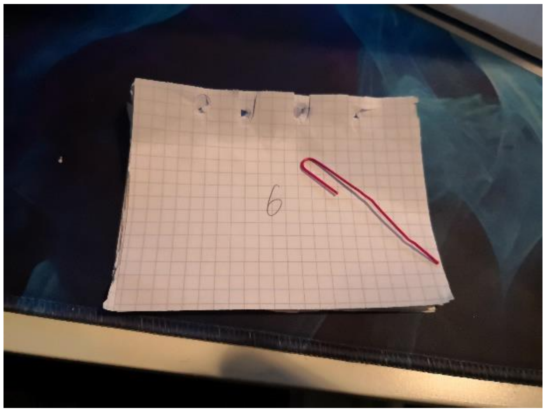
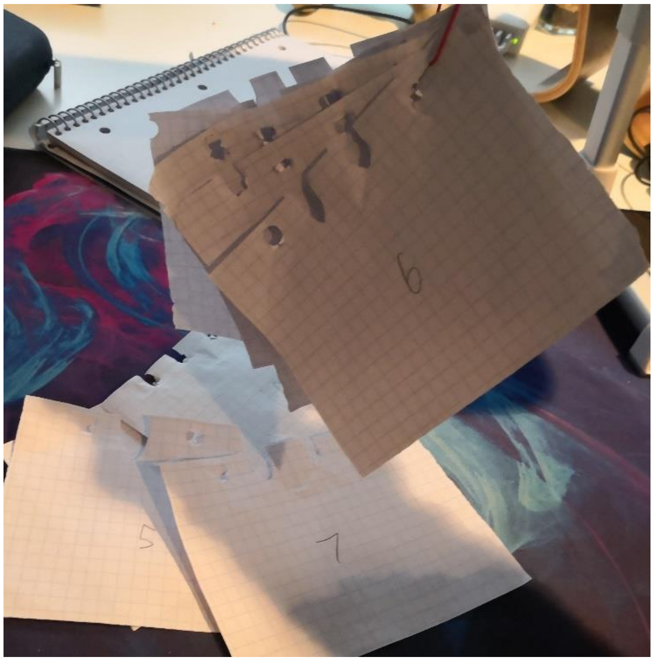
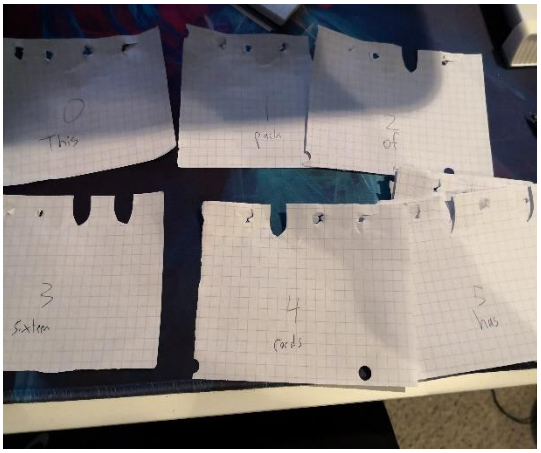
Theo Shin – Number Theory and Primes Problem Set
HW Week 7

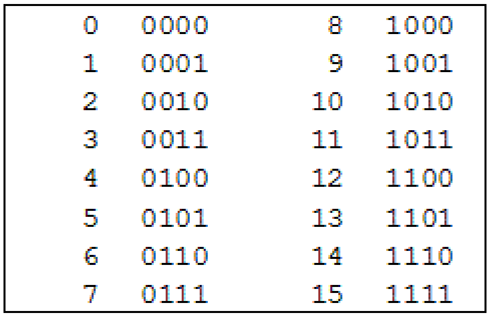
1.







The self-sorting cards use binary numbers in base two (0,1) to represent digits to 15 in this case.

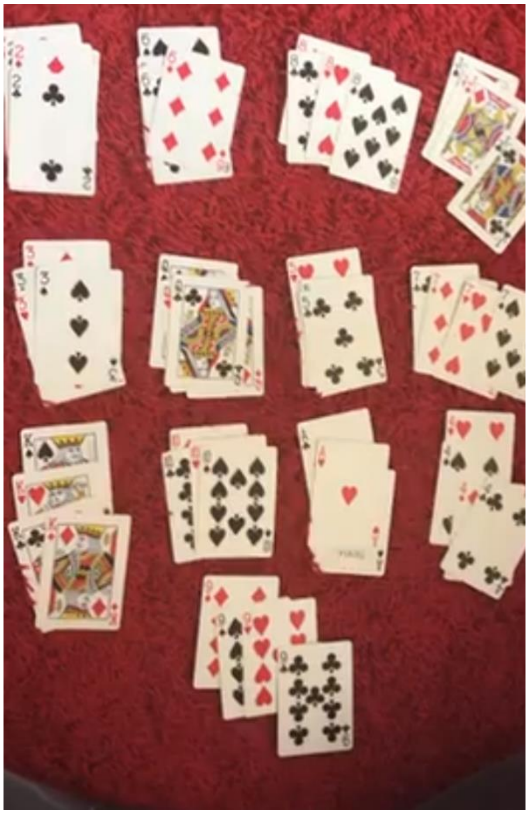


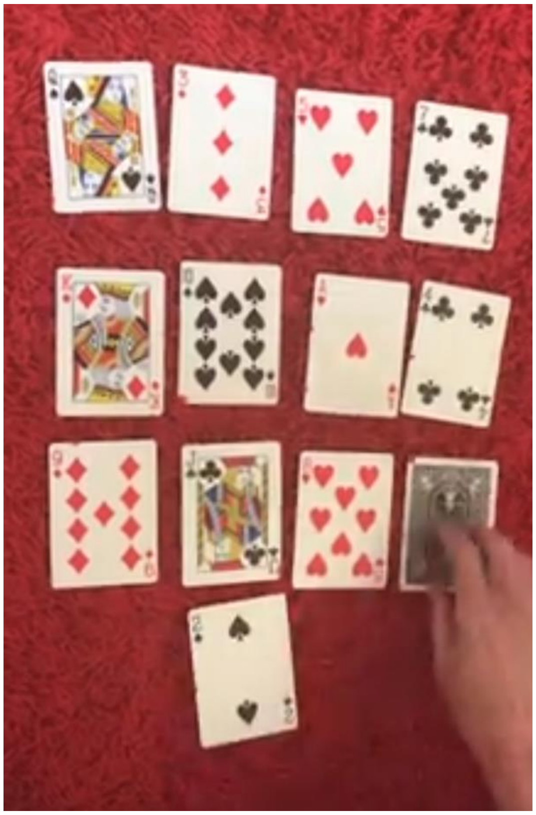
0	0000	8	1000
1	0001	9	1001
2	0010	10	1010
3	0011	11	1011
4	0100	12	1100
5	0101	13	1101
6	0110	14	1110
7	0111	15	1111

