MATH 404 Homework

Maxwell Lin
maxwell.lin [at] duke [dot] edu

Textbook: *Introduction to Cryptography with Coding Theory* by Wade Trappe and Lawrence C. Washington, Second Edition.

MATH 404 — Homework #1

Due January 23, 2024

Maxwell Lin

Problem 1

Chapter 2, #1
Brute forcing the ciphertext EVIRE results in 2 sensible plaintexts: arena ($k = 4$) and river ($k = 13$). Therefore, either location is plausible.

Problem 2

Chapter 2, #10

(a) The predicted key length is the displacement that creates the largest number of coincidences. For this ciphertext, this is when the displacement is 2 since 6 coincidences occur.

Displacement	1	2	3	4	...
Coincidences	2	6	2	5	...

(b) Let $W_1 = (0.2, 0.8)$ be the frequency vector of the first letters in each block and A_i be the frequency vector of this language ($A_0 = (0.1, 0.9)$) rotated by i. We observe that $W_1 \cdot A_0 > W_1 \cdot A_1$. Thus, the first shift is 0.

Likewise, let $W_2 = (1, 0)$ be the frequency vector of the second letters in each block. We observe that $W_2 \cdot A_1 > W_2 \cdot A_0$. Thus, the first shift is 1.

Therefore, the key is $(0, 1) =$ AB and the plaintext is BBBBBBABBB.

Problem 3

Chapter 2, #11

(a) Using the same method as Problem 2, we observe that a displacement of 2 results in the largest number of coincidences.

Displacement	1	2	3
Coincidences	2	3	1

The letter frequencies for the first and second letters in each block are $W_1 = (0.6, 0.2, 0.2)$ and $W_2 = (0, 0.8, 0.2)$.

We have

$$\arg\max_i W_1 \cdot A_i = 0$$

and

$$\arg\max_i W_2 \cdot A_i = 1.$$

Thus, the most probable key is $(0, 1) =$ AB.

Problem 4

Chapter 2, #12
This fact is equivalent to the Cauchy-Schwarz inequality

$$\begin{aligned} v \cdot w &= |v||w|\cos(\theta) \\ \frac{v \cdot w}{|v||w|} &= \cos(\theta) \\ \frac{|v \cdot w|}{|v||w|} &= |\cos(\theta)| \leq 1 \\ |v \cdot w| &\leq |v||w|. \end{aligned}$$

Applying the Cauchy-Schwarz inequality, we obtain

$$A_0 \cdot A_i = |A_0 \cdot A_i| \leq |A_0||A_i| = |A_0||A_0| = A_0 \cdot A_0.$$

The first equality holds since frequencies are nonnegative. The second equality holds since addition is commutative. Therefore,

$$A_0 \cdot A_i \leq A_0 \cdot A_0$$

as required.

Problem 5

Chapter 2, #25

(a) The ciphertext will repeat every 6 characters. Therefore, Eve will likely suspect that the plaintext is one repeated letter shifted in blocks of 6.

(b) Take the first 6 characters of the ciphertext. Brute force all 26 possible shifts; only one of these shifts will result in a recognizable English word (since no English word of length six is a shift of another English word). This word is the key.

(c) Since the ciphertext repeats every 6 characters, all letters will match whenever the displacement is a multiple of 6. The number of matches will always be less otherwise (or equal, in the case that the key is also a repeated letter). In the case that each letter in the key is unique, the number of matches will be exactly 0 if the displacement is not a multiple of the key length.

Problem 6

Find the last two digits of 361^{361}. Hint: explain why computing the last two digits of a number is equivalent to computing the number mod 100. Then start computing the powers of $361 \pmod{100}$ and look for a pattern. Note that you should reduce mod 100 at each stage (but not the exponent).

Solution

Since

$$\mathbb{Z}/100\mathbb{Z} = \{C_0, C_1, \ldots, C_{99}\},$$

computing a number mod 100 will always result in its last two digits (two digit integers range from 0 to 99).

We observe the following pattern

$$\begin{aligned}
361^1 & &&\equiv 61 \\
361^2 &\equiv (61)(361) &&\equiv 21 \\
361^3 &\equiv (21)(361) &&\equiv 81 \\
361^4 &\equiv (81)(361) &&\equiv 41 \\
361^5 &\equiv (41)(361) &&\equiv 01 \\
361^6 &\equiv (01)(361) &&\equiv 61 \\
361^7 &\equiv (61)(361) &&\equiv 21
\end{aligned}$$

Since $361 \equiv 1 \pmod 5$,

$$361^{361} \equiv 361^1 \equiv 61.$$

MATH 404 — Homework #2

Due February 1, 2024

Maxwell Lin

Problem 1

Chapter 3, #1

(a) Using the Euclidean algorithm, we obtain $17(6) + 101(-1) = 1$ so $x = 6$ and $y = -1$.

(b) From part (a), $17^{-1} = x = 6 \pmod{101}$.

Problem 2

Chapter 3, #3

(a) We first divide the congruence by $\gcd(12, 236) = 4$.

$$3x \equiv 7 \pmod{59}$$

Using the Euclidean algorithm, we find that $3^{-1} = 20 \pmod{59}$. Therefore,

$$x \equiv 140 \equiv 22 \pmod{59}.$$

This means the solutions to the original congruence are 22, 81, 140, and 199 (mod 236).

(b) Since $4 \nmid 30$, this congruence has no solutions.

Problem 3

Chapter 3, #4

(a) We have

$$\begin{aligned}
30030 &= 257 \cdot 116 + 218 \\
257 &= 218 \cdot 1 + 39 \\
218 &= 39 \cdot 5 + 23 \\
39 &= 23 \cdot 1 + 16 \\
23 &= 16 \cdot 1 + 7 \\
16 &= 7 \cdot 2 + 2 \\
7 &= 2 \cdot 3 + 1 \\
2 &= 1 \cdot 2 + 0
\end{aligned}$$

Therefore, $\gcd(30030, 257) = 1$.

(b) Since $\gcd(30030, 257) = 1$, the prime factors of 30030 do not divide 257. That is, $2 \nmid 257$, $3 \nmid 257$, $5 \nmid 257$, $7 \nmid 257$, $11 \nmid 257$, and $13 \nmid 257$.

This is all we need to show that 257 is prime. To see why, suppose 257 can be factored into at least two primes that we haven't checked yet (i.e., greater than 13). The smallest such number would be $17^2 = 289 > 257$. Therefore, if 257 can be factored into multiple primes, at least one of the primes must be less than or equal to 13. Since there are no primes that satisfy this condition, 257 cannot be factored into multiple primes and its prime factorization is itself. Thus, 257 is prime.

Problem 4

Chapter 3, #5

(a) Using the Euclidean algorithm, we obtain $\gcd(4883, 4369) = 257$.

(b) We divide by the gcd to obtain the prime factorizations

$$\begin{aligned} 4883 &= 257 \cdot 19 \\ 4369 &= 257 \cdot 17. \end{aligned}$$

Problem 5

Chapter 3, #6

(a) We apply the Euclidean algorithm

$$\begin{aligned} F_n &= F_{n-1} \cdot 1 + F_{n-2} \qquad \text{since } 0 \leq F_{n-2} < F_{n-1} \\ F_{n-1} &= F_{n-2} \cdot 1 + F_{n-3} \\ &\cdots \\ 2 &= 1 \cdot 1 + 1 \\ 1 &= 1 \cdot 1 + 0. \end{aligned}$$

Therefore, $\gcd(F_n, F_{n-1}) = 1$ for all $n \geq 1$.

(b) Applying the Euclidean algorithm, we obtain $\gcd(11111111, 11111) = 1$.

(c) Let $\mathbb{1}_i$ be a string of 1's of length F_i.

We observe the pattern

$$\begin{aligned} \mathbb{1}_n &= \mathbb{1}_{n-1} \cdot 10^{F_{n-2}} + \mathbb{1}_{n-2} \\ \mathbb{1}_{n-1} &= \mathbb{1}_{n-2} \cdot 10^{F_{n-3}} + \mathbb{1}_{n-3} \\ &\cdots \\ 11 &= 1 \cdot 10 + 1 \\ 1 &= 1 \cdot 1 + 0. \end{aligned}$$

Therefore, $\gcd(a, b) = 1$.

Problem 6

Chapter 3, #7

(a) Let p be prime. Suppose $a, b \in \mathbb{Z}$ such that $ab \equiv 0 \pmod{p}$.

If $a \equiv 0$, we are done. We need to show that if $a \not\equiv 0$, then $b \equiv 0$. Since $ab \equiv 0 \pmod{p}$, we have $p \mid ab$.

Since p is prime, its divisors are 1 and p. Therefore, $\gcd(p, a)$ must be either 1 or p. Since $a \not\equiv 0$, we have $p \nmid a$. Therefore, $\gcd(p, a) = 1$.

Since $p \mid ab$ and $\gcd(p, a) = 1$, we must have $p \mid b$. That is, $b \equiv 0 \pmod{p}$ as required.

(b) Let $a, b, n \in \mathbb{Z}$ with $n \mid ab$ and $\gcd(a, n) = 1$.

Since $\gcd(a, n) = 1$, there exists $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. Then,

$$\begin{aligned} ax + ny &= 1 \\ (ax + ny)b &= b \\ axb + nyb &= b \end{aligned}$$

Obviously, $n \mid nyb$. Also, since $n \mid ab$, we have $n \mid axb$. Therefore, $n \mid (axb + nyb)$ which is equivalent to $n \mid b$.

