Math 139 Solution
Hour Exam II 18 April 2003

---

1. A bowl of alphabet soup is prepared that contains only vowels: there are 25 `A`'s, 35 `E`'s, 20 `I`'s, 18 `O`'s, and 12 `U`'s. We stir the soup thoroughly, and then scoop up a spoonful that contains exactly three letters.

   (a) What is the probability that all three letters in the spoon are the same letter of the alphabet?

   Solution: There are 110 letters in the bowl altogether, so we have $C(110, 3) = 215,820$ possible outcomes for this experiment.

   We can get three `A`'s in $C(25, 3) = 2300$ ways, three `E`'s in $C(35, 3) = 6545$ ways, three `I`'s in $C(20, 3) = 1140$ ways, three `O`'s in $C(18, 3) = 816$ ways, and three `U`'s in $C(12, 3) = 220$ ways. The total number of ways to get three of the same letter is

   $$2300 + 6545 + 1140 + 816 + 220 = 11021.$$

   The probability of this event is

   $$\frac{11021}{215820} \approx 0.051.$$

   (b) What is the probability that two of the letters in the spoon are `E`'s and the other one is not an `E`?

   Solution: There are $C(35, 2) = 595$ ways to get two `E`'s. There are $C(75, 1) = 75$ ways to get a non-`E` for the other letter, so the size of this event is $595 \times 75 = 44625$. The probability is

   $$\frac{44625}{215820} \approx 0.2068.$$

2. Consider the following Vigenère-enciphered text:

```
WEFDM CSACK TNFWW TRKDM
EHFWJ TVQPK ALMCL DFGAD
RRALF WEFDM CDMJY STQGK
TNFWW TREQW LSODJ YEDHL
ZNQHX ZRMES WAOT
```

(a) Use the Kasiski test to determine the most likely length for the keyword. (Hint: there are repeated strings beginning with `WEF` and with `KTN`.)

Solution: We find the string `WEDFMC` occurring twice, separated by a distance of 45 letters, so the keyword length is a factor of 45. We find the string `KTNFWWTR` occurring twice, at a distance of 50 letters. The keyword length is a common factor of 45 and 50, so it must be 1 or 5. We suspect that it's 5.

(b) Determine the keyword, given the following cribs: The first word of the plaintext is `let`, and each of the two occurrences of `FWW` decrypts to `the`.

Solution: Using a cipher disk, we fill in the keyword row in the following:

Plaintext:	l	e	t	.	.		Plaintext:	.	.	t	h	e
Keyword:	L	A	M	.	.	and	Keyword:	.	.	M	P	S
Ciphertext:	W	E	F	D	M		Ciphertext:	T	N	F	W	W

Since the keyword length is 5, we know these two keyword fragments fit together at the central M to form the keyword LAMPS.

3. (a) Let π denote the prime counting function. Use the accompanying table of primes to determine the exact value of $\pi(2100) - \pi(2000)$.

Solution: The number of primes between 2000 and 2100 is 14, so

$$\pi(2100) - \pi(2000) = 14.$$

(b) Use the Prime Number Theorem to estimate the number of primes between $50,000,000$ and $100,000,000$.

Solution: According to the PNT,

$$\begin{aligned} \pi(100,000,000) &\approx \frac{100,000,000}{\ln(100,000,000)} \\ &\approx 5428681 \end{aligned}$$

and

$$\begin{aligned}\pi(50,000,000) &\approx \frac{50,000,000}{\ln(50,000,000)} \\ &\approx 2820471\end{aligned}$$

The difference between these approximations is 2608210.

4. (a) Use the extended Euclidean algorithm to find integers s and t such that

$$415s + 126t = 1.$$

Solution: The steps in the Euclidean algorithm are

$$\begin{aligned}415 &= 3 \times 126 + 37 \\ 126 &= 3 \times 37 + 15 \\ 37 &= 2 \times 15 + 7 \\ 15 &= 2 \times 7 + 1.\end{aligned}$$

Making the back-substitutions, we get

$$\begin{aligned}1 &= 15 - 2 \times 7 \\ &= 15 - 2(37 - 2 \times 15) \\ &= -2 \times 37 + 5 \times 15 \\ &= -2 \times 37 + 5(126 - 3 \times 37) \\ &= 5 \times 126 - 17 \times 37 \\ &= 5 \times 126 - 17(415 - 3 \times 126) \\ &= -17 \times 415 + 56 \times 126.\end{aligned}$$

(b) Given that $66 \times 517 - 149 \times 229 = 1$, solve the congruence

$$229x \equiv 18 \pmod{517}.$$

Solution: The given equation says that $229 \times 149 \equiv -1 \pmod{517}$. Thus the muliplicative inverse of 229 modulo 517 must be

$$-149 \equiv 368 \pmod{517}.$$

Multiplying both sides of the given congruence by 368, we get

$$368 \times 229x \equiv 368 \times 18 \pmod{517}$$

which simplifies to $x \equiv 420 \pmod{517}$.

5. Compute $54^{37} \bmod 1223$.

Solution: We compute the following powers of 54:

$$\begin{aligned} 54^1 &\equiv 54 \pmod{1223} \\ 54^2 &\equiv 470 \pmod{1223} \\ 54^4 &\equiv 760 \pmod{1223} \\ 54^8 &\equiv 344 \pmod{1223} \\ 54^{16} &\equiv 928 \pmod{1223} \\ 54^{32} &\equiv 192 \pmod{1223} \end{aligned}$$

Since $37 = 32 + 4 + 1$, we get

$$\begin{aligned} 54^{37} &\equiv 54^{32} \times 54^4 \times 54 \pmod{1223} \\ &\equiv 192 \times 760 \times 54 \pmod{1223} \\ &\equiv 7879680 \pmod{1223} \\ &\equiv 1114 \pmod{1223}. \end{aligned}$$

Bonus: Given that 107 is prime, that $a^{25} \equiv 30 \pmod{107}$, and that $0 \leq a \leq 106$, find a.

Solution: We first need to invert 25 modulo 106. This is routine – the answer is 17. Then from Fermat's little theorem, we know that $a^{25\times 17} \equiv (a^{25})^{17} \equiv a \pmod{107}$. We calculate

$$30^{17} \equiv 79 \pmod{107}.$$

The answer is 79.