With 5 holes per card, the binary sort system could sort up to number 27 (16,8,4,2,1) or 28 cards including the 0 card. And if each card had 10 holes, it could sort up to number 1,023 or 1,024 cards (512,256,128,64,32,16,8,4,2,1). It could be sorted in 10 steps through the same method of using the paperclip to "drop" the cards with the groove cut out where the binary digit 1 is occupied (from right to left).

Theo Shin – Number Theory and Primes Problem Set
HW Week 7

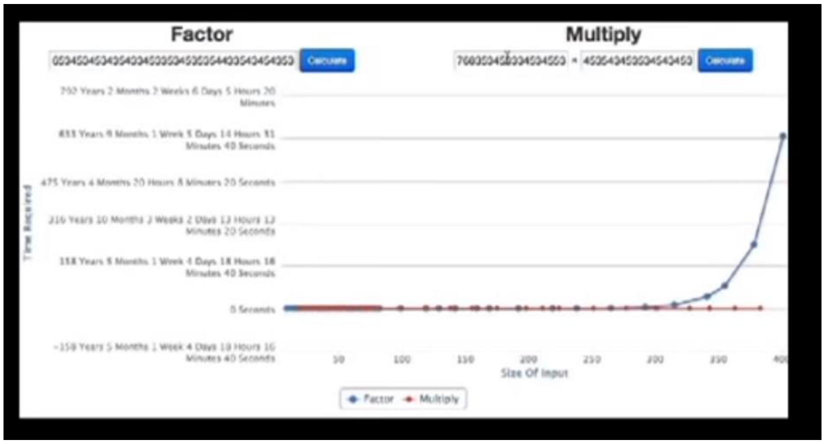
2. By revealing the first 12 (in the video, showing the Q ♣ but not the 9♦) you could deduct the last card was a 9, however, the suit would remain unclear. By observing the screenshots below of the card trick setup and the result, the pattern goes [2,6,8,J,3,Q,5,7,K,10,A,4,9]. So, we know the 9 will be followed by cards from the first row as the cycle repeats with some combination of [2,5,8,J]. The remaining rows we can memorize as [3,Q,5,7] and [K,10,A,4] (*coincidentally, the [K,10,A,4] came out exactly the same). Every 4th card (right-most) in the row could be left face down for a reveal since a distinct row corresponds to the same 4 cards and with each card in the row representing a suit, we could deduct the exact card and suit. However, if you only needed to know the one card left unturned (the card with your hand on top of) you could leave the first 8 cards or top 2 rows face down. You must turn over the first three cards in each row and the lone card at the bottom for a total of 10 to predict how the cycle of cards played out.



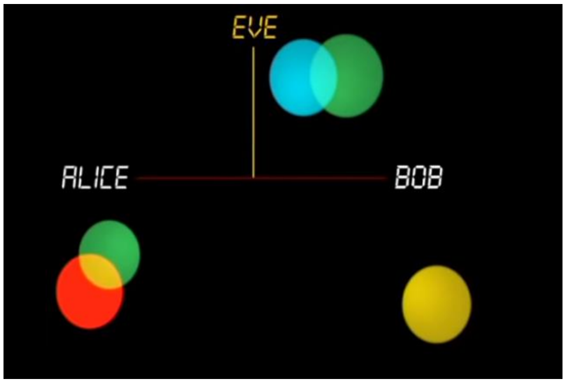


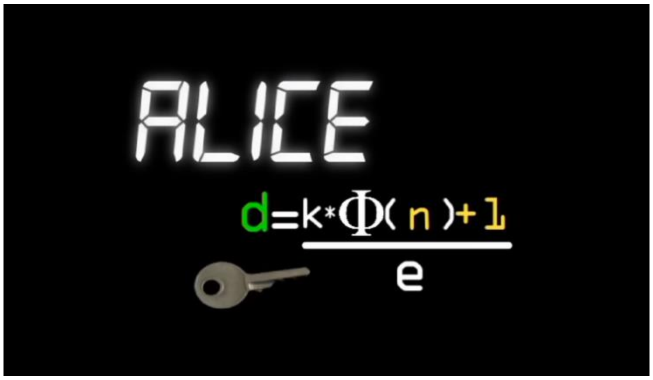
Theo Shin – Number Theory and Primes Problem Set
HW Week 7

3. RSA (Rivest-Shamir-Adleman; the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman) is the most widely used public key algorithm used and the most copied software in history. I didn't realize RSA algorithms were used to set up network security and to verify cryptocurrency transactions and find it amazingly clever how the system/algorithm became implemented. Most notably (as seen in image) we can see observe why RSA algorithms are so effectively implemented as the complexity of the private key grows, the time constraint to solve for the private key grows enormously.