Problem 7

Chapter 3, #18

(a) We have

$$\begin{aligned} \begin{pmatrix} 1 & 1 \\ 6 & 1 \end{pmatrix}^{-1} &\equiv \frac{1}{-5} \begin{pmatrix} 1 & -1 \\ -6 & 1 \end{pmatrix} \pmod{26} \\ &\equiv 5 \begin{pmatrix} 1 & -1 \\ -6 & 1 \end{pmatrix} \\ &\equiv \begin{pmatrix} 5 & -5 \\ -30 & 5 \end{pmatrix} \\ &\equiv \begin{pmatrix} 5 & 21 \\ 22 & 5 \end{pmatrix} \end{aligned}$$

(b) We need $\gcd(1 - b, 26) = 1$. We obtain $b = 0, 2, 4, 6, 8, 10, 12, 16, 18, 20, 22, 24 \pmod{26}$.

Problem 8

Chapter 2, #3

The plaintext is $7, 14, 22, 0, 17, 4, 24, 14, 20$.

Applying the affine function, we obtain the ciphertext $16, 25, 13, 7, 14, 1, 23, 25, 3$ (QZNHOBXZD).

The decryption function is $x = \frac{1}{5}(y - 7) = 21(y - 7)$ since $\frac{1}{5} = 21$ in mod 26.

Applying the decryption function, we recover the original plaintext $7, 14, 22, 0, 17, 4, 24, 14, 20$.

Problem 9

Chapter 2, #5
We have the following system

$$\begin{aligned} 7\alpha + \beta &\equiv 2 \\ 0\alpha + \beta &\equiv 17 \end{aligned}$$

We immediately obtain $\beta = 17$. Subtracting the 2 equations, we have $7\alpha \equiv -15 \pmod{26}$. Since $7^{-1} = -11$, we obtain $\alpha \equiv 165 \equiv 9 \pmod{26}$.
The decryption function is

$$\begin{aligned} x &= \alpha^{-1}(y - \beta) \\ &= 3(y - 17) \end{aligned}$$

Applying the decryption function to the ciphertext, we obtain the plaintext $7, 0, 15, 15, 24$ (happy).

Problem 10

Chapter 2, #15
We have the following matrix equation

$$\begin{bmatrix} 1 & 0 \\ 25 & 25 \end{bmatrix} M \equiv \begin{bmatrix} 7 & 2 \\ 6 & 19 \end{bmatrix}.$$

We multiply by the inverse to obtain

$$\begin{aligned} M &\equiv \begin{bmatrix} 1 & 0 \\ 25 & 25 \end{bmatrix} \begin{bmatrix} 7 & 2 \\ 6 & 19 \end{bmatrix} \\ &\equiv \begin{bmatrix} 7 & 2 \\ 13 & 5 \end{bmatrix} \pmod{26}. \end{aligned}$$

MATH 404 — Homework #3

Due February 8, 2024

Maxwell Lin

Problem 1

Chapter 3, #9
Applying the Chinese Remainder Theorem, we obtain

$$x = (3)(3)(7) - (2)(2)(10) = 23 \pmod{70}.$$

Problem 2

Chapter 3, #10
We obtain the following system

$$\begin{align} x &\equiv 1 \pmod 3 \tag{1}\\ x &\equiv 2 \pmod 4 \tag{2}\\ x &\equiv 3 \pmod 5. \tag{3}\end{align}$$

Applying the Chinese Remainder Theorem to the first two congruences, we obtain

$$x \equiv 10 \pmod{12}.$$

Applying the Chinese Remainder Theorem to this congruence and (3) we obtain

$$x \equiv 58 \pmod{60}.$$

Therefore, the smallest number of people is 58 and the next smallest number is $58 + 60 = 118$.

Problem 3

Chapter 3, #19
This is equivalent to finding all primes p such that $\gcd(p, -26) \neq 1$.
Since the prime factorization of 26 is $26 = 2 \cdot 13$, we have $p = 2, 13$.

Problem 4

Chapter 3, #24
We have

$$\begin{aligned} x &= a_1y_1z_1 + \cdots + a_iy_iz_i + \cdots + a_ky_kz_k \\ &= a_1y_1(m_2\cdots m_k) + \cdots + a_iy_i(m_1\cdots m_{i-1}m_{i+1}\cdots m_k) + \cdots + a_ky_k(m_1\cdots m_{k-1}). \end{aligned}$$

Therefore,

$$x \equiv a_i y_i (m_1 \cdots m_{i-1} m_{i+1} \cdots m_k) \pmod{m_i}$$

since $m_i \mid z_j$ if and only if $j \neq i$ (since $\gcd(m_i, m_j) = 1$).
Since $y_i \equiv z_i^{-1} \pmod{m_i}$,

$$x \equiv a_i \pmod{m_i}$$

for all i as desired.

Problem 5

Chapter 3, #39

(a) Let $S = \{kp \mid k \in \{1, 2, \ldots, q-1\}\}$. For all $m \in S$, we have $1 \leq m < pq$. This set cannot be any larger since if $k = 0$, $1 \nleq 0p$ and if $k = q$, $pq \nless pq$. Since $|S| = q - 1$, there are exactly $q - 1$ multiples of p satisfying this condition.

Following a symmetric argument, there are $p - 1$ multiples of q.

(b) We prove the contrapositive. Assume $p \nmid m$ and $q \nmid m$. Since p and q are prime, the prime factorization of pq is $pq = p \cdot q$. However, since neither of these two primes also divide m, we must have that $\gcd(m, pq) = 1$ as desired.

(c) Since p and q are distinct primes, $\operatorname{lcm}(p, q) = \frac{pq}{\gcd(p,q)} = pq$. Since the first (positive) multiple of both p and q is pq, m cannot be a multiple of both p and q since it is strictly less than pq.

(d) The total number of integers n with $1 \leq n < pq$ is $pq - 1$. We need to subtract off the number of n such that $\gcd(n, pq) \neq 1 \iff \gcd(n, pq) > 1$. By Part (b), this is equivalent to finding all n such that n is a multiple of p or a multiple of q. By Part (a), there are $q - 1$ multiples of p and $p - 1$ multiples of q. Additionally, these sets are disjoint since m cannot be a multiple of both p and q by Part (c). Therefore, the total number of n where $\gcd(n, pq) = 1$ is $pq - 1 - (p - 1) - (q - 1)$ as desired.

Problem 6

Chapter 3, #40

(a)

$$x \equiv 0 \pmod{2}$$
$$x \equiv 1 \pmod{4}$$

(b)

$$x \equiv 0 \pmod{2}$$
$$x \equiv 2 \pmod{4}$$

A possible solution is $x = 2$.

MATH 404 — Homework #4

Due February 15, 2024

Maxwell Lin

Problem 1

Let G be a finite group. Show that for each element $a \in G$, there exists a positive integer n such that $a^n = e$. Furthermore, show that e is the first repeat in the list of powers of $a : a^0 = e, a^1 = a, a^2, a^3, \cdots$.

Solution

Consider the set

$$S = \{ a^n \mid n \in \mathbb{Z}^+ \}.$$

Since a group is closed under multiplication, $s \in S \implies s \in G$ so that $S \subset G$. But $\mathbb{Z}^+$ is an infinite set, so there exists $x, y \in \mathbb{Z}^+$ with $x < y$ such that $a^x = a^y$. Since every element in G has an inverse we have

$$\begin{aligned} a^x &= a^y \\ e &= a^{y-x} \end{aligned}$$

where $y - x \in \mathbb{Z}^+$ as desired.

Since there exists some $n \in \mathbb{Z}^+$ such that $a^n = e$, there exists a least such element d by the well-ordering property. For the sake of contradiction, suppose e is not the first repeat in the list of powers of a. That is, suppose there exists some $x, y \in \mathbb{Z}$ with $0 < x < y < d$ such that $a^x = a^y$. Taking the inverse, we obtain $e = a^{y-x}$. But $0 < y - x < d$ contradicting that a has order d. Thus, e is the first repeat in the list of powers of a.

Problem 2

Let G be a group and suppose that $a \in G$ has order n. Prove that $a^k = e$ if and only if $n \mid k$.

Solution

$(\implies)$ Suppose $a^k = e$. We divide k by n

$$k = nq + r \qquad 0 \leq r < n.$$

Thus

$$\begin{aligned} a^k &= e \\ a^{nq+r} &= e \\ (a^n)^q \cdot a^r &= e \\ a^r &= e. \end{aligned}$$

Since G has order n and $0 \leq r < n$, it must be that $r = 0$. Thus, $k = nq$ and $n \mid k$.

$(\impliedby)$ If $n \mid k$, then $k = nq$. Then

$$a^k = a^{nq} = (a^n)^q = e^q = e.$$

Problem 3

Let G be a finite abelian group. Show that $a^{\#G} = 1$. Using the previous exercise, conclude that the order of a divides $\#G$.

Solution

Let $d = |G|$. Consider the function $f : G \to G$ where $f(x) = ax$ for some $a \in G$.
We now prove that f is injective

$$\begin{aligned} f(x) &= f(y) \\ ax &= ay \\ a^{-1}(ax) &= a^{-1}(ay) \\ (a^{-1}a)x &= (a^{-1}a)y \\ ex &= ey \\ x &= y \end{aligned}$$

as desired.
Applying f to the elements of $G = \{x_1, x_2, \ldots, x_d\}$, we obtain another set $G' = \{ax_1, ax_2, \ldots, ax_d\}$. Since f is injective and $|G| = |G'|$, it must be that $G = G'$. Thus,

$$\begin{aligned} x_1x_2\cdots x_d &= ax_1ax_2\cdots ax_d && \text{Since } G \text{ abelian} \\ x_1x_2\cdots x_d &= a^d x_1x_2\cdots x_d \\ e &= a^d \end{aligned}$$

as desired.
By the previous exercise, $n \mid d$ where n is the order of a.

