SOLUTIONS TO PROBLEM SET 6

1. Section 8.1

Problem 2. The Caeser cipher uses the encryption function $E(x) = x + 3 \pmod{26}$ whose corresponding decryption function is $D(x) = x - 3 \pmod{26}$. We apply $D$ to the numerical values of the letters to obtain the message

I CAME I SAW I CONQUERED.

Problem 6. We know that the decryption function corresponding to the affine encryption function $E(x) = 3x + 24$ is given by

$$D(y) = cy + d \pmod{26}, \quad \text{where} \quad c = 3^{-1} \equiv 9, \quad d \equiv -9 \cdot 24 \equiv 18.$$ 

Using $D$ to decrypt the message we obtain PHONE HOME.

Problem 8. The most commonly occurring letter in the ciphertext is $V$ (8 occurrences) which has numerical value of 21. It is reasonable to guess this is the image of $E$, the most common letter in English. The numerical value of $E$ is 4, therefore, the decryption function $D(y) = y - k$ must satisfy

$$D(21) = 21 - k \equiv 4 \pmod{26},$$

that is $k = 17$. Using $D$ to decode the ciphertext gives

THE VALUE OF THE KEY IS SEVENTEEN.

Problem 10. The most common letters in English are $E$ and $T$ (in this order), therefore it is reasonable to assume that $E$ is encrypted as $X$ and $T$ is encrypted as $Q$. In terms of the affine encryption function $E(x) = ax + b \pmod{26}$ this gives rise to the congruences

$$4a + b \equiv 23 \pmod{26} \quad \text{and} \quad 19a + b \equiv 16 \pmod{26}.$$ 

Subtracting the first congruence from the second gives $15a \equiv -7 \pmod{26}$, hence $a \equiv 3 \pmod{26}$. Then $b \equiv 23 - 12 \equiv 11 \pmod{26}$.

Thus the most likely values for $a$ and $b$ are $a = 3$ and $b = 11$. 

1
**Problem 12.** The two most frequent letters in the cipher text are $M$ (7 occurrences) and $R$ (6 occurrences). We guess these correspond to $E$ and $T$. In terms of the affine transformation $E(x) = ax + b \pmod{26}$ we get

$$4a + b \equiv 12 \pmod{26} \quad \text{and} \quad 19a + b \equiv 17 \pmod{26}.$$  

Subtracting the first congruence from the second gives $15a \equiv 5 \pmod{26}$. As $(5, 26) = 1$, this is equivalent to $3a \equiv 1 \pmod{26}$, which gives $a \equiv 9 \pmod{26}$.

Thus $b \equiv 12 - 36 \equiv 2 \pmod{26}$. Then the encryption becomes $E(x) = 9x + 2 \pmod{26}$ and its corresponding decryption function is

$$D(y) = a^{-1}y - a^{-1}b = 3y - 6 \pmod{26}.$$  

Using this the message decodes to

EVERY ALCHEMIST OF ANCIENT TIMES KNEW HOW TO TURN LEAD INTO GOLD.

2. Section 3.6

**Problem 4.**

a) 
(i) We have $\sqrt{8051} \approx 89.7$, so $t = 90$ is the smallest integer $\geq \sqrt{8051}$;

(ii) We calculate $90^2 - 8051 = 49 = 7^2$;

(iii) Thus $8051 = 90^2 - 7^2 = (90 - 7)(90 + 7) = 83 \cdot 97$ is the (prime) factorization.

b) 
(i) We have $\sqrt{73} \approx 8.5$, so $t = 9$ is the smallest integer $\geq \sqrt{73}$;

(ii) We calculate

$$9^2 - 73 = 8,$$

$$10^2 - 73 = 27,$$

$$11^2 - 73 = 48,$$

$$12^2 - 73 = 71,$$

$$\vdots$$

$$37^2 - 73 = 1296 = 36^2;$$

(iii) Thus we have that $73 = 37^2 - 36^2 = (37 - 36)(37 + 36) = 1 \cdot 73$ is the only factorization of $73$, hence $73$ is prime.

c) 
(i) We have $\sqrt{46009} \approx 214.5$, so $t = 215$ is the smallest integer $\geq \sqrt{46009}$.

(ii) We calculate

$$215^2 - 46009 = 216,$$

$$216^2 - 46009 = 647,$$

$$217^2 - 46009 = 1080,$$

$$218^2 - 46009 = 1515,$$
\[ 235^2 - 46009 = 9216 = 96^2; \]

(iii) Thus \(46009 = 235^2 - 96^2 = (235 - 96)(235 + 96) = 139 \cdot 331\) is a factorization. Since the two factors are primes we conclude this is the prime factorization.

d)

(i) We have \(\sqrt{11021} \approx 104.98\), so \(t = 105\) is the smallest integer \(\geq \sqrt{11021}\);

(ii) We calculate \(105^2 - 11021 = 4 = 2^2\);

(iii) Thus we have that \(11021 = 105^2 - 2^2 = (105 - 2)(105 + 2) = 103 \cdot 107\) is a factorization. Since the two factors are primes we conclude this is the prime factorization.

3. Section 8.3

**Problem 6.** The encryption function is \(E(x) = x^e \pmod{p = 29}\), where \(e\) is the encryption key which satisfies \((p - 1, e) = (28, e) = 1\). We know that

\[ E(20) \equiv 24 \pmod{29} \iff 20^e \equiv 24 \pmod{29}. \]

We calculate

\[ 20^2 \equiv 400 \equiv -6 \pmod{29}, \]
\[ 20^4 \equiv 36 \equiv 7 \pmod{29}, \]
\[ 20^8 \equiv 49 \equiv 20 \pmod{29}, \]

which shows that \(20^7 \equiv 1 \pmod{29}\); therefore there must be a value \(e' \leq 6\) such that \(20^{e'} \equiv 24 \pmod{29}\). We continue calculating

\[ 20^3 \equiv 54 \equiv 25 \equiv -4 \pmod{29}, \]
\[ 20^5 \equiv 20^2 \cdot 20^3 \equiv (-6) \cdot (-4) \equiv 24 \pmod{29} \]

to find that \(e' = 5\). Note that this is not necessarily the correct encryption key \(e\), but we have that \(e = e' + 7k\).

