Homework6 – Group 2

3.8

1. N = pq = 352717 and (p - 1) (q - 1) = 351520

Using (3.5) to compute,

(p + q) = N + 1 - (p - 1) (q - 1)

(p + q) = 352718 - 351520

p + q) = 1198

X^2 - (p + q)X + N = X^2 - 1198 X + 352717

= (X - 677) (X - 521)

This gives the factorization N = 352717 = 677, 521

1. N = pq = 77083921 and (p - 1) (q - 1) = 77066212

Using (3.5) to compute,

(p + q) = N + 1 - (p - 1) (q - 1)

(p + q) = 77083922 - 77066212

(p + q) = 17710

X^2 - (p + q)X + N = X^2 - 17710 X + 77083921

= (X - 10007) (X - 7703)

This gives the factorization N = 77083921 = 10007, 7703

1. N = pq = 109404161 and (p - 1) (q - 1) = 109380612

Using (3.5) to compute,

(p + q) = N + 1 - (p - 1) (q - 1)

(p + q) = 109404162 - 109380612

(p + q) = 23550

X^2 - (p + q)X + N = X^2 - 23550 X + 109404161

= (X - 17183) (X - 6367)

This gives the factorization N = 109404161 = 17183, 6367

1. N = pq = 172205490419 and (p - 1) (q - 1) = 172204660344

Using (3.5) to compute,

(p + q) = N + 1 - (p - 1) (q - 1)

