M/CS 478 Assignment 1

Isaac Boaz

January 24, 2024

Problem 1.2

(a) ITHINKTHATISHALLNEVERSEEABILLBOARDLOVELYASATREE

(b) LOVEISNOTLOVEWHICHALTERSWHENITALTERATIONFINDS

(c) INBAITINGAMOUSETRAPWITHCHEESEALWAYSLEAVEROOMFORTHEMOUSE

Problem 1.4

THESE CHARA CTERS ASONE MIGHT READI LYGUE SSFOR MACIP
HERTH ATIST OSAYT HEYCO NVEYA MEANI NGBUT THENF ROMWH
ATISK NOWNO FCAPT AINKI DDICO ULDNO TSUPP OSEHI MCAPA
BLEOF CONST RUCTI NGANY OFTHE MOREA BSTRU SECRY PTOGR
APHSI MADEU PMYMI NDATO NCETH ATTHI SWASO FASIM PLESP
ECIES SUCHH OWEVE RASWO ULDAP PEART OTHEC RUDEI NTELL
ECTOF THESA ILORA BSOLU TELYI NSOLU BLEWI THOUT THEKE Y

Problem 1.5

For simplicity's sake, I'll be using A, B, C, D as the alphabet.

(a) $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$ possible substitution ciphers

(b) (i) For no fixed letters, A can map to B, C, or D, so...

$3 \cdot 2 \cdot 1 = 6$ possible substitution ciphers that have no letters fixed

(ii) For at least one fixed letter, we have 4 choices for the fixed letter, and then we simply deal with a 3-letter alphabet.

$4 \cdot 3 \cdot 2 \cdot 1 = 24$ possible substitution ciphers that have at least one letter fixed

(iii) For only one fixed letter, we have 4 choices for the fixed letter, and then we simply deal with a 3-letter alphabet. without any fixed letters, so...

$4 \cdot 2 \cdot 1 = 8$ possible substitution ciphers that have exactly one letter fixed

(iv) For exactly two fixed letters, we first have $4 \cdot 3$ choices for the fixed letters, and then we simply deal with a 2-letter alphabet.

$4 \cdot 3 \cdot 1 = 12$ possible substitution ciphers that have exactly two letters fixed

Problem 1.9

(a) gcd(291, 252)

$$\begin{aligned} 291 &= 252(1) + 39 \\ 252 &= 39(6) + 18 \\ 39 &= 6(6) + \mathbf{3} \\ 6 &= 6(1) + 0 \\ &\rightarrow 3 \end{aligned}$$

(b) gcd(16261, 86562)

$$\begin{aligned} 86562 &= 16261(5) + 5257 \\ 16261 &= 5257(3) + 490 \\ 5257 &= 490(10) + 357 \\ 490 &= 357(1) + 133 \\ 357 &= 133(2) + 91 \\ 133 &= 91(1) + 42 \\ 91 &= 42(2) + \mathbf{7} \\ 42 &= 7(7) + 0 \\ &\rightarrow 7 \end{aligned}$$

Problem 1.17

(a) $347 + 513 = 860 \equiv 97 \pmod{763}$

(b) $3264 + 1238 + 7231 + 6437 = 18170 \equiv 8916 \pmod{9254}$

(c) $153 \cdot 287 = 43851 \equiv 79 \pmod{353}$

(d) $357 \cdot 862 \cdot 193 = 59392662 \equiv 1545 \pmod{8157}$

(e) $5327 \cdot 6135 \cdot 7139 \cdot 2187 \cdot 5219 \cdot 1873 = 4.06854 \times 10^{23} \equiv 603 \pmod{8157}$

(f) $137^2 = 18769 \equiv 137 \pmod{327}$

(g) $373^6 = 2693103168443689 \equiv 463 \pmod{581}$

(h) $23^3 \cdot 19^5 \cdot 11^4 = 441084963939653 \equiv 93$

Problem 1.26

(a) $17^{183} \pmod{256}$

$$
\begin{aligned}
183_{10} = 10110111_2 \rightarrow \quad & & 17^2 &= 289 \equiv 33 \\
17^{183} \pmod{256} &\equiv 17^{128} \times 17^{32} \times \cdots & 17^4 &\equiv 33^2 \equiv 65 \\
&\equiv 1 \times 1 \times 1 \times 1 \times 65 \times 33 \times 17 & 17^8 &\equiv 65^2 \equiv 129 \\
&\equiv 36465 & 17^{16} &\equiv 129^2 \equiv 1 \\
&\equiv 113 \pmod{256} & 17^{32} &\equiv 1^2 \equiv 1 \\
& & 17^{64} &\equiv 1^2 \equiv 1 \\
& & 17^{128} &\equiv 1^2 \equiv 1
\end{aligned}
$$

(b) $2^{477} \pmod{1000}$

$$
\begin{aligned}
477_{10} = 111011101_2 \rightarrow \quad & & 2^2 &\equiv 4 \\
2^{477} \pmod{1000} &\equiv 2^{256} \times 2^{128} \times 2^{64} \times 2^{16} \times 2^8 \times 2^4 & 2^8 &\equiv 256 \\
&\equiv 936 \times 456 \times 616 \times 536 \times 256 \times 16 \times 2 & 2^{16} &\equiv 536 \\
&\equiv 272 \pmod{1000} & 2^{32} &\equiv 296 \\
& & 2^{64} &\equiv 616 \\
& & 2^{128} &\equiv 456 \\
& & 2^{256} &\equiv 936
\end{aligned}
$$

(c) $11^{507} \pmod{1237}$

$$
\begin{aligned}
507_{10} = 111111011_2 \rightarrow \quad & & 11^2 &\equiv 121 \\
11^{507} \pmod{1237} &\equiv 11^{256} \times 11^{128} \times 11^{64} \times 11^{32} \times 11^{16} \times 11^8 \times 11^2 & 11^4 &\equiv 1034 \\
&\equiv 380 \times 748 \times 1128 \times 830 \times 867 \times 388 \times 121 \times 11 & 11^8 &\equiv 388 \\
&\equiv 322 \pmod{1237} & 11^{16} &\equiv 867 \\
& & 11^{32} &\equiv 830 \\
& & 11^{64} &\equiv 1128 \\
& & 11^{128} &\equiv 748 \\
& & 11^{256} &\equiv 380
\end{aligned}
$$