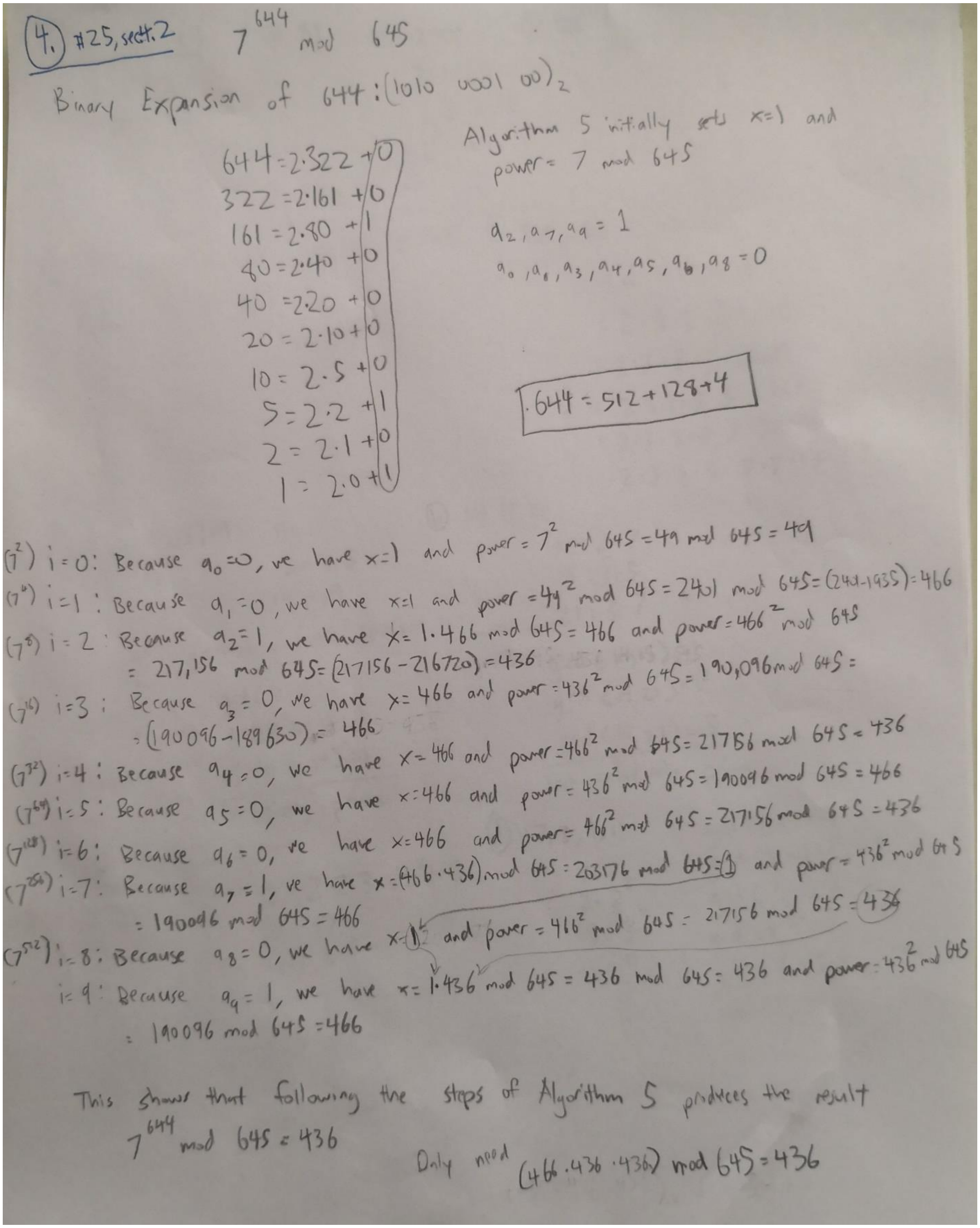
It's remarkable how the concept was expounded from using complementary colors of lights where the private key (red from image below) is used to decrypt Bob's message and developed into the equivalent formula shown to the right.





Theo Shin – Number Theory and Primes Problem Set
HW Week 7

4. From section 4.2 exercises, do #25 by hand



4. #25, sect4.2 $7^{644} \bmod 645$

Binary Expansion of 644: $(1010\ 0001\ 00)_2$

$644 = 2\cdot 322 + 0$
$322 = 2\cdot 161 + 0$
$161 = 2\cdot 80 + 1$
$80 = 2\cdot 40 + 0$
$40 = 2\cdot 20 + 0$
$20 = 2\cdot 10 + 0$
$10 = 2\cdot 5 + 0$
$5 = 2\cdot 2 + 1$
$2 = 2\cdot 1 + 0$
$1 = 2\cdot 0 + 1$

Algorithm 5 initially sets $x=1$ and power $= 7 \bmod 645$

$a_2, a_7, a_9 = 1$

$a_0, a_1, a_3, a_4, a_5, a_6, a_8 = 0$

$\boxed{644 = 512+128+4}$

(7^2) $i=0$: Because $a_0=0$, we have $x=1$ and power $= 7^2 \bmod 645 = 49 \bmod 645 = 49$

(7^4) $i=1$: Because $a_1=0$, we have $x=1$ and power $= 49^2 \bmod 645 = 2401 \bmod 645 = (2401-1935) = 466$

(7^8) $i=2$: Because $a_2=1$, we have $x = 1\cdot 466 \bmod 645 = 466$ and power $= 466^2 \bmod 645$ $= 217{,}156 \bmod 645 = (217156-216720) = 436$

(7^{16}) $i=3$: Because $a_3=0$, we have $x=466$ and power $= 436^2 \bmod 645 = 190{,}096 \bmod 645 =$ $(190096-189630) = 466$

(7^{32}) $i=4$: Because $a_4=0$, we have $x=466$ and power $= 466^2 \bmod 645 = 217156 \bmod 645 = 436$

(7^{64}) $i=5$: Because $a_5=0$, we have $x=466$ and power $= 436^2 \bmod 645 = 190096 \bmod 645 = 466$

(7^{128}) $i=6$: Because $a_6=0$, we have $x=466$ and power $= 466^2 \bmod 645 = 217156 \bmod 645 = 436$

(7^{256}) $i=7$: Because $a_7=1$, we have $x = (466\cdot 436) \bmod 645 = 203176 \bmod 645 = \boxed{1}$ and power $= 436^2 \bmod 645$ $= 190096 \bmod 645 = 466$

(7^{512}) $i=8$: Because $a_8=0$, we have $x=\boxed{1}$ and power $= 466^2 \bmod 645 = 217156 \bmod 645 = \boxed{436}$

