p = 227
a = 2
- $a^{32} \bmod p = 2^{32} \bmod 227 = 176 = 2^4 \times 11$
- $a^{40} \bmod p = 2^{40} \bmod 227 = 110 = 2 \times 5 \times 11$
- $a^{59} \bmod p = 2^{59} \bmod 227 = 60 = 2^2 \times 3 \times 5$
- $a^{156} \bmod p = 2^{156} \bmod 227 = 28 = 2^2 \times 7$
B.
$\log_2 = 1$
- $\log_3 = 46$
- $\log_5 = 11$
- $\log_7 = 154$
- $\log_{11} = 28$

4.


GCD(57,93)
93 = 1(57) + 36
57 = 1(36) + 21
36 = 1(21) + 15
21 = 1(15) + 6
15 = 2(6) + 3
6 = 2(3) + 0
36 = 93 - 1(57)
21 = 57 - 1(36)
15 = 36 - 1(21)
6 = 21 - 1(15)
3 = 15 - 2(6)
= 3(15) - 2(21)
= 3(36 - 1(21)) - 2(21)
= 3(36) - 5(21)
= 3(36) - 5(57 - 1(36))
= 8(36) - 5(57)
= 8(93 - 1(57)) - 5(57)
= 8(93) - 13(57)
= GCD(57,93) = 3 = 8(93) - 13(57)