Problem 4

Chapter 3, #11
Let p be prime. Suppose $p \nmid a$. Then

$$\begin{aligned} a^{p-1} &\equiv 1 \pmod p \\ a^p &\equiv a \pmod p \end{aligned}$$

as desired.
If $p \mid a$, then $a \equiv 0 \pmod p$ and $a = kp$ for some $k \in \mathbb{Z}$. Then

$$a^p \equiv (kp)^p \equiv k^p p^p \equiv 0 \equiv a \pmod p$$

as desired.

Problem 5

Chapter 3, #12

Problem 5 continued on next page. . .

We want to find $2^{10203} \pmod{101}$. Since $\gcd(2, 101) = 1$, we can reduce the exponent mod $\phi(101) = 100$. Since

$$10203 \equiv 3 \pmod{100},$$

we have

$$2^{10203} \equiv 2^3 \equiv 8 \pmod{101}.$$

Problem 6

Chapter 3, #13
We want to find $123^{562} \pmod{100}$. Since $\gcd(123, 100) = 1$, we can reduce the exponent mod $\phi(100) = 100(1 - 1/2)(1 - 1/5) = 40$. Since

$$562 \equiv 2 \pmod{40},$$

we have

$$123^{562} \equiv 123^2 \equiv 15129 \equiv 29 \pmod{100}.$$

Problem 7

Chapter 3, #14

(a) We can use Pingala's algorithm.

$$\begin{aligned} 7^1 &\equiv 7 \equiv 3 \pmod 4 \\ 7^2 &\equiv 49 \equiv 1 \pmod 4 \\ 7^4 &\equiv 1^2 \equiv 1 \pmod 4 \end{aligned}$$

Thus, $7^7 \equiv 7^4 7^2 7^1 \equiv (1)(1)(3) \equiv 3 \pmod 4$.

(b) We want to find $7^{7^7} \pmod{10}$. Since $\gcd(7, 10) = 1$, we can reduce the exponent mod $\phi(10) = 4$. Since

$$7^7 \equiv 3 \pmod 4 \qquad \text{Part (a)},$$

we have

$$7^{7^7} \equiv 7^3 \equiv 3 \pmod{10}.$$

Problem 8

Chapter 3, #16

(a) Since $p \nmid a$ and p prime, $\gcd(p, a) = 1$. Therefore, we can reduce the exponent mod $\phi(p)$.

We have

$$1728 \equiv 0 \pmod{6}$$
$$1728 \equiv 0 \pmod{12}$$
$$1728 \equiv 0 \pmod{18}$$

for $p = 7, 13, 19$ respectively.

Therefore,

$$a^{1728} \equiv a^0 \equiv 1 \pmod{p}$$

as desired.

(b) From Part (a), we know that if $p \nmid a$

$$a^{1728} \equiv 1 \pmod{p}$$
$$a^{1729} \equiv a \pmod{p}.$$

Now suppose $p \mid a$. Then, $a \equiv 0 \pmod{p}$ and $a = pk$ for some $k \in \mathbb{Z}$.

$$a^{1729} \equiv (pk)^{1729} \equiv 0 \equiv a \pmod{p}$$

as desired.

(c) From Part (b), we know that

$$a^{1729} \equiv a \pmod{7}$$
$$a^{1729} \equiv a \pmod{13}$$
$$a^{1729} \equiv a \pmod{19}.$$

Since 7, 13, and 19 are pairwise coprime,

$$a^{1729} \equiv a \pmod{7 \cdot 13 \cdot 19}$$
$$a^{1729} \equiv a \pmod{1729}.$$

MATH 404 — Homework #5

Due February 29, 2024

Maxwell Lin

Problem 1

Chapter 3, #17

(a) We have

$$\begin{aligned}
2^0 &\equiv 1 \pmod{11} \\
2^1 &\equiv 2 \pmod{11} \\
2^2 &\equiv 4 \pmod{11} \\
2^3 &\equiv 8 \pmod{11} \\
2^4 &\equiv 5 \pmod{11} \\
2^5 &\equiv 10 \pmod{11} \\
2^6 &\equiv 9 \pmod{11} \\
2^7 &\equiv 7 \pmod{11} \\
2^8 &\equiv 3 \pmod{11} \\
2^9 &\equiv 6 \pmod{11}
\end{aligned}$$

So 2 is a primitive root mod 11.

(b) We wish to find

$$\begin{aligned}
8^x &\equiv 2 \pmod{11} \\
\left(2^3\right)^x &\equiv 2 \pmod{11} \\
2^{3x} &\equiv 2 \pmod{11}.
\end{aligned}$$

Since 2 and 11 are coprime, we can reduce the exponent mod $\phi(11) = 10$. Thus, $x = 7$ is the inverse of 3 mod 10.

(c) We have

$$\begin{aligned}
8^0 &\equiv 1 \pmod{11} \\
8^1 &\equiv 8 \pmod{11} \\
8^2 &\equiv 9 \pmod{11} \\
8^3 &\equiv 6 \pmod{11} \\
8^4 &\equiv 4 \pmod{11} \\
8^5 &\equiv 10 \pmod{11} \\
8^6 &\equiv 3 \pmod{11} \\
8^7 &\equiv 2 \pmod{11} \\
8^8 &\equiv 5 \pmod{11} \\
8^9 &\equiv 7 \pmod{11}.
\end{aligned}$$

So 8 is a primitive root mod 11.

(d) Since $\gcd(g,p) = 1$, we can reduce the exponent mod $\phi(p) = p - 1$.

$$\begin{aligned} h &\equiv g^y \pmod p \\ h^x &\equiv (g^y)^x \pmod p \\ h^x &\equiv g^{xy} \pmod p \\ h^x &\equiv g \pmod p \qquad \text{since } xy \equiv 1 \pmod{p-1}. \end{aligned}$$

(e) Since $h^x \equiv g \pmod p$ where g is a primitive root mod p, taking $(h^x)^k = h^{xk}$ with $k \in \mathbb{Z}$ will result in all nonzero congruence classes mod p. Thus, h is a primitive root mod p.

Problem 2

Chapter 3, #21

(a) Since $r \mid 600$, we can write r in the form

$$r = 2^a \cdot 3^b \cdot 5^c$$

where $a \leq 3$, $b \leq 1$, and $c \leq 2$ are positive integers. Additionally, since $r < 600$, at least $a \neq 3$, $b \neq 1$, or $c \neq 2$.

Note that

$$\begin{aligned} 300 &= 2^{3-1} \cdot 3^1 \cdot 5^2 \\ 200 &= 2^3 \cdot 3^{1-1} \cdot 5^2 \\ 120 &= 2^3 \cdot 3^1 \cdot 5^{2-1}. \end{aligned}$$

Thus, a number d that divides one of these must be in the form

$$d = 2^a \cdot 3^b \cdot 5^c$$

using the same conditions on a, b, and c as before. So r must divide at least one of 300, 200, or 120.

(b) We know that $\text{ord}_{601}(7) \mid \phi(601)$ and $\phi(601) = 600$. Since $\text{ord}_{601}(7) \mid 600$ and $\text{ord}_{601}(7) < 600$, $\text{ord}_{601}(7)$ divides at least one of 300, 200, or 120 by Part (a).

(c) Write $d := \text{ord}_{601}(7)$. We proved earlier that $d \mid n$ if and only if $7^n \equiv 1$. Since $7^{300} \not\equiv 1$, $7^{200} \not\equiv 1$, $7^{120} \not\equiv 1$, d does not divide 300, 200, or 120.

(d) By parts (b) and (c), it must be that $d \geq 600$. By Fermat's theorem, $d = 600$. Since $\text{ord}_{601}(7) = 600 = 601 - 1$, 7 is a primitive root mod 601.

(e) First, ensure that $p \nmid g$ so that $g \in (\mathbb{Z}/p\mathbb{Z})^*$.

Compute $g^{\frac{p-1}{q_i}} \pmod p$ for all i using Pingala's algorithm. If $g^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p$ for all i, then g is a primitive root mod p. Otherwise, g is not a primitive root.

Problem 3

Chapter 3, #22

(a) We have

$$\begin{aligned} 3^{16k} \equiv (3^k)^{16} \equiv 2^{16} \not\equiv 1 \pmod{65537} \\ \implies 65536 \nmid 16k \\ \implies 4096 \nmid k \end{aligned}$$

and

$$\begin{aligned} 3^{32k} \equiv (3^k)^{32} \equiv 2^{32} \equiv 1 \pmod{65537} \\ \implies 65536 \mid 32k \\ \implies 2048 \mid k. \end{aligned}$$

(b) We need to find the number of k mod 65536 such that both $2048 \mid k$ and $4096 \nmid k$. There are $\frac{65536}{(2048)(2)} = 16$ choices.

Exhaustively trying all values 2048, 6144, 10240, ..., we obtain $k = 55296$.

MATH 404 — Homework #6

Due March 7, 2024

Maxwell Lin

Problem 1

Chapter 6, #1
We know $11413 = 101 \cdot 113$ and

$$5859 = m^{7467} \pmod{11413}.$$

The decryption key is

$$7467^{-1} \pmod{(100 \cdot 112)} = 3.$$

Thus, the plaintext is

$$5859^3 \equiv 1415 \pmod{11413} = \texttt{no}.$$

Problem 2

Chapter 6, #2

(a) The decryption key is

$$d = 3^{-1} \equiv 27 \pmod{40}.$$

(b) Since $\gcd(m, 55) = 1$, we can reduce the exponent by $\phi(55) = 40$.

$$c^d \equiv (m^3)^{27} \equiv m^{81} \equiv m^1 \equiv m \pmod{55}.$$

Problem 3

Chapter 6, #3
We have

$$8^3 \equiv 75 \pmod{437}$$
$$9^3 \equiv 292 \pmod{437}$$

so 8 is the plaintext.