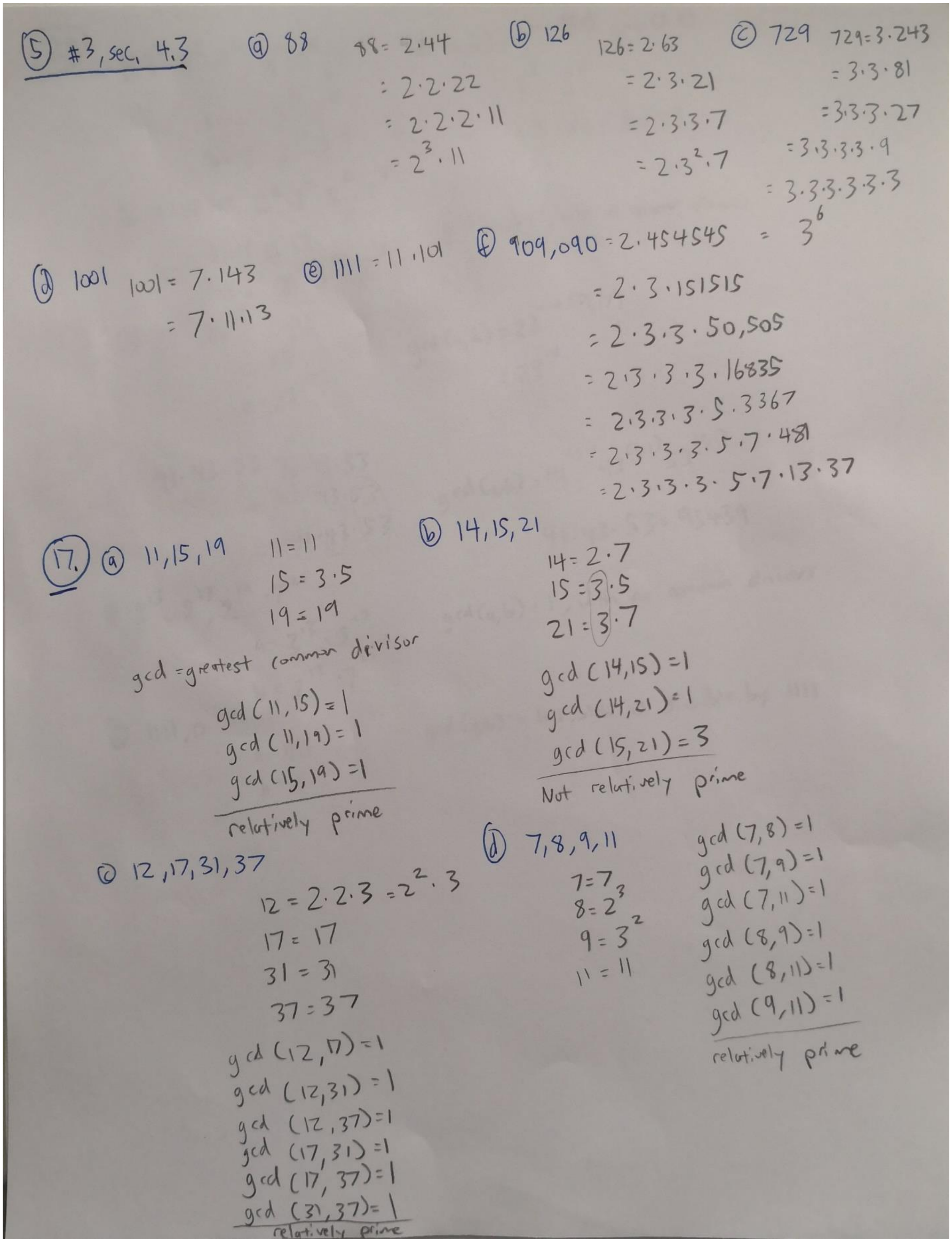
$i=9$: Because $a_9=1$, we have $x = 1\cdot 436 \bmod 645 = 436 \bmod 645 = 436$ and power $= 436^2 \bmod 645$ $= 190096 \bmod 645 = 466$

This shows that following the steps of Algorithm 5 produces the result
$7^{644} \bmod 645 = 436$

Only need $(466\cdot 436\cdot 436) \bmod 645 = 436$

Theo Shin – Number Theory and Primes Problem Set
HW Week 7

5. From section 4.3 #3, #17



(5) #3, sec, 4.3

(a) 88

$88 = 2\cdot 44$
$= 2\cdot 2\cdot 22$
$= 2\cdot 2\cdot 2\cdot 11$
$= 2^3\cdot 11$

(b) 126

$126 = 2\cdot 63$
$= 2\cdot 3\cdot 21$
$= 2\cdot 3\cdot 3\cdot 7$
$= 2\cdot 3^2\cdot 7$

(c) 729

$729 = 3\cdot 243$
$= 3\cdot 3\cdot 81$
$= 3\cdot 3\cdot 3\cdot 27$
$= 3\cdot 3\cdot 3\cdot 3\cdot 9$
$= 3\cdot 3\cdot 3\cdot 3\cdot 3\cdot 3$
$= 3^6$

(d) 1001

$1001 = 7\cdot 143$
$= 7\cdot 11\cdot 13$

(e) $1111 = 11\cdot 101$

(f) $909{,}090 = 2\cdot 454545$
$= 2\cdot 3\cdot 151515$
$= 2\cdot 3\cdot 3\cdot 50{,}505$
$= 2\cdot 3\cdot 3\cdot 3\cdot 16835$
$= 2\cdot 3\cdot 3\cdot 3\cdot 5\cdot 3367$
$= 2\cdot 3\cdot 3\cdot 3\cdot 5\cdot 7\cdot 481$
$= 2\cdot 3\cdot 3\cdot 3\cdot 5\cdot 7\cdot 13\cdot 37$