We guess that our encryption key is \(e = 5\). To find the corresponding decryption key \(d\) we need to solve \(5d \equiv 1 \pmod{\phi(29) = 28}\). We obtain \(d = 17\) as a solution. The decryption function is \(D(y) = y^{17} \pmod{29}\) and the decoded message would become

\[ 061414030620041818 \]

which corresponds to

GOOD GUESS.
Problem 2. Recall that for a quadratic polynomial $ax^2 + bx + c$ its two roots are given by the quadratic resolvent formula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$ 

We note that

$$\phi(n) = \phi(pq) = (p-1)(q-1) = pq - p - q + 1 = n - (p + q) + 1$$

and so

$$-(p + q) = \phi(n) - n - 1.$$ 

Note that $p$ and $q$ are roots of the quadratic polynomial $P(x) = (x-p)(x-q)$, which becomes

$$P(x) = x^2 - (p + q)x + pq = x^2 + (\phi(n) - n - 1)x + n.$$ 

In our case, $n = 4386607$ and $\phi(n) = 4382136$ and this becomes

$$P(X) = x^2 + (4382136 - 4386607 - 1)x + 4386607 = x^2 - 4472x + 4386607.$$ 

Using the resolvent formula, we find the roots $p$ and $q$ of $P(x)$ to be

$$x = \frac{4472 \pm \sqrt{4472^2 - 4 \cdot 1 \cdot 4386607}}{2} = 1453 \text{ and } 3019.$$ 

Problem 8. The encryption key is $(e, n) = (5, 2881)$. We have $2881 = 43 \cdot 67$. Thus $\phi(n) = 42 \cdot 66 = 2772$. Using the Euclidean Algorithm, we compute the decryption key, $d \equiv e^{-1} \pmod{2772}$. This gives $d \equiv 1109 \pmod{2772}$. To decrypt the message, we raise each block in

$$0504 \ 1874 \ 0347 \ 0515 \ 2088 \ 2356 \ 0736 \ 0468$$

to the power of 1109 and reduce modulo 2881. This gives us

$$0400 \ 1902 \ 0714 \ 0214 \ 1100 \ 1904 \ 0200 \ 1004$$

or EAT CHOCOLATE CAKE

Problem 14. Let the moduli be $n_1, n_2, n_3$ and write $n_1 = p_1q_1$, $n_2 = p_2q_2$ and $n_3 = p_3q_3$, with $p_i, q_i$ all prime and $p_i \neq q_i$ for fixed $i$.

First, using Euclidean Algorithm, we compute $\gcd(n_1, n_2)$, $\gcd(n_2, n_3)$, and $\gcd(n_1, n_3)$. If one of these numbers is not 1, say $\gcd(n_1, n_2) \neq 1$, then $n_1$ and $n_2$ have a prime factor in common, say $p_1 = p_2$. Then $\gcd(n_1, n_2) = p_1$ and we have factored $n_1$, thus breaking the code. Thus can assume $\gcd(n_1, n_2) = \gcd(n_1, n_3) = \gcd(n_2, n_3) = 1$, that is, the moduli $n_1$, $n_2$ and $n_3$ are pairwise coprime.

We know that each encryption function is $E_i(x) = x^3 \pmod{n_i}$ and from a plaintext message $P$ we intercepted the three ciphertext messages $C_i$ that satisfy $0 \leq C_i < n_i$ and

$$P^3 \equiv C_1 \pmod{n_1}, \quad P^3 \equiv C_2 \pmod{n_2}, \quad P^3 \equiv C_3 \pmod{n_3}.$$ 

This means that the system of congruences

$$x \equiv C_1 \pmod{n_1}, \quad x \equiv C_2 \pmod{n_2}, \quad x \equiv C_3 \pmod{n_3}$$

for fixed $i$. Thus can assume $\gcd(n_1, n_2) = \gcd(n_1, n_3) = \gcd(n_2, n_3) = 1$, that is, the moduli $n_1$, $n_2$ and $n_3$ are pairwise coprime.
has the solution $P^3$. On the other hand, by the CRT, there is a unique solution $C$ to

$$C \equiv C_i \pmod{n_i},$$
satisfying $0 \leq C \leq n_1n_2n_3 - 1$.

Now, $P$ satisfies $0 \leq P \leq \min\{n_1, n_2, n_3\} - 1$, and so $P^3$ is an integer satisfying

$$0 \leq P^3 \leq (\min\{n_1, n_2, n_3\} - 1)^3 < n_1n_2n_3 - 1,$$

therefore $C = P^3$. We can apply CRT recipe to determine $P^3 = C$ from the $C_i$ and $n_i$ and then recover $P$ by taking the cube root.

**Problem 16.** Write $n_i = p_i q_i$ and suppose $n_1 \neq n_2$. If $(n_1, n_2) > 1$ then $1 < (n_1, n_2) < n_1$ and we can factor $n_1$ as $n_1 = (n_1, n_2) \cdot \frac{n_1}{(n_1, n_2)}$. Thus the two factors in this factorization correspond in some order to $p_1$ and $q_1$. This allows to calculate $\phi(n) = (p_1 - 1)(q_1 - 1)$ and find $d \equiv e^{-1} \mod{\phi(n)}$, breaking the system.