Problem 4

Chapter 6, #6
Note that

$$e = ((m^a)^b)^{a_1} \equiv m^{aa_1b} \equiv m^b \pmod{n}.$$

Let $b_1 = b^{-1} \pmod{\phi(n)}$ which exists since $\gcd(b, \phi(n)) = 1$. To recover m, Bob must exponentiate e by b_1

$$e^{b_1} \equiv (m^b)^{b_1} \equiv m^{bb_1} \equiv m \pmod{n}.$$

Problem 5

Chapter 6, #7
We decrypt as follows

$$\begin{aligned}(2^e c)^d &\equiv e^{ed} c^d \pmod{n}\\ &\equiv 2m \pmod{n}.\end{aligned}$$

Since n should be made of two *large* primes, $\gcd(2, n) = 1$. Thus, there exists $2^{-1} \pmod{n}$ such that Eve can uniquely determine m.

Problem 6

Chapter 6, #16
Since $\gcd(e_A, e_B) = 1$, Eve can use the Euclidean algorithm to find $a, b \in \mathbb{Z}$ such that $ae_A + be_B = 1$. Then Eve can compute

$$c_A^a c_B^b \equiv m^{ae_A} m^{be_B} = m^{ae_A+be_B} = m \pmod{n}.$$

Problem 7

Chapter 6, #17
Since we are only encrypting letters, this algorithm is no stronger than a substitution cipher. Create a lookup table for all possible plaintext to ciphertext mappings to decrypt the message.
For example,

$$\begin{aligned}1^{13} &\equiv 1 \pmod{8881}\\ 2^{13} &\equiv 8192 \pmod{8881}\\ 3^{13} &\equiv 4624 \pmod{8881}\\ 4^{13} &\equiv 4028 \pmod{8881}\\ &\vdots\end{aligned}$$

so $1 \mapsto A$, $8192 \mapsto B$, $4624 \mapsto C$, $4028 \mapsto D$, $\ldots$
Decrypting the given ciphertext, we obtain `hello`.

Problem 8

Chapter 6, #19

(a) Let $m = k\phi(n)$ for some $k \in \mathbb{Z}$. Since $\gcd(a, n) = 1$,

$$\begin{aligned} a^{\phi(n)} &\equiv 1 \pmod{n} \\ (a^{\phi(n)})^k &\equiv 1 \pmod{n} \\ a^{k\phi(n)} &\equiv 1 \pmod{n} \\ a^m &\equiv 1 \pmod{n} \end{aligned}$$

Since p and q divide n, this implies

$$\begin{aligned} a^m &\equiv 1 \pmod{p} \\ a^m &\equiv 1 \pmod{q}. \end{aligned}$$

(b) From Part (a), if $\gcd(a, n) = 1$

$$\begin{aligned} a^m &\equiv 1 \pmod{n} \\ a^{m+1} &\equiv a \pmod{n}. \end{aligned}$$

Since p and q divide n

$$\begin{aligned} a^{m+1} &\equiv a \pmod{p} \\ a^{m+1} &\equiv a \pmod{q}. \end{aligned}$$

Now suppose $\gcd(a, n) \neq 1$. Then, either $p \mid a$ or $q \mid a$. We split into cases:

1. $p \mid a$ and $q \nmid a$.
   Write $pl = a$ for some $l \in \mathbb{Z}$. Then

   $$a^{m+1} \equiv (pl)^{m+1} \equiv 0 \pmod{p}$$

   and

   $$a \equiv pl \equiv 0 \pmod{p}$$

   so $a^{m+1} \equiv a \pmod{p}$.
   Additionally, since $\gcd(a, q) = 1$

   $$a^{m+1} \equiv a \pmod{q}.$$

2. $p \nmid a$ and $q \mid a$.
   Follows the same argument as (a). Just swap p and q.
3. $p \mid a$ and $q \mid a$. Since $p \mid a$, $q \mid a$, and p and q are coprime, we have $n \mid a$. Write $nl = a$ for some $l \in \mathbb{Z}$. Then

   $$a^{m+1} \equiv (nl)^{m+1} \equiv 0 \pmod{n}$$

   and

   $$a \equiv (nl) \equiv 0 \pmod{n}.$$

   Thus, $a^{m+1} \equiv a \pmod{n}$. Since p and q divide n, this implies

   $$\begin{aligned} a^{m+1} &\equiv a \pmod{p} \\ a^{m+1} &\equiv a \pmod{q}. \end{aligned}$$

Problem 8 continued on next page. . .

Thus, in all cases $a^{m+1} \equiv a \pmod p$ and $\pmod q$.

(c) We know that $ed \equiv 1 \pmod{\phi(n)}$. Write $ed = 1 + \phi(n)k$ for some $k \in \mathbb{Z}$. Then, $ed = \phi(n)k + 1 = m + 1$. Thus

$$a^{ed} \equiv a^{m+1} \overset{\text{(b)}}{\equiv} a \pmod p$$
$$a^{ed} \equiv a^{m+1} \overset{\text{(b)}}{\equiv} a \pmod q.$$

Since p and q are coprime, this implies

$$a^{ed} \equiv a \pmod n.$$

(d) For $\gcd(a, n) \neq 1$, $p \mid a$ or $q \mid a$. The probability of this occurring is $\frac{1}{p} + \frac{1}{q} - \frac{1}{pq}$ which approaches 0 as p and q grow towards infinity. Thus, it is very likely that $\gcd(a, n) = 1$ for large p and q.

Problem 9

Chapter 6, #27

(a) Eve intercepts $c_1 \equiv m_1^e \equiv (10^{100}m)^e \equiv 10^{100e}m^e \pmod n$. Thus, Eve can simply divide c_1 by $10^{100e} \pmod n$ to produce m^e, then apply the same short plaintext attack as before.

(This requires that 10^{100e} has an inverse mod n, but this is likely by Problem 8.d, since n is the product of two large primes.)

(b) Let the length of m be d. Eve knows that $m||m = (10^d+1)m$. Thus, the ciphertext is $c_1 \equiv ((10^d+1)m)^e \equiv (10^d + 1)^e m^e \pmod n$. As with Part (a), Eve can divide c_1 by $(10^d + 1)^e \pmod n$, to obtain m^e then apply the short plaintext attack.

MATH 404 — Homework #7

Due March 21, 2024

Maxwell Lin

Problem 1

In this problem we're going to prove that the continued fraction convergents of an irrational number x converge to x. We use the notation from class.

1. Prove by induction that for every $n \geq 0$ we have
$$x = \frac{x_n p_{n-1} + p_{n-2}}{x_n q_{n-1} + q_{n-2}}.$$
2. Using the previous part, prove that
$$x - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_{n-1}\left(x_n q_{n-1} + q_{n-2}\right)}.$$
3. Use the previous part to show that $\lim_{n\to\infty} \left|x - \frac{p_n}{q_n}\right| = 0$, in other words,
$$\lim_{n\to\infty} p_n/q_n = x.$$

Solution

1. Base case ($k = 0$):
$$\begin{aligned}\frac{x_0 p_{-1} + p_{-2}}{x_0 q_{-1} + q_{-2}} &= \frac{(x)(1) + (0)}{(x)(0) + (1)}\\ &= x.\end{aligned}$$
Inductive step: Assume for some $k = n$ where $n \geq 0$
$$x = \frac{x_k p_{k-1} + p_{k-2}}{x_k q_{k-1} + q_{k-2}}.$$
Then,
$$\begin{aligned}\frac{x_{k+1} p_k + p_{k-1}}{x_{k+1} q_k + q_{k-1}} &= \frac{x_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{x_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}}\\ &= \frac{\frac{1}{x_k - a_k}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{\frac{1}{x_k - a_k}(a_k q_{k-1} + q_{k-2}) + q_{k-1}}\\ &= \frac{a_k p_{k-1} + p_{k-2} + p_{k-1} x_k + p_{k-1} a_k}{a_k q_{k-1} + q_{k-2} + q_{k-1} x_k + q_{k-1} a_k}\\ &= \frac{p_{k-2} + p_{k-1} x_k}{q_{k-2} + q_{k-1} x_k}\\ &= x \qquad \text{by Inductive Hypothesis.}\end{aligned}$$

2. By part (1),
$$x = \frac{x_n p_{n-1} + p_{n-2}}{x_n q_{n-1} + q_{n-2}}.$$
We compute
$$\begin{aligned} x - \frac{p_{n-1}}{q_{n-1}} &= \frac{x_n p_{n-1} + p_{n-2}}{x_n q_{n-1} + q_{n-2}} - \frac{p_{n-1}}{q_{n-1}} \\ &= \frac{x_n p_{n-1} q_{n-1} + p_{n-2} q_{n-1} - p_{n-1} x_n q_{n-1} - p_{n-1} q_{n-2}}{(x_n q_{n-1} + q_{n-2}) q_{n-1}} \\ &= \frac{-(p_{n-1} q_{n-2} - q_{n-1} p_{n-2})}{(x_n q_{n-1} + q_{n-2}) q_{n-1}} \\ &= \frac{(-1)^{n-1}}{q_{n-1} (x_n q_{n-1} + q_{n-2})} \end{aligned}$$
since $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$.