(17.) (a) 11, 15, 19

$11 = 11$
$15 = 3\cdot 5$
$19 = 19$

gcd = greatest common divisor

gcd (11, 15) = 1
gcd (11, 19) = 1
gcd (15, 19) = 1

relatively prime

(b) 14, 15, 21

$14 = 2\cdot 7$
$15 = 3\cdot 5$
$21 = 3\cdot 7$

gcd (14, 15) = 1
gcd (14, 21) = 1
gcd (15, 21) = 3

Not relatively prime

(c) 12, 17, 31, 37

$12 = 2\cdot 2\cdot 3 = 2^2\cdot 3$
$17 = 17$
$31 = 31$
$37 = 37$

gcd (12, 17) = 1
gcd (12, 31) = 1
gcd (12, 37) = 1
gcd (17, 31) = 1
gcd (17, 37) = 1
gcd (31, 37) = 1

relatively prime

(d) 7, 8, 9, 11

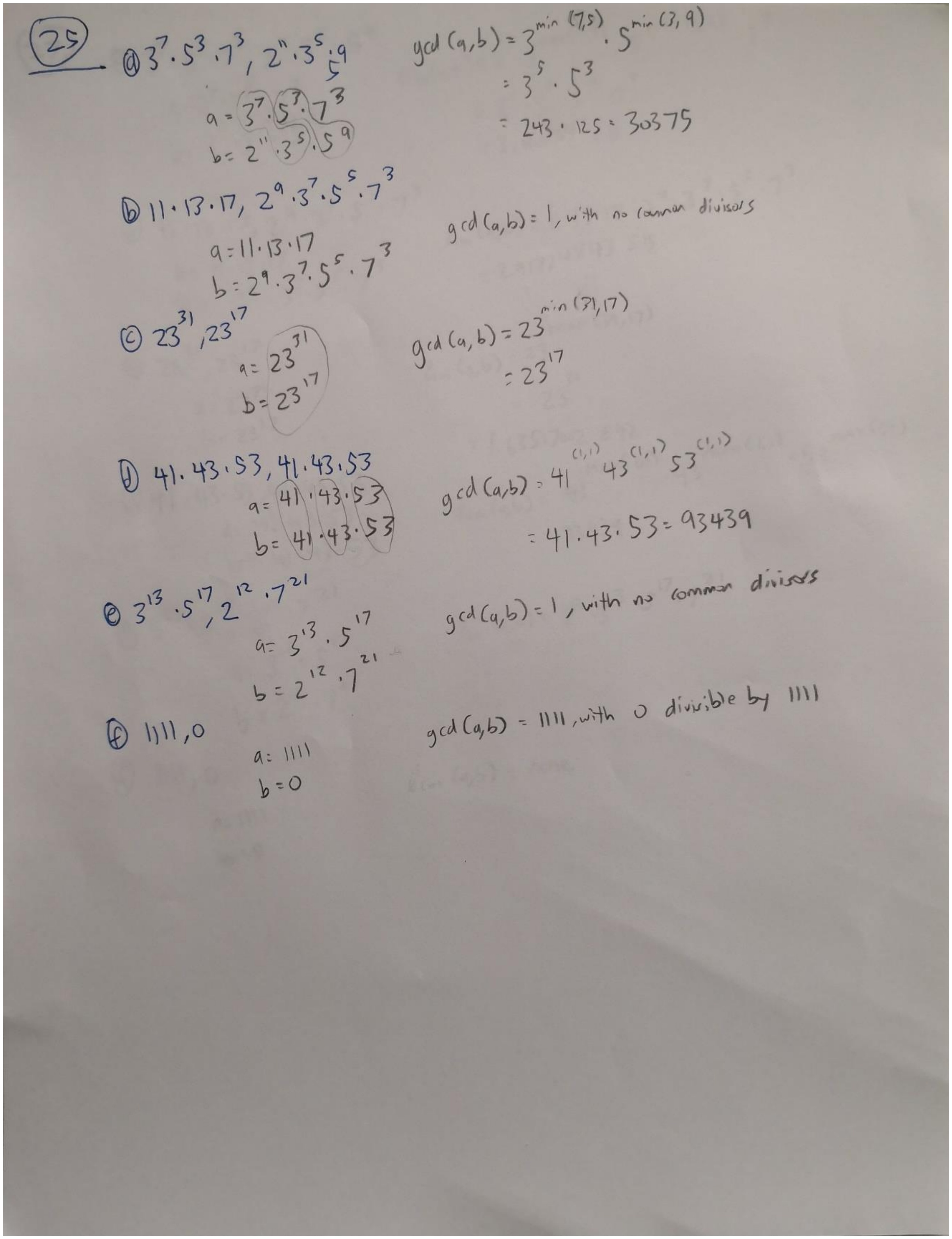
$7 = 7$
$8 = 2^3$
$9 = 3^2$
$11 = 11$

gcd (7, 8) = 1
gcd (7, 9) = 1
gcd (7, 11) = 1
gcd (8, 9) = 1
gcd (8, 11) = 1
gcd (9, 11) = 1

relatively prime

Theo Shin – Number Theory and Primes Problem Set
HW Week 7

From section 4.3 #25



25

(a) $3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9$

$a = 3^7 \cdot 5^3 \cdot 7^3$
$b = 2^{11} \cdot 3^5 \cdot 5^9$

$\gcd(a,b) = 3^{\min(7,5)} \cdot 5^{\min(3,9)}$
$= 3^5 \cdot 5^3$
$= 243 \cdot 125 = 30375$

(b) $11 \cdot 13 \cdot 17, 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$

$a = 11 \cdot 13 \cdot 17$
$b = 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$