(p + q) = 172205490420 - 172204660344

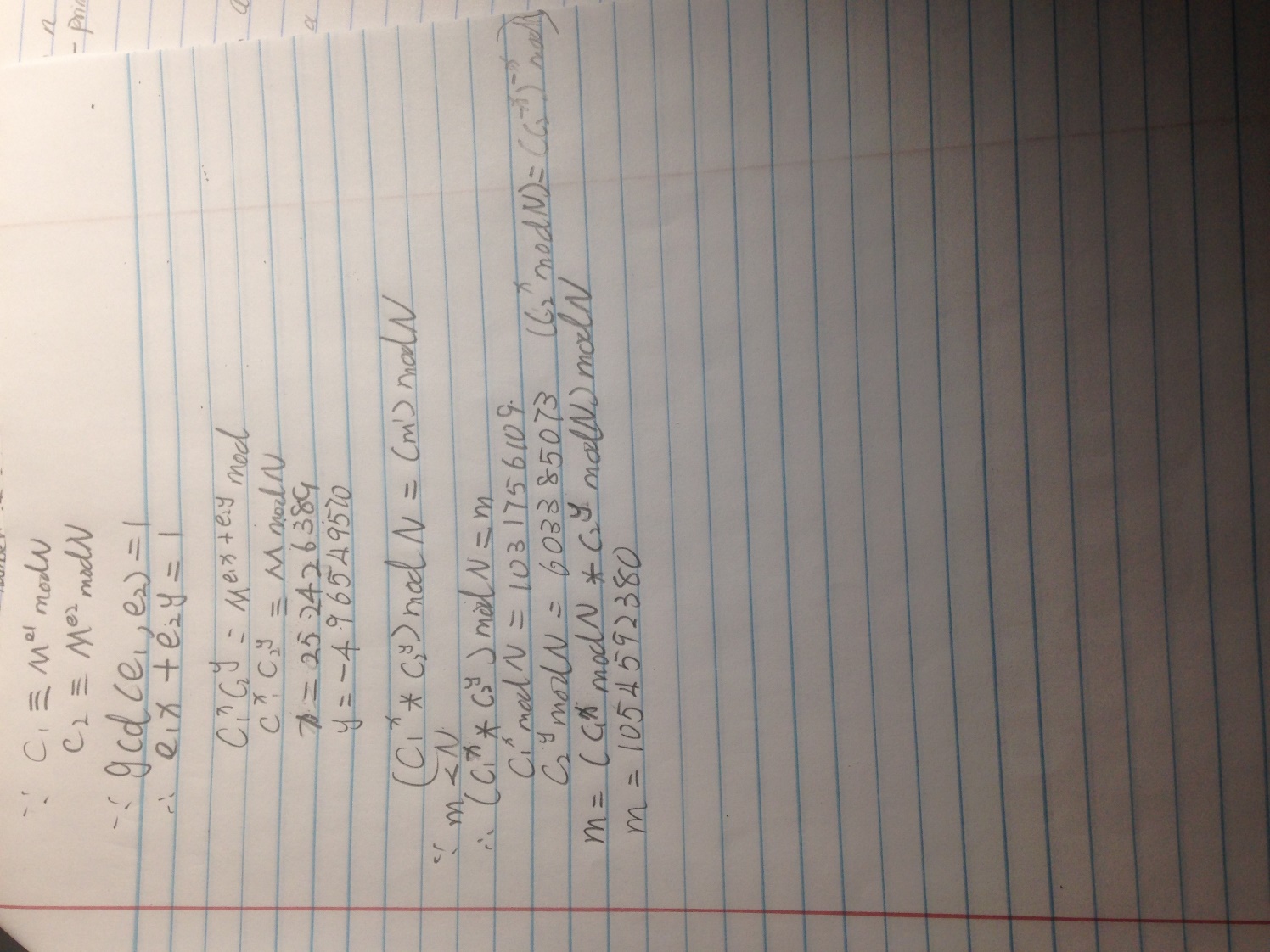
(p + q) = 830076

X^2 - (p + q)X + N = X^2 - 830075 X + 172205490419

= (X - 422183) (X - 407893)

This gives the factorization N = 352717 = 422183, 4078

**3.12**



3.14

a)

Let a = 10

Since none of these congruencies equals 1 or -1 10 is a Miller-Rabin witness for 1105 and 1105 is composite by the MRT.

b)

Let a = 69

Since , by the MRT 69 is a witness for 294409 and 294409 is composite.

c) The book had b and c as the same n.

d)

Let a = 2

Let a = 3

Let a = 5

Let a = 7

Let a = 11

Let a = 13

Let a = 17

Let a = 19

Let a = 23

Let a = 29

Thus, by the MRT is probably prime.

e)

Let a = 82

Since , by the MRT 82 is a witness for and is composite.

f)

Let a = 2

Let a = 3

Let a = 5

Let a = 7

Let a = 11

Let a = 13

Let a = 17

Let a = 19

Let a = 23

Let a = 29

Thus, by the MRT is probably prime.

g)

Let a = 2

Since none of these congruencies equals 1 or -1 2 is a Miller-Rabin witness for and is composite by the MRT.

3.21

1. n = 1739

22! – 1 = 3 (mod 1739) GCD(3, 1739) = 1

23! – 1 = 63 (mod 1739) GCD(63, 1739) = 1

24! – 1 = 1082 (mod 1739) GCD(1082, 1739) = 1

25! – 1 = 1394 (mod 1739) GCD(1394, 1739) = 1

26! – 1 = 1443 (mod 1739) GCD(1443, 1739) = 37

1739 / 37 = 47

(37 – 1) = 36 = 22 \* 33

Factors are 37 and 47, 37 has the property that p – 1 is a product of small primes

1. n = 220459

22! – 1 = 3 (mod 220459) GCD(3, 220459) = 1

23! – 1 = 63 (mod 220459) GCD(63, 220459) = 1

24! – 1 = 22331 (mod 220459) GCD(22331, 220459) = 1

25! – 1 = 85053 (mod 220459) GCD(85053, 220459) = 1

26! – 1 = 4045 (mod 220459) GCD(4045, 220459) = 1

27! – 1 = 43102 (mod 220459) GCD(43102, 220459) = 1

28! – 1 = 179600 (mod 220459) GCD(179600, 220459) = 449

220459 / 449 = 491

(449 – 1) = 448 = 26 \* 7

Factors are 449 and 491, 449 has the property that p – 1 is a product of small primes

1. n = 48356747

22! – 1 = 3 (mod 220459) GCD(3, 48356747) = 1

23! – 1 = 63 (mod 220459) GCD(63, 48356747) = 1

24! – 1 = 16777215 (mod 220459) GCD(16777215, 48356747) = 1

25! – 1 = 29007255 (mod 220459) GCD(29007255, 48356747) = 1

26! – 1 = 6497325 (mod 220459) GCD(6497325, 48356747) = 1

27! – 1 = 11540769 (mod 220459) GCD(11540769, 48356747) = 1

28! – 1 = 13320679 (mod 220459) GCD(13320679, 48356747) = 1

29! – 1 = 2119446 (mod 220459) GCD(2119446, 48356747) = 1

210! – 1 = 32129513 (mod 220459) GCD(32129513, 48356747) = 1

211! – 1 = 4931911 (mod 220459) GCD(4931911, 48356747) = 1

212! – 1 = 35410323 (mod 220459) GCD(35410323, 48356747) = 1

213! – 1 = 46845550 (mod 220459) GCD(46845550, 48356747) = 1

214! – 1 = 45774460 (mod 220459) GCD(45774460, 48356747) = 1

215! – 1 = 46983890 (mod 220459) GCD(46983890, 48356747) = 1

216! – 1 = 8398520 (mod 220459) GCD(8398520, 48356747) = 1

217! – 1 = 9367159 (mod 220459) GCD(9367159, 48356747) = 1

218! – 1 = 17907955 (mod 220459) GCD(17907955, 48356747) = 1

219! – 1 = 13944672 (mod 220459) GCD(13944672, 48356747) = 6917

48356747 / 6917 = 6991

(6917 – 1) = 6916 = 22 \* 7 \* 13 \* 19

Factors are 6917 and 6991, 6917 has the property that p – 1 is a factor of small primes