3. From part (2),
$$x - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_{n-1} (x_n q_{n-1} + q_{n-2})}.$$
Thus,
$$\begin{aligned} \left| x - \frac{p_{n-1}}{q_{n-1}} \right| &= \frac{1}{q_{n-1} (x_n q_{n-1} + q_{n-2})} \\ &\le \frac{1}{q_{n-1} q_n} \qquad \text{since } a_n \le x_n \\ &< \frac{1}{q_{n-1}^2} \qquad \text{since } q_{n-1} < q_n. \end{aligned}$$
Since $\lim_{n\to\infty} q_n = \infty$, this implies that $\lim_{n\to\infty} \left| x - \frac{p_n}{q_n} \right| = 0$ as required.

Problem 2

Chapter 3, #35
Denote the Euclidean Algorithm as
$$\begin{aligned} a &= b q_0 + r_0 \\ b &= r_0 q_1 + r_1 \\ r_0 &= r_1 q_2 + r_2 \\ &\vdots \\ r_{k-2} &= r_{k-1} q_k + r_k \\ r_{k-1} &= r_k q_{k+1} + 0 \end{aligned}$$
where $0 \le r_i < r_{i-1}$. Also, let $x_0 = a/b$, $a_i = \lfloor x_i \rfloor$, and $x_{i+1} = \frac{1}{x_i - a_i}$. We must show that $a_i = q_i$ for all $i \ge 0$.

For $i = 0$, we have
$$a_0 = \left\lfloor \frac{a}{b} \right\rfloor$$

Problem 2 continued on next page. . .

and

$$\begin{aligned} a &= bq_0 + r_0 \quad 0 \le r_0 < b \\ \frac{a}{b} &= q_0 + \frac{r_0}{b} \quad 0 \le \frac{r_0}{b} < 1 \\ \left\lfloor \frac{a}{b} \right\rfloor &= q_0 \end{aligned}$$

since $q_0 \in \mathbb{Z}$. Thus, $a_0 = q_0$.

Applying the same argument for arbitrary i, we obtain

$$\begin{aligned} r_{i-2} &= r_{i-1}q_i + r_i \qquad 0 \le r_i < r_{i-1} \\ \frac{r_{i-2}}{r_{i-1}} &= q_i + \frac{r_i}{r_{i-1}} \qquad 0 \le \frac{r_i}{r_{i-1}} < 1 \\ \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor &= q_i \qquad \text{since } q_i \in \mathbb{Z}. \end{aligned}$$

Also, assume $x_{k-1} = \frac{r_{k-3}}{r_{k-2}}$ and $a_{k-1} = q_{k-1}$ for some $k = n$ where $n \ge 1$. Then

$$\begin{aligned} x_k &= \frac{1}{x_{k-1} - a_{k-1}} \\ &= \frac{1}{\frac{r_{k-3}}{r_{k-2}} - q_{k-1}} \\ &= \frac{r_{k-2}}{r_{k-3} - q_{k-1}r_{k-2}} \\ &= \frac{r_{k-2}}{r_{k-1}}. \end{aligned}$$

Thus, $a_i = \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor$ for all $i \ge 0$. Therefore, $a_i = q_i$ for all $i \ge 0$.

Problem 3

Chapter 6, #12
We have

$$51607^2 \equiv 7 \pmod{n}$$

Multiplying by 2^2, we obtain

$$\begin{aligned} 2^2 51607^2 &\equiv 2^2 7 \pmod{n} \\ 1032214^2 &\equiv 187722^2 \pmod{n}. \end{aligned}$$

Since $1032214 \equiv 389813 \not\equiv \pm 187722 \pmod{n}$, the $\gcd(1032214 - 187722, n)$ is a factor of n. We obtain $n = 1129 \cdot 569$ as the prime factorization of n.

Problem 4

Chapter 6, #13
Let $n = 2288233$. Note that

$$\begin{aligned} 880525^2 \cdot 2057202^2 \cdot 648581^2 &\equiv 2 \cdot 3 \cdot 6 \pmod{n} \\ (880525 \cdot 2057202 \cdot 648581)^2 &\equiv 6^2 \pmod{n} \\ a^2 &\equiv b^2 \pmod{n}. \end{aligned}$$

Since $a \not\equiv \pm b \pmod{n}$, $\gcd(a - b, n)$ is a factor of n.

Problem 5

Chapter 6, #14
Since p, q are coprime, use the Chinese Remainder Theorem to find the unique solution $x \bmod pq$ to the system

$$x \equiv 7 \pmod{p}$$
$$x \equiv -7 \pmod{q}.$$

For the sake of contradiction, suppose $x \equiv 7 \pmod{pq}$. Then, $7 \equiv -7 \pmod{q} \iff 14 = kq$ for some $k \in \mathbb{Z}$. The possible values for q are 1, 2, 7, and 14. But, q is a large prime! Thus, $x \not\equiv 7 \pmod{pq}$. Similarly, $x \not\equiv -7 \pmod{pq}$. Lastly, note that x satisfies

$$x^2 \equiv 49 \pmod{p}$$
$$x^2 \equiv 49 \pmod{q}$$

which implies that

$$x^2 \equiv 49 \pmod{pq}$$

since p and q are coprime.

Problem 6

Chapter 6, #23
We claim that $d = e^{-1} \pmod{12345}$ (which can be found using the Euclidean Algorithm). That is, $ed \equiv 1 \pmod{12345} \iff ed = 1 + 12345k$ for some $k \in \mathbb{Z}$. We verify that this decryption key works:

$$c^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{1+12345k} \equiv (m^{12345})^k \cdot m \equiv m \pmod{n}$$

since $m^{12345} \equiv 1 \pmod{n}$.

Problem 7

Chapter 6, #26
We are given two ciphertexts c_a and c_b where

$$c_a \equiv m^e \pmod{n}$$

and

$$c_b \equiv m^e \pmod{p}$$
$$c_b \equiv m^e + 1 \pmod{q}.$$

Since $n = pq$,

$$c_a \equiv m^e \pmod{p}$$
$$c_a \equiv m^e \pmod{q}.$$

Subtracting these congruences, we obtain

$$c_b - c_a \equiv 0 \pmod{p} \implies p \mid c_b - c_a$$
$$c_b - c_a \equiv 1 \pmod{q} \implies q \nmid c_b - c_a.$$

The factors of n are 1, p, q, and n. Since $p \mid c_b - c_a$ but $q \nmid c_b - c_a$, the $\gcd(c_b - c_a, pq) = p$. Compute $q = n/p$.

Problem 8

Chapter 6, #28

(a) Define $s = \lceil\sqrt{n}\rceil = \sqrt{n} + e \in \mathbb{Z}$ with $0 \leq e < 1$. Clearly, $s < \sqrt{n} + 1$ so $x + s < x + \sqrt{n} + 1$. Also, since $x < (\sqrt{2} - 1)\sqrt{n} - 1$, we have $x + \sqrt{n} + 1 < ((\sqrt{2} - 1)\sqrt{n} - 1) + \sqrt{n} + 1 = \sqrt{2n}$. Thus, $x + s < x + \sqrt{n} + 1 < \sqrt{2n}$. This implies $f(x) = (x + s)^2 - n < n$.

Since f is an increasing function, we must show that when $x = 0$, $f(x) \geq 0$. Since $f(0) = s^2 - n$, we must show that $s^2 - n \geq 0 \iff s^2 \geq n$. To see this, note $s^2 = (\sqrt{n} + e)^2 \geq n$ when $0 \leq e < 1$.

Therefore, $0 \leq f(x) < n$.

(b) Write $p \mid f(x)$ as $p \mid (x+s)^2 - n \iff kp = (x+s)^2 - n$ for some $k \in \mathbb{Z}$. Rewrite as $n = (x+s)^2 - kp \iff n \equiv (x + s)^2 \pmod{p}$ as required.

(c) Let $n \equiv a^2 \pmod{p}$ for some $a \in \mathbb{Z}$. Since $p \nmid n$, we have $a^2 \not\equiv 0 \pmod{p} \implies a \not\equiv 0 \pmod{p}$. We have

$$\begin{aligned} f(x) &\equiv 0 \pmod{p} \\ (x + s)^2 - n &\equiv 0 \pmod{p} \\ (x + s)^2 - a^2 &\equiv 0 \pmod{p} \\ (x + s + a)(x + s - a) &\equiv 0 \pmod{p}. \end{aligned}$$

Since p is prime, either $x + s + a = 0$ or $x + s - a = 0 \pmod{p}$. Let $x_{p,1} \equiv a - s \pmod{p}$ and $x_{p,2} \equiv -a - s \pmod{p}$. Since $p \nmid 2$ and $a \not\equiv 0 \pmod{p} \implies p \nmid a$, we have $x_{p,1} - x_{p,2} \equiv 2a \not\equiv 0 \pmod{p}$. That is, $x_{p,1}$ and $x_{p,2}$ are unique mod p. Furthermore, since p is prime and $f(x)$ has degree 2, no further roots exist.

(d) Suppose $f(x)$ is a product of k distinct primes in B. Then $f(x) = b_1 b_2 \cdots b_k$. If $x \equiv x_{p,1}$ or $x_{p,2} \pmod{p}$, then $f(x) \equiv 0 \pmod{p} \iff p \mid f(x)$. That is, for all factors of $f(x)$ subtract

$$\log(f(x)) - [\log(b_1) + \log(b_2) + \ldots + \log(b_k)] = \log\left(\frac{f(x)}{b_1 b_2 \cdots b_k}\right) = \log(1) = 0$$

as required.

(e) If $f(x)$ is a product of (possibly nondistinct) primes in B, then the sieve will still divide off *one of each distinct prime* from $f(x)$. We expect the residual to be small since repeated factors tend to be smaller.

On the other hand, if $f(x)$ is the product of some $p \notin B$, then the register will not be reduced by that p. Additionally, the register will be big since the $p \notin B$ are large.

(f) Part (d) only checks congruence to $x \equiv x_{p,1}$ and $x_{p,2} \pmod{p}$ for each x while trial division requires looping through all p for each x.