$\gcd(a,b) = 1$, with no common divisors

(c) $23^{31}, 23^{17}$

$a = 23^{31}$
$b = 23^{17}$

$\gcd(a,b) = 23^{\min(31,17)}$
$= 23^{17}$

(d) $41 \cdot 43 \cdot 53, 41 \cdot 43 \cdot 53$

$a = 41 \cdot 43 \cdot 53$
$b = 41 \cdot 43 \cdot 53$

$\gcd(a,b) = 41^{(1,1)} 43^{(1,1)} 53^{(1,1)}$
$= 41 \cdot 43 \cdot 53 = 93439$

(e) $3^{13} \cdot 5^{17}, 2^{12} \cdot 7^{21}$

$a = 3^{13} \cdot 5^{17}$
$b = 2^{12} \cdot 7^{21}$

$\gcd(a,b) = 1$, with no common divisors

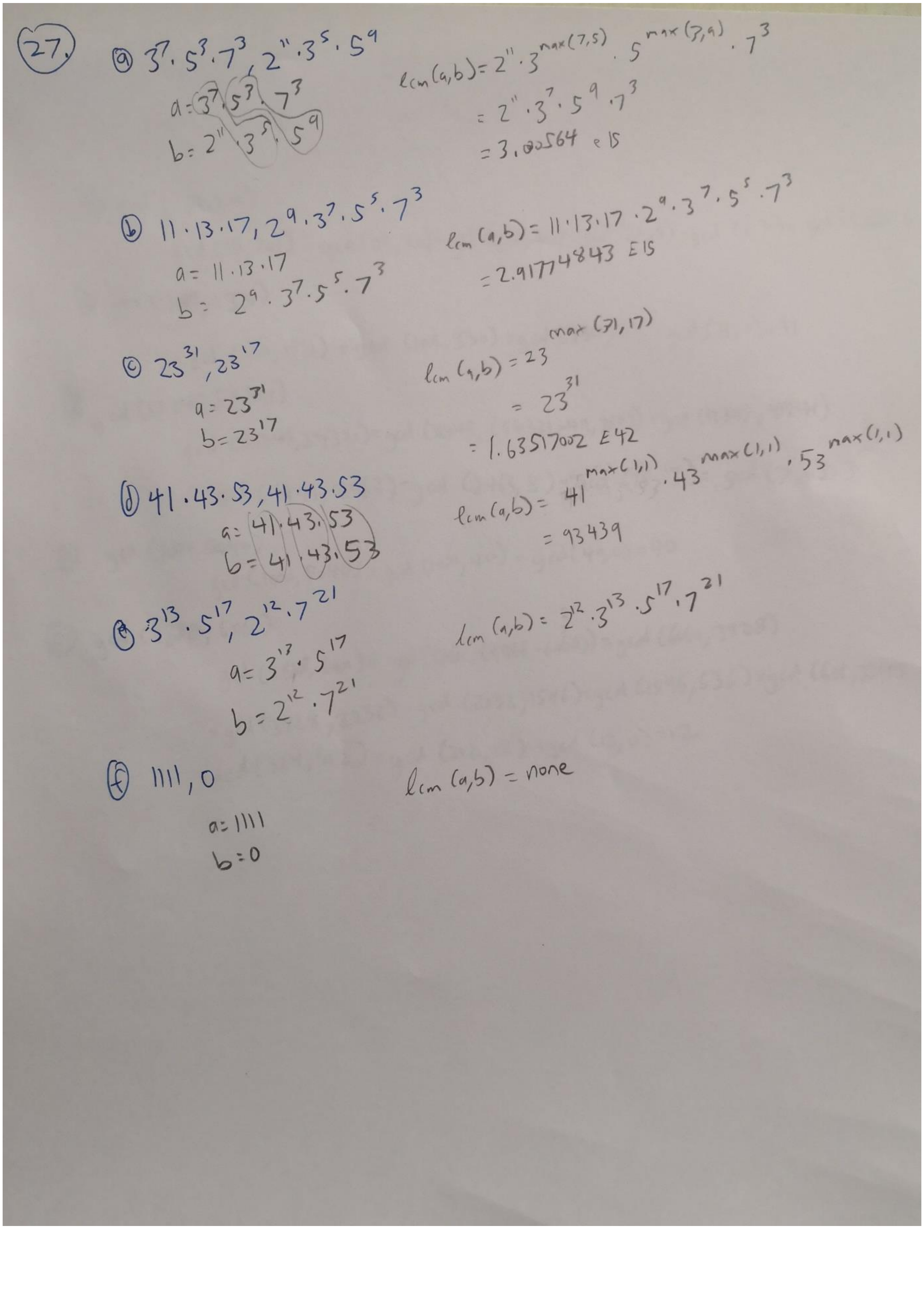
(f) 1111, 0

$a = 1111$
$b = 0$

$\gcd(a,b) = 1111$, with 0 divisible by 1111

Theo Shin – Number Theory and Primes Problem Set
HW Week 7

From section 4.3 #27



27.