3.25

a.) N = 61063

1882^2= 270 mod 61063 and 270 = 2 \* 3^3 \* 5

1898^2 = 60750 mod 61063 and 60750 = 2 \* 3^5 \* 5^3

So,

1882^2 \* 1898^2 = (2 \* 3^3 \* 5) (2 \* 3^5 \* 5^3) = (2 \* 3^4 \*5^2)^2 = (4050)^2 mod 61063 🡨 4050 = b

And,

1882 \* 1898 = 3572036 = 30,382 mod 61063 🡨30,382 = a

GCD(N, a-b) = GCD(61063, (30,382 – 4,050)) = GCD(61063, 26332) = **227**

b.) N = 52907

339^2 = 480 mod 52907 = 2^5 \* 3 \* 5

763^2 = 192 mod 52907 = 2^6 \* 3

773^2 = 52907 mod 52907 = 2^6 \* 3^5

976^2 = 250 mod 52907 = 2 \* 5^3

So, 339^2 \*763^2\*773^2\*976^2 = (2^5 \* 3 \* 5)( 2^6 \* 3)( 2^6 \* 3^5)( 2 \* 5^3) = 2^18 \* 3^7 \*5^4 however this is not a power of 2 so we have to find a new combo. This combo is:

339^2\*773^2\*976^2 = (2^5 \* 3 \* 5)( 2^6 \* 3^5)( 2 \* 5^3) = 2^12 \* 3^6 \*5^4 = ( 2^6 \* 3^3 \* 5^2)^2 = 43200^2 🡨 43200 = b

And,

339 \* 773 \* 976 = 301024752 = 36829 mod 52907 🡨 36829 = a

GCD(N, b- a) = GCD(52907, (43200, 36829)) = GCD(52907, 6371) = **277**

c.) N = 198103

1189^2 = 27000 mod 198103 = 2^5 \* 3 \* 5

1605^2 = 27000 mod 198103 = 2 \* 7^3

2378^2 = 108000 mod 198103 = 2^5 \* 3^3 \* 5^3

2815^ 2 = 105 mod 198103 = 3 \* 5 \* 7

So,

1189^2 \* 1605^2 \* 2378^2 \*2815^ 2 = (2^5 \* 3 \* 5)( 2 \* 7^3)( 2^5 \* 3^3 \* 5^3)( 3 \* 5 \* 7)

= 2^3 \* 3^2 \* 5^2 \* 7^2 however this is not a power of two so another combination so I find a new combination which is:

1605^2 \* 2378^2 \*2815^ 2 = ( 2 \* 7^3)( 2^5 \* 3^3 \* 5^3)( 3 \* 5 \* 7) = (2^6 \* 3^4 \* 5^4 \* 7^4 ) = (2^3 \*3^2 \* 5^2 \* 7^2)^2 = (88200)^2 mod 198103 🡨 b

So,

1605 \* 2378 \* 2815 mod 198103 = 64248 🡨 a

GCD ( N, b – a) = GCD (198103 , (88200 – 64248)) = GCD (198103, 23952) = 499

d.) N = 2525891

1591^2 = 5390 mod 2525891 = 2 \* 5 \* 7^2 \* 11

3182^2 = 21560 mod 2525891 = 2^3 \* 5 \* 7^2 \* 11

4773^2 = 48150 mod 2525891 = 2 \* 3^2 \* 5 \* 7^2 \* 11

5275^2 = 40824 mod 2525891 = 2^3 \* 3^6 \* 7

5401^2 = 13860000 mod 2525891 = 2^4 \* 3^2 \* 5^3 \* 7 \* 11

1591^2 \* 3182^2 \*4773 ^ 2 \* 5275^2 \* 5401^2 = ( 2 \* 5 \* 7^2 \* 11)( =2^3 \* 5 \* 7^2 \* 11)( 2 \* 3^2 \* 5 \* 7^2 \* 11)( 2^3 \* 3^6 \* 7)( 2^4 \* 3^2 \* 5^3 \* 7 \* 11) = (2^6 \* 3^4 ^ 5^3 \* 7^4 \* 11^2)^2 = (18825760800)^2

So,

1591 \* 3182 \*4773 \* 5275 \* 5401 = 739064

GCD (N, b- a) = GCD(2525891, 18825686936) = 1