Subtraction is a less expensive computation than division.

MATH 404 — Homework #8

Due March 28, 2024

Maxwell Lin

Problem 1

Chapter 7, #1

(a) Through brute-force, we obtain

$$2^4 \equiv 16 \equiv 3 \pmod{13}$$

so $\mathscr{L}_2(3) = 4$.

(b) We check

$$2^7 \equiv 128 \equiv 11 \pmod{13}$$

so $\mathscr{L}_2(11) = 7$.

Problem 2

Chapter 7, #2

(a) Since $6^2 \equiv 3 \pmod{11}$ and $6^4 \equiv 9 \pmod{11}$, we have $6^5 \equiv 6 \cdot 9 \equiv 54 \equiv 10 \pmod{11}$.

(b) Since 2 is a generator for $(\mathbb{Z}/11\mathbb{Z})^*$, $2^{\frac{p-1}{2}} \equiv 2^5 \equiv -1 \pmod{11}$. We have

$$2^x \equiv 6 \pmod{11}$$
$$(2^x)^5 \equiv 6^5 \equiv 10 \equiv -1 \pmod{11}.$$

Therefore $(2^x)^5 \equiv (2^5)^x \equiv (-1)^x \equiv -1$ so x must be odd.

Problem 3

Chapter 7, #3
We have

$$5^x \equiv 3 \pmod{1223}$$
$$(5^x)^{611} \equiv 3^{611} \equiv 1 \pmod{1223}.$$

Since 5 is a generator for $(\mathbb{Z}/1223\mathbb{Z})^*$, $5^{611} \equiv -1 \pmod{1223}$. Therefore, $(5^x)^{611} \equiv (5^{611})^x \equiv (-1)^x \equiv 1$. Thus, x is even.

Problem 4

Chapter 7, #4
Let $p = 19$, $g = 2$, and $y = 14$. We know that $p - 1 = 3^2 \cdot 2$.
Let $q = 3$ and $r = 2$. Then, $y^{\frac{p-1}{q}} \equiv 7 \pmod{p}$ and $g^{\frac{p-1}{q}} \equiv 7 \pmod{p}$. Therefore, $x_0 = 1$. Let $y_1 \equiv yg^{-x_0} \equiv 7 \pmod{p}$. Then, $y_1^{\frac{p-1}{q^2}} \equiv 11 \pmod{p}$ and $(g^{\frac{p-1}{q}})^2 \equiv 11 \pmod{p}$ so $x_1 = 2$. Therefore, $\mathscr{L}_2(14) = 1 + 2(3) = 7 \pmod{9}$.
Now let $q = 2$ and $r = 1$. Then, $y^{\frac{p-1}{q}} \equiv 18 \pmod{p}$ and $g^{\frac{p-1}{q}} \equiv 18 \pmod{p}$ so $x_0 = 1$ and $\mathscr{L}_2(14) = 1 \pmod{2}$.
Applying the CRT to

$$\mathscr{L}_2(14) = 7 \pmod{9}$$
$$\mathscr{L}_2(14) = 1 \pmod{2}$$

we obtain $\mathscr{L}_2(14) = 7 \pmod{18}$.

Problem 5

Chapter 7, #5

(a) We know that

$$\alpha^{\mathscr{L}_\alpha(\beta_1\beta_2)} \equiv \beta_1\beta_2 \equiv \alpha^{\mathscr{L}_\alpha(\beta_1)}\alpha^{\mathscr{L}_\alpha(\beta_2)} \equiv \alpha^{\mathscr{L}_\alpha(\beta_1)+\mathscr{L}_\alpha(\beta_2)} \pmod{p}.$$

Since α is a primitive root mod p, it must be that $\mathscr{L}_\alpha(\beta_1\beta_2) \equiv \mathscr{L}_\alpha(\beta_1) + \mathscr{L}_\alpha(\beta_2) \pmod{p-1}$.

(b) From (a), we know that

$$\alpha^{\mathscr{L}_\alpha(\beta_1\beta_2)} \equiv \alpha^{\mathscr{L}_\alpha(\beta_1)+\mathscr{L}_\alpha(\beta_2)} \pmod{p}$$
$$\alpha^{\mathscr{L}_\alpha(\beta_1\beta_2)-(\mathscr{L}_\alpha(\beta_1)+\mathscr{L}_\alpha(\beta_2))} \equiv 1 \pmod{p}$$

Therefore, $\mathrm{ord}_p(\alpha) \mid \mathscr{L}_\alpha(\beta_1\beta_2) - (\mathscr{L}_\alpha(\beta_1) + \mathscr{L}_\alpha(\beta_2)) \iff \mathscr{L}_\alpha(\beta_1\beta_2) \equiv \mathscr{L}_\alpha(\beta_1) + \mathscr{L}_\alpha(\beta_2) \pmod{\mathrm{ord}_p(\alpha)}$.

Problem 6

Chapter 7, #9

Problem 6 continued on next page. . .

$3^k \equiv 2 \pmod{65537}$

$p = 65537 \quad g = 3 \quad \beta = 2$

$65536 = 2^{16}$

$q = 2 \quad r = 16$

$\beta^{\left(\frac{p-1}{q}\right)} \equiv 1 \pmod p \quad \left(g^{\frac{p-1}{q}}\right)^0 \equiv 1 \pmod p \Rightarrow x_0 = 0$

$\beta_1 \equiv \beta g^{-x_0} \equiv 2(3)^0 \equiv 2$

$\beta_1^{\frac{p-1}{q^2}} \equiv 1 \quad$ so $\quad x_1 = 0$

$\beta_2 \equiv \beta_1 g^{-x_1 q^1} \equiv 2$

$\beta_2^{\frac{p-1}{q^3}} \equiv 1 \quad$ so $\quad x_2 = 0$

$\beta_3 \equiv \beta_2 g^{-x_2 q^2} \equiv 2$

$\beta_3^{\frac{p-1}{q^4}} \equiv 1 \quad$ so $\quad x_3 = 0$

$\beta_4 \equiv \beta_3 g^{-x_3 q^3} \equiv 2$

$\beta_4^{\frac{p-1}{q^5}} \equiv 1 \quad$ so $\quad x_4 = 0$

$\beta_5 = \beta_4 g^{-x_4 q^4} = 2$

$\beta_5^{\frac{p-1}{q^6}} = 1 \quad$ so $\quad x_5 = 0$

$\beta_6 = \beta_5 g^{-x_5 q^5} = 2$

$\beta_6^{\frac{p-1}{q^7}} \equiv 1 \quad$ so $\quad x_6 = 0$

$\beta_7 = 2$

$\beta_7^{\frac{p-1}{q^8}} = 1 \quad x_7 = 0$

$\beta_8 = 2$

$\beta_8^{\frac{p-1}{q^9}} \equiv 1 \quad x_8 = 0$

$\beta_9 = 2$

$\beta_9^{\frac{p-1}{q^{10}}} = 1 \quad x_9 = 0$

$\beta_{10} = 2$

$\beta_{10}^{\frac{p-1}{q^{11}}} = 1 \quad x_{10} = 0$

$\beta_{11} = 2$

(a)

$\left(\beta_{11}^{\frac{p-1}{q^{12}}}\right) \equiv -1 \qquad g^{\frac{p-1}{q}} = -1$ so $x_{11} = 1$

$\beta_{12} = \beta_{11} g^{-x_{11} q^{11}} = 2(3)^{-1(2^{11})} \equiv 16384$

$\beta_{12}^{\left(\frac{p-1}{q^{13}}\right)} \equiv -1$ so $x_{12} = 1$

$\beta_{13} = \beta_{12} g^{-x_{12} q^{12}} = 256$

$\beta_{13}^{\frac{p-1}{q^{14}}} = 1$ so $x_{13} = 0$

$\beta_{14} = 256$

$\beta_{14}^{\frac{p-1}{q^{15}}} = -1$ so $x_{14} = 1$

$\beta_{15} = \beta_{14} g^{-x_{14} q^{14}} = -1$

$(\beta_{15})^{\frac{p-1}{q^{16}}} = -1$ so $x_{15} = 1$

$\boxed{k = 2^{11} + 2^{12} + 2^{14} + 2^{15} = 55296}$

(b)

Problem 7

Chapter 7, #10
Since $\gcd(b, p-1) = 1$, Eve can compute $b' :\equiv b^{-1} \pmod{p-1}$. Then

$$x_2^{b'} \equiv (\alpha^b)^{b'} \equiv \alpha^{bb'} \equiv \alpha \pmod{p}.$$

MATH 404 — Homework #9

Due April 4, 2024

Maxwell Lin

Problem 1

Chapter 7, #6

(a) Since $24 = 2^3 \cdot 3$,

$$\mathscr{L}_2(24) \equiv 3 + \mathscr{L}_2(3) \equiv 72 \pmod{100}.$$

(b) Since $24 \equiv 5^3 \pmod{101}$,

$$\mathscr{L}_2(24) \equiv 3\mathscr{L}_2(5) \equiv 72 \pmod{100}.$$

Problem 2

Chapter 7, #7
We have

$$\begin{aligned} 3^6 &\equiv 44 \pmod{137} \\ 3^6(3^{-10})^2 &\equiv 44 \cdot (2^{-1})^2 \pmod{137} \\ 3^{-14} &\equiv 11 \pmod{137} \\ 3^{122} &\equiv 11 \pmod{137} \qquad \text{since } -14 \equiv 122 \pmod{136}. \end{aligned}$$

So $x = 122$.

Problem 3

Chapter 7, #8

(a) This is the discrete log problem which is hard. Eve can use an algorithm like Pohlig–Hellman to try to determine the password, but it would still take a long time since p is 500 digits long.