a) $3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9$

$a = 3^7 \cdot 5^3 \cdot 7^3$

$b = 2^{11} \cdot 3^5 \cdot 5^9$

$lcm(a,b) = 2^{11} \cdot 3^{max(7,5)} \cdot 5^{max(3,9)} \cdot 7^3$

$= 2^{11} \cdot 3^7 \cdot 5^9 \cdot 7^3$

$= 3.00564\ e\ 15$

b) $11 \cdot 13 \cdot 17, 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$

$a = 11 \cdot 13 \cdot 17$

$b = 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$

$lcm(a,b) = 11 \cdot 13 \cdot 17 \cdot 2^9 \cdot 3^7 \cdot 5^5 \cdot 7^3$

$= 2.91774843\ E15$

c) $23^{31}, 23^{17}$

$a = 23^{31}$

$b = 23^{17}$

$lcm(a,b) = 23^{max(31,17)}$

$= 23^{31}$

$= 1.63517002\ E42$

d) $41 \cdot 43 \cdot 53, 41 \cdot 43 \cdot 53$

$a = 41 \cdot 43 \cdot 53$

$b = 41 \cdot 43 \cdot 53$

$lcm(a,b) = 41^{max(1,1)} \cdot 43^{max(1,1)} \cdot 53^{max(1,1)}$

$= 93439$

e) $3^{13} \cdot 5^{17}, 2^{12} \cdot 7^{21}$

$a = 3^{13} \cdot 5^{17}$

$b = 2^{12} \cdot 7^{21}$

$lcm(a,b) = 2^{12} \cdot 3^{13} \cdot 5^{17} \cdot 7^{21}$

f) $1111, 0$

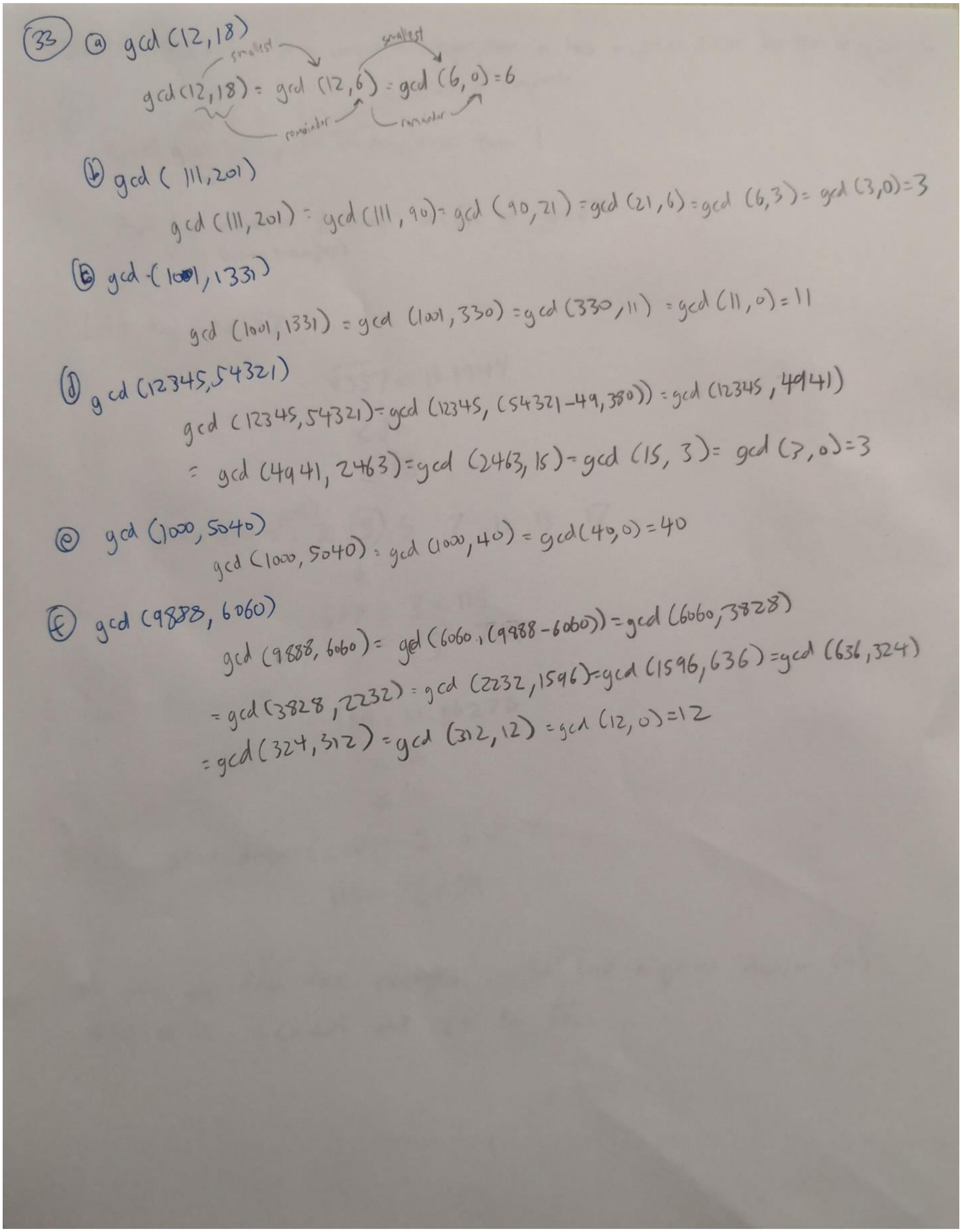
$a = 1111$

$b = 0$

$lcm(a,b) = none$

Theo Shin – Number Theory and Primes Problem Set
HW Week 7

6. From section 4.3 exercises, do #33 by hand



㉝ ⓐ gcd (12, 18)

smallest smallest

gcd (12, 18) = gcd (12, 6) = gcd (6, 0) = 6

remainder remainder

ⓑ gcd (111, 201)

gcd (111, 201) = gcd (111, 90) = gcd (90, 21) = gcd (21, 6) = gcd (6, 3) = gcd (3, 0) = 3

ⓒ gcd (1001, 1331)

gcd (1001, 1331) = gcd (1001, 330) = gcd (330, 11) = gcd (11, 0) = 11

ⓓ gcd (12345, 54321)

gcd (12345, 54321) = gcd (12345, (54321 − 49,380)) = gcd (12345, 4941)

= gcd (4941, 2463) = gcd (2463, 15) = gcd (15, 3) = gcd (3, 0) = 3

ⓔ gcd (1000, 5040)

gcd (1000, 5040) = gcd (1000, 40) = gcd (40, 0) = 40

ⓕ gcd (9888, 6060)

gcd (9888, 6060) = gcd (6060, (9888 − 6060)) = gcd (6060, 3828) = gcd (636, 324)

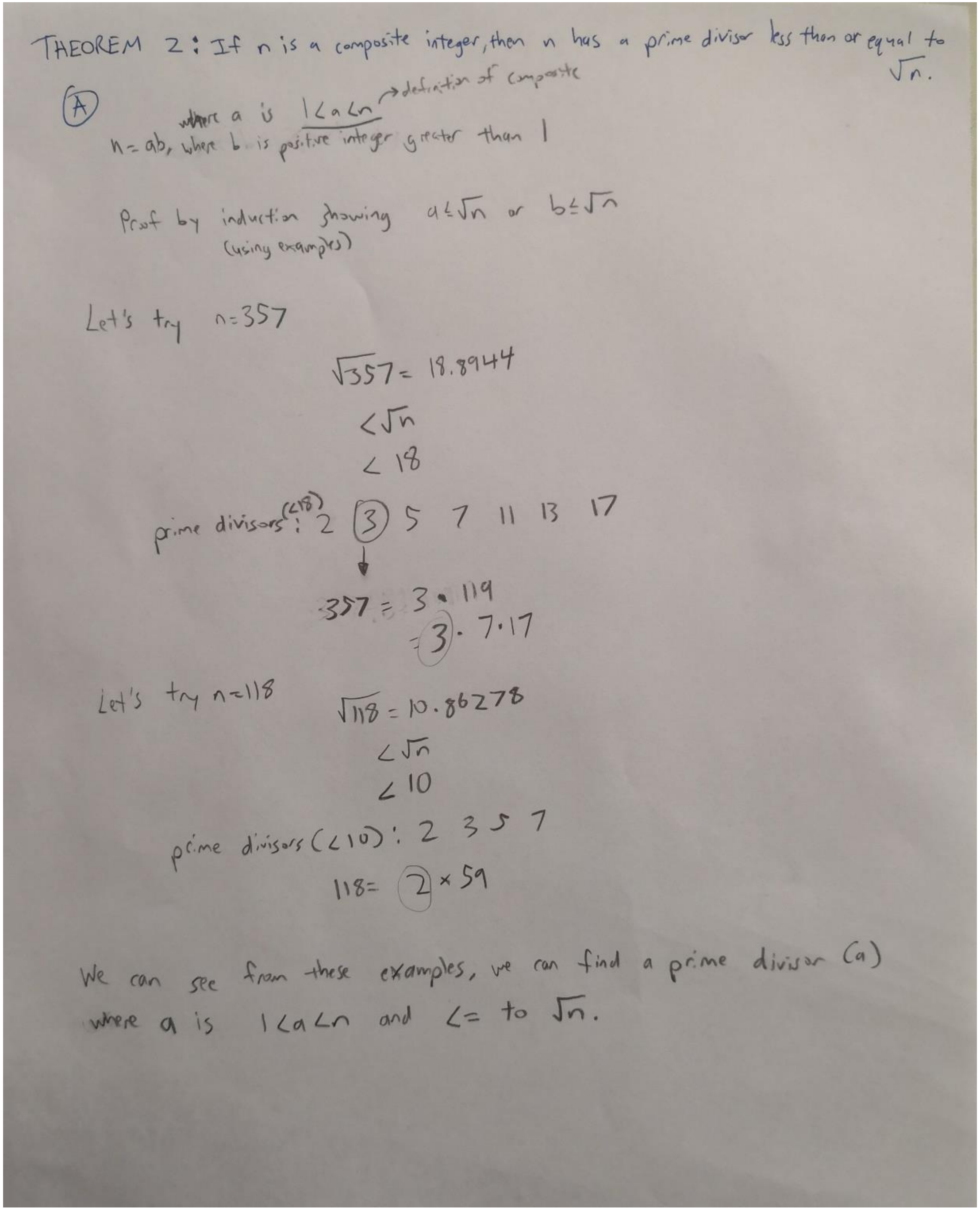
= gcd (3828, 2232) = gcd (2232, 1596) = gcd (1596, 636)

= gcd (324, 312) = gcd (312, 12) = gcd (12, 0) = 12

Theo Shin – Number Theory and Primes Problem Set
HW Week 7

7. A. Theorem 2 induction proof and examples

Base Step: lowest prime value n=2
Induction Step: Assume n = k+1 where k+1 is prime then k+1 has no prime divisor and is its own prime factorization. If k+1 is not prime then n = a * b ⇒ k+1 = a * b where integers a and b are 1<a<k+1 and 1<b<k+1. As shown in theorem 3 (p.260) a and b can be written as a = $p_1,p_2…p_n$ and b = $q_1,q_2…q_n$ where we know there will always be a larger prime integer. Therefore, k+1 can also be factored into prime numbers.



THEOREM 2: If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

(A)

where a is $1<a<n$ → definition of composite
n = ab, where b is positive integer greater than 1

Proof by induction showing $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$
(using examples)

Let's try n=357

$\sqrt{357} = 18.8944$

$< \sqrt{n}$

< 18

prime divisors (<18): 2 3 5 7 11 13 17

$357 = 3 \cdot 119$

$= 3 \cdot 7 \cdot 17$

Let's try n=118 $\sqrt{118} = 10.86278$

$< \sqrt{n}$

< 10

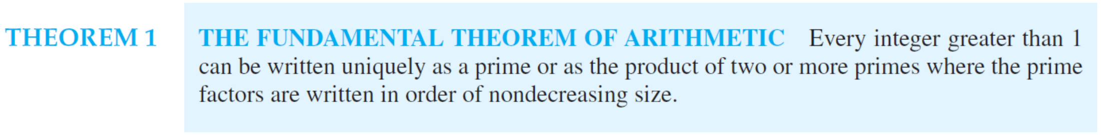
prime divisors (<10): 2 3 5 7

$118 = 2 \times 59$

We can see from these examples, we can find a prime divisor (a) where a is $1<a<n$ and <= to $\sqrt{n}$.

Theo Shin – Number Theory and Primes Problem Set
HW Week 7

B.



THEOREM 1 **THE FUNDAMENTAL THEOREM OF ARITHMETIC** Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

By reading Theorem 2 (p.258) we can see the importance of being able to show that an integer is prime based on “if n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.” As demonstrated in part A, we know by definition of a factor n = a * b where a is 1<a<n (definition of composite) and b is a positive integer greater than 1. Similar to part A, we will need to show a <= $\sqrt{\mathrm{n}}$ or b <= $\sqrt{\mathrm{n}}$, but this time by trying to show a > $\sqrt{\mathrm{n}}$ and b $> \sqrt{\mathrm{n}}$.

Proof by contradiction:

Assumptions:
There exists a and b such that a > $\sqrt{n}\ and\ b > \sqrt{n}$ (trying to show n can’t be written as product of primes)
n is composite otherwise there would be no prime divisors

Suppose there is an a and b such that a > $\sqrt{n}\ and\ b > \sqrt{n}$ then ab > $\sqrt{n} * \sqrt{n} = n$. However, this means n is a product of primes and divisible by a and b, which is a contradiction. Thus, a ≤ $\sqrt{n}$ or b ≤ $\sqrt{n}$ and n has a divisor less than or equal to $\sqrt{n}$. The divisor is either prime or by theorem 1 the product of two or more primes where prime factors are written in order of nondecreasing size.

C. The theorem will be extremely useful for writing our RSA project code since we will be working with large primes to encrypt and send our secret messages. In order to generate the key pairs (public/private) for RSA we will have to determine the factorization of n and the factorization of prime numbers unique to our keys.