(b) In the worst case, $p = 99991$. Using a naive approach, you would need to brute-force up to 99990 possibilities. But this can be done quickly today.

Problem 4

Chapter 7, #11
We have

$$m \equiv tr^{-a} \equiv (6)(7)^{-6} \equiv 12 \pmod{17}.$$

Problem 5

Chapter 7, #12

(a) If $0 \leq d < N^2$, then we can write $d = j + Nk$ with $0 \leq j, k < N$. Then, $m \equiv c^d \equiv c^{j+Nk} \pmod{n} \iff c^j \equiv mc^{-Nk} \pmod{n}$ so a match will exist between the two lists.

(b) If $m = 1$ and $c = 1$, then the two lists match for all $0 \leq j, k < N$. Therefore, we would obtain all d such that $0 \leq d < N^2$. Not all d in this range can be the decryption exponent.

(c) The lists are length $O(\sqrt{n})$ which is the same complexity as factoring n by trial division. There are factoring methods faster than this.

MATH 404 — Homework #10

Due April 11, 2024

Maxwell Lin

Problem 1

Chapter 16, #1

(a) Factor the polynomial to obtain

$$\begin{aligned} x^3 + ax^2 + bx + c &= (x - r_1)(x - r_2)(x - r_3) \\ &= (-r_1 - r_2 - r_3)x^2 + \cdots . \end{aligned}$$

Therefore, $r_1 + r_2 + r_3 = -a$.

(b) We have

$$\begin{aligned} x_1^3 + b'x_1 + c' &= \left(x + \frac{a}{3}\right)^3 + \left(b - \frac{1}{3}a^2\right)\left(x + \frac{a}{3}\right) + \left(c - \frac{1}{3}ab + \frac{2}{27}a^3\right) \\ &= \left(\frac{27x^3 + 27ax^2 + 9xa^2 + a^3}{27}\right) + \left(bx + \frac{ba - a^2x}{3} - \frac{a^3}{9}\right) + \left(c - \frac{1}{3}ab + \frac{2}{27}a^3\right) \\ &= x^3 + ax^2 + bx + c. \end{aligned}$$

Problem 2

Chapter 16, #2

(a) $(3,2), (3,5), (5,2), (5,5), (6,2), (6,5), \infty$.

(b) The line through $(3,2)+(5,5)$ is $y = 5(x-3)+2$. Substituting into E, we obtain $(5(x-3)+2)^2 = x^3 - 2$. We obtain $-25x^2 + \cdots = 0$. Therefore, the sum of the roots is $x + 3 + 5 = 25$ and we obtain the point $(3,2)$. Reflecting about the y-axis, we obtain $(3,5)$.

(c) We differentiate $2y\,dy = 3x^2\,dx \implies \frac{dy}{dx} = \frac{3x^2}{2y}$. Evaluating at $(3,2)$ we obtain $27/4 \equiv 5$. Therefore, the tangent line at $(3,2)$ is $y = 5(x-3)+2$. This is the same line as Part (b). Therefore, the sum of the roots is $x + 3 + 3 = 25$ and we obtain the point $(5,5)$. Reflecting about the y-axis, we obtain $(5,2)$.

Problem 3

Chapter 16, #3

We know that $-(x,0) = (x,-0) = (x,0)$. Since ∞ is the identify element of the group E, $2P = (x,0) + (x,0) = 0_E = \infty$.

Problem 4

Chapter 16, #4
We add $(3,5)+(3,5)$ to obtain a new point on E. The tangent line to $(3,5)$ is $y = \frac{27}{10}(x-3)+5$. Substituting in E, we obtain $(\frac{27}{10}(x-3)+5)^2 = x^3 - 2$. Thus, $-\frac{729}{100}x^2 + \cdots = 0$ and the sum of roots is $3+3+x = \frac{729}{100}$. We obtain $(\frac{129}{100}, \frac{383}{1000})$. Reflect about the y-axis to get $(\frac{129}{100}, -\frac{383}{1000})$.

Problem 5

Chapter 16, #9
Let Q be a point on $E \pmod{n}$. Given $P = xQ$, Eve wants to find x. Eve chooses a bound N such that $N^2 \geq \#E$. By Hasse's Theorem, $|\#E - (p+1)| < 2\sqrt{p}$ so $N^2 \geq 2\sqrt{p} + p + 1 > \#E$. She makes two lists:

1. jQ for $0 \leq j < N$
2. $P - NkQ$ for $0 \leq k < N$.

If a match occurs then

$$\begin{aligned} jQ &= P - NkQ \\ (j+Nk)Q &= P \\ x &= j + Nk. \end{aligned}$$

Since $j + Nk \in \{0, 1, \ldots, N^2 - 1\}$ and $N^2 \geq \#E$, a match will exist.

Problem 6

Chapter 16, #15

(a) Since $k \equiv k' \pmod{2^n}$, we can write $k = k' + 2^n l$ for $l \in \mathbb{Z}$. Then

$$\begin{aligned} B &= kA \\ &= (k' + 2^n l)A \\ &= k'A + 2^n lA \\ &= k'A + (2^n A)l \\ &= k'A + \infty l \\ &= k'A + \infty \\ &= k'A. \end{aligned}$$

(b) If j is even

$$\begin{aligned} jT &= j2^{n-1}A \\ &= 2^{n-1}A + 2^{n-1}A + \cdots + 2^{n-1}A + 2^{n-1}A \qquad j \text{ times} \\ &= 2(2^{n-1}A) + \cdots + 2(2^{n-1}A) \qquad j/2 \text{ times} \\ &= 2^n A + \cdots + 2^n A \qquad j/2 \text{ times} \\ &= \infty + \cdots + \infty \qquad j/2 \text{ times} \\ &= \infty. \end{aligned}$$

Problem 6 continued on next page. . .

If j is odd

$$\begin{aligned} jT &= (2^n A + \cdots + 2^n A) + 2^{n-1} A \\ &= 2^{n-1} A \\ &\neq \infty. \end{aligned}$$

(c) We have $x_0 = 0 \iff k$ even $\iff kT = \infty$. Also, $\infty = kT = k2^{n-1}A = 2^{n-1}(kA) = 2^{n-1}B$.

(d) We have

$$\begin{aligned} 2^{n-m-1}(B - (x_0 + \cdots + 2^{m-1}x_{m-1})A) &= 2^{n-m-1}(2^m x_m + \cdots + 2^{n-1}x_{n-1})A \\ &= 2^{n-1}(x_m + \cdots + 2^{n-m-1}x_{n-1})A \\ &= T(x_m + \cdots + 2^{n-m-1}x_{n-1}) \end{aligned}$$

which is ∞ if and only if $x_m = 0$.

Problem 7

Chapter 16, #16

(a) We have $3d \equiv 1 \pmod{p-1} \iff \gcd(3, p-1) = 1 \iff 3 \nmid (p-1)$. Since $3 \mid (p+1)$, we cannot also have $3 \mid (p-1)$ so therefore, $3d \equiv 1 \pmod{p-1}$.

(b) ($\implies$) We have $(a^3)^d \equiv a^{3d} \equiv a^1 \equiv a \pmod{p}$ since $3d \equiv 1 \pmod{p-1}$. Thus, $b^d \equiv (a^3)^d \equiv fa \pmod{p}$.
($\impliedby$) We have $(b^d)^3 \equiv b^{3d} \equiv b^1 \equiv b \pmod{p}$ since $3d \equiv 1 \pmod{p-1}$. Thus, $a^3 \equiv (b^d)^3 \equiv b \pmod{p}$.

(c) By (b), $x^3 \equiv y^2 - 1 \pmod{p} \iff x \equiv (y^2-1)^d \pmod{p}$. Therefore, every value of y has a unique x mod p. Since there are p values of y, there are p points (excluding ∞). Thus, there are a total of $p+1$ points on E.

MATH 404 — Homework #11

Due April 18, 2024

Maxwell Lin

Problem 1

Chapter 16, #6

(a) We compute $2P = (10, 9) + (10, 9) = (5, 16)$. Next, we compute $3P = (10, 9) + (5, 16)$. The slope is $m = \frac{7}{30}$. However, 30 is not invertible mod 35 since $\gcd(30, 35) = 5$. Thus, $35 = 5 \cdot 7$.

(b) The slope of the tangent line at P is $\frac{8}{21}$. However, 21 is not invertible mod 35 since $\gcd(21, 35) = 7$. Thus, $35 = 7 \cdot 5$.

Problem 2

Chapter 16, #7
We compute $2P = (2, 0) + (2, 0)$. The slope of the tangent line at $(2, 0)$ is $\frac{8}{0}$ so $2P = \infty$. Computing $\gcd(0, n) = n$ provides no useful information to factor n.

Problem 3

Chapter 16, #8
Choose an elliptic curve E mod p and a point Q on E with high order. If x is the password, then the point xQ is stored in a file. When y is given as a password, the point yQ is compared with xQ. Recovering x from xQ is hard since the elliptic curve discrete log problem is hard.

Problem 4

Chapter 16, #11

(a) Since the elliptic curve is over $\mathbb{Z}/n\mathbb{Z}$, the size of E can be at most $n^2 + 1$ (including ∞). Therefore, there are only finitely many points on E.

(b) Since E is a finite group, there exists some $j \in \mathbb{Z}^+$ such that $jP = \infty$ (Homework #4, Problem 1). Let $i = 2j$. Then $iP = (2j)P = 2(jP) = 2(\infty) = \infty$. Thus, $iP = jP$. We also have $(i - j)P = (2j - j)P = jP = \infty$.

(c) Write $m = kq + r$ with $0 \leq r < k$. Then

$$\infty = mP = (kq + r)P = kqP + rP = \infty + rP = rP.$$

Since $0 \leq r < k$ and k is the order of P, it must be that $r = 0$. Therefore, $m = kq \iff k \mid m$.

(d) Let m be the number of points on E. Lagrange's theorem says that $mP = \infty$. By (c), $\text{ord}(P) \mid m$.

Problem 5

Chapter 16, #13 (a)
We induct on w, the length of the binary representation of x. Consider the bitstrings of length 1:

1. If $x = 0$, then $R_1 = \infty = 0P$ as required.
2. If $x = 1$, then $R_1 = \infty + P = 1P$ as required.

Now fix $w \in \mathbb{Z}$ with $w \geq 1$ and let $x = b_1 b_2 \cdots b_w$ be an arbitrary bitstring of length w. Assume that this algorithm works on x and outputs $R_w = xP$. Now let $x' = b_1 b_2 \cdots b_w b_{w+1}$. We need to show that this algorithm works on x' and outputs $R_{w+1} = x'P$. We split into two cases:

1. If $b_{w+1} = 0$, then $x' = 2x$. We know $R_w = xP$ so $S_{w+1} = 2R_w = 2xP$. Then, $R_{w+1} = S_{w+1} = 2xP = x'P$ as required.
2. If $b_{w+1} = 1$, then $x' = 2x + 1$. We know $R_w = xP$ so $S_{w+1} = 2R_w = 2xP$. Then, $R_{w+1} = S_{w+1} + P = 2xP + P = (2x + 1)P = x'P$ as required.

Thus, this algorithm outputs $R_w = xP$ for all $x \in \mathbb{N}$.

MATH 404 — Homework #12

Due April 30, 2024

Maxwell Lin

Problem 1

Chapter 9, #1
Eve solves

$$ar \equiv m - ks \pmod{p-1}$$

for a. There are $\gcd(r, p-1)$ possibilities which is small. For each possible a, Eve computes $\alpha^a \pmod{p}$ until she obtains β in which case she has found a.

Problem 2

Chapter 9, #2

(a) Choose $m_1 \equiv r^h m r^{-1} \pmod{p-1}$. Then,

$$\begin{aligned} \beta^{r_1} r_1^{s_1} &\equiv \alpha^{a\alpha^{kh}} \alpha^{(m-ar)\alpha^{kh} r^{-1}} \\ &\equiv \alpha^{\alpha^{kh} m r^{-1}} \\ &\equiv \alpha^{r^h m r^{-1}} \\ &\equiv \alpha^{m_1}. \end{aligned}$$

(b) Eve can only control h when she chooses m_1. To find an h such that $r^h m r^{-1} \pmod{p-1}$ results in a sensible message is the discrete log problem which is hard.

Problem 3

Chapter 9, #4

(a) We have

$$\begin{aligned} (\alpha^a)^s r^r &\equiv \alpha^{a(a^{-1}(m-kr))} r^r \\ &\equiv \alpha^{m-kr} r^r \\ &\equiv \alpha^m r^{-r} r^r \\ &\equiv \alpha^m \pmod{p}. \end{aligned}$$

(b) We have

$$\begin{aligned} \alpha^s &\equiv \alpha^{am+kr} \\ &\equiv (\alpha^a)^m r^r \pmod{p}. \end{aligned}$$

(c) We have

$$\begin{aligned} \alpha^s &\equiv \alpha^{ar+km} \\ &\equiv (\alpha^a)^r r^m \pmod{p}. \end{aligned}$$

Problem 4

Chapter 9, #6

Eve notices that $r \equiv \alpha^a \equiv \beta \pmod{p}$. Since $k = a$, Eve knows that $s = k^{-1}(m - ar) \equiv k^{-1}(m - kr) \equiv k^{-1}m - r \pmod{p-1}$. Thus, Eve solves

$$(s + r)k \equiv m \pmod{p-1}$$

for k. There are $\gcd(s + r, p - 1)$ possibilities which is small. For each possible k, Eve computes $\alpha^k \pmod{p}$ until she obtains β in which case she has found $k = a$.

Problem 5

Chapter 9, #8

(a) Since $s \equiv k^{-1}(m - f(r)a) \pmod{p-1}$, we have $af(r) + ks \equiv m \pmod{p-1}$. Thus

$$\begin{aligned} \beta^{f(r)} r^s &\equiv \alpha^{af(r)} \alpha^{ks} \\ &\equiv \alpha^{af(r)+ks} \\ &\equiv \alpha^m \pmod{p}. \end{aligned}$$

(b) Eve needs to choose k and s such that $ks \equiv m \pmod{p-1}$. Then

$$\begin{aligned} \beta^{f(r)} r^s &\equiv \alpha^{ks} \\ &\equiv \alpha^m \pmod{p}. \end{aligned}$$

For example, let $k = 1$, $r = \alpha$, and $s = m$.

Problem 6

Chapter 19, #1

(a) The period is 4.

(b) Pick $m = 8$ so that $n^2 \leq 2^m < 2n^2$.

(c) Since $c = 192$, we have

$$\frac{c}{2^m} = \frac{192}{256} = \frac{3}{4} = \frac{j}{r}$$

so $r = 4$. This agrees with part (a).

(d) We use the exponent factorization method. Write $r = (2^2)(1)$. Then (in mod 15),

$$\begin{aligned} b_0 &\equiv 2^1 \equiv 2 \\ b_1 &\equiv b_0^2 \equiv 4 \\ b_2 &\equiv b_1^2 \equiv 1. \end{aligned}$$

Thus, $\gcd(b_1 - 1, n) = 3$ gives a nontrivial factor for $n = 15$.

Problem 7

Chapter 19, #2

(a) Write $c = c_0 + j2^s$ with $0 \le j < 2^{m-s}$. If $x \not\equiv 0 \pmod{2^{m-s}}$, then

$$\begin{aligned}\sum_{\substack{0\le c<2^m\\ c\equiv c_0 \pmod{2^s}}} e^{\frac{2\pi icx}{2^m}} &= \sum_{0\le j<2^{m-s}} e^{\frac{2\pi ix}{2^m}(c_0+j2^s)}\\ &= e^{\frac{2\pi ixc_0}{2^m}} \sum_{0\le j<2^{m-s}} e^{\frac{2\pi ixj2^s}{2^m}}\\ &= e^{\frac{2\pi ixc_0}{2^m}} \frac{e^{2\pi ix}-1}{e^{2^{s-m+1}\pi ix}-1}\\ &= 0\end{aligned}$$

since $e^{2\pi ix} - 1 = 0$ and $e^{2^{s-m+1}\pi ix} - 1 \neq 0$.

If $x \equiv 0 \pmod{2^{m-s}}$, then

$$\begin{aligned}\sum_{\substack{0\le c<2^m\\ c\equiv c_0 \pmod{2^s}}} e^{\frac{2\pi icx}{2^m}} &= \sum_{0\le j<2^{m-s}} e^{\frac{2\pi ix}{2^m}(c_0+j2^s)}\\ &= e^{\frac{2\pi ixc_0}{2^m}} \sum_{0\le j<2^{m-s}} e^{\frac{2\pi ixj2^s}{2^m}}\\ &= e^{\frac{2\pi ixc_0}{2^m}} \sum_{0\le j<2^{m-s}} 1\\ &= 2^{m-s}e^{\frac{2\pi ixc_0}{2^m}}.\end{aligned}$$

(b) Note that for a fixed c_0

$$\sum_{\substack{0\le c<2^m\\ c\equiv c_0 \pmod{2^s}}} e^{\frac{2\pi icx}{2^m}} a_{c_0} = a_{c_0} \sum_{\substack{0\le c<2^m\\ c\equiv c_0 \pmod{2^s}}} e^{\frac{2\pi icx}{2^m}}$$

since $a_k = a_{k+j2^s}$. Write

$$\begin{aligned}F(x) &= \frac{1}{\sqrt{2^m}} \sum_{c=0}^{2^m-1} e^{\frac{2\pi icx}{2^m}} a_c\\ &= \frac{1}{\sqrt{2^m}} \left[\sum_{c_0=0}^{2^s-1} a_{c_0} \sum_{\substack{0\le c<2^m\\ c\equiv c_0 \pmod{2^s}}} e^{\frac{2\pi icx}{2^m}}\right]\\ &= 0\end{aligned}$$

since $x \not\equiv 0 \pmod{2^{m-s}}$ by part (a).

Problem 8

Chapter 19, #3

Problem 8 continued on next page...

(a) Since $0 < r < n$ and $0 < r_1 < n$, we have $r_1 r < n^2$. Also, since j/r and j_1/r_1 are two distinct rational numbers, $|j_1 r - j r_1| > 1$. Thus,

$$\begin{aligned}\left|\frac{j_1}{r_1} - \frac{j}{r}\right| &= \left|\frac{j_1 r - j r_1}{r_1 r}\right| \\ &= \frac{|j_1 r - j r_1|}{r_1 r} \\ &> \frac{|j_1 r - j r_1|}{n^2} \\ &> \frac{1}{n^2}.\end{aligned}$$

(b) Adding the inequalities, we obtain

$$\left|\frac{c}{2^m} - \frac{j}{r}\right| + \left|\frac{c}{2^m} - \frac{j_1}{r_1}\right| < \frac{1}{n^2}.$$

We bound

$$\left|\frac{j_1}{r_1} - \frac{j}{r}\right| \leq \left|\frac{c}{2^m} - \frac{j}{r}\right| + \left|\frac{c}{2^m} - \frac{j_1}{r_1}\right| < \frac{1}{n^2}.$$

Applying the contrapositive of (a), $j/r = j_1/r_1$.