1997 Q4

(a) Describe Euclid’s algorithm for determining the highest common factor hcf\([l, m]\) of positive integers \(l, m\). [4]

(b) Explain how Euclid’s algorithm can be used to find one solution of \(ax + by = d\) in integers \(x, y\), where \(a, b, d\) are integers and hcf\([a, b]\) divides \(d\). [4]

(c) Explain the RSA algorithm for public key encryption/decryption and the relevance of (b). [6]

(d) A public key system which uses the RSA algorithm is based on the modulus \(n = 517\) and the (private) decryption key \(d = 307\).

(i) What is the encryption key? [3]

(ii) What is the encrypted form of the number 245? [3]

Solution

4. (a) Describe Euclid’s algorithm for determining the highest common factor hcf\([l, m]\) of two integers \(l, m\).

The algorithm proceeds as follows:

We can assume that \(l = x > y = m\). Put \(x_0 = x\), \(x_1 = y\). Then compute \(x_2\), \(x_3\), ...
defined by

\[ x_{n+1} = m_n x_n + x_{n+1} \quad (0 \leq x_{n+1} < x_n) \]

If \(x_{n+1} = 0\) then \(x_n = \text{hcf}[x, y]\) (so stop). If \(x_n \neq 0\) then increase \(n\) by one and repeat the process.
The algorithm works because: (1) \( \text{hcf}[x, y] \) coincides with \( \text{hcf}[r, x] \), where \( r \) is the remainder of \( y \) after division by \( x \) and (2) the recursion eventually falls into the \( \text{hcf}[, 0] \) case because the remainder \( r < x \) and so the remainders form a decreasing sequence of non-negative integers (and it follows from the Well Ordering Principle that such a set has zero as its minimum).

(b) Explain how Euclid’s algorithm can be used to solve \( ax + by = d \) in integers \( x, y \), where \( a, b, d \) are integers and \( \text{hcf}[a, b] \) divides \( d \).

If \( \text{hcf}[a, b] \) divides \( d \) to solve this equation in integers \( x, y \) we execute Euclid’s algorithm to find \( \text{hcf}[a, b] \). This gives a set of equations:

\[
\begin{align*}
x_0 &= a, \quad x_1 = b \\
x_0 &= m_1x_1 + x_2 \quad (0 < x_2 < x_1) \\
& \quad \vdots \\
x_{n-1} &= m_{n-1}x_n + d \\
(x_n &= m_{n-1}d + 0) \quad (\text{i.e.} \, d = x_{n-1})
\end{align*}
\]

Next substitute for \( x_{n-1} \) in terms of \( x_{n-2}, x_{n-3}, \ldots \) etc. until we finally reach an identity involving \( x_0 (= a) \) and \( x_1 (= b) \) of the type \( d = ux_0 + vx_1 \), ie. \( d = au + bv \).

(c) The system is based on choosing three integers \((e, p, q)\) where \( p \) and \( q \) are large primes \((\approx 10^{100})\) and \( e \) is coprime (has no factors in common) to \((p - 1)(q - 1)\).

Let \( n = pq \). Then \textit{e and n are made public} and only the owner of the system knows \( p \) and \( q \).

To encrypt the message:

1. Convert the message into a stream of decimal digits (the method
for doing this is not secret, indeed it must be known).

2. Cut the stream into blocks of equal length and convert these to decimal numbers \( m_1, m_2, ..., \) where \( m_i < n \).

3. Raise each number \( m_i \) to the power \( e \) and replace \( m_i^e \) by its remainder \( r_i \pmod{n} \) (so \( m_i^e = r_i \pmod{n} \) in mathematical notation).

4. The encrypted message is then the stream \( r_1 r_2 r_3 ... \)

\[ \text{To decrypt the message.} \]

1. Let \( d \) be the number that has the property

\[ ed = 1 \pmod{(p-1)(q-1)} \]

(this is not too hard to compute, it can be done by using Euclid’s algorithm, and can be worked out once and for all and saved).

2. Then

\[ r_i^d = (m_i^e)^d = m_i^{ed} = m_i^{\phi(pq)} \cdot 1 = m_i \pmod{n} \]

by the Euler-Fermat theorem, and the decrypted message is \( m_1 m_2 m_3 ... \)

(d) \( pq = 517 \) factorises to \( p = 47 \) and \( q = 11 \). Thus \( \phi(pq) = (p-1)(q-1) = 46 \cdot 10 = 460 \).

(i) \( d = 307 \) so we have to solve \( 307e \equiv 1 \pmod{460} \). This can be done with Euclid’s algorithm (but the numbers have been chosen so that it is easy to find a solution by inspection) giving \( e = 3 \), which is the public encryption key.
(ii) Now we know the encrypted form of 245 is $245^3 \equiv 20 \pmod{517}$, i.e. 20.
1998 Q4.

(a) Define Euler’s function \( \varphi(n) \) and state the Euler-Fermat theorem. \[5\]

(b) Explain the RSA algorithm for public key encryption/decryption. \[8\]

(c) A public key system which uses the RSA algorithm is based on the modulus \( n = 253 \) and encryption key \( e = 139 \). What is the decryption key? \[7\]

Solution

4. (a) \( \varphi(n) \) is the number of integers \( k \) (\( 1 \leq k \leq n \)) such that \( k \) and \( n \) are coprime. Euler-Fermat theorem. Given coprime integers \( a, m \) then
\[ a^{\varphi(m)} \equiv 1 \pmod{m} \]

(b) The RSA public key encryption system

The system is based on choosing three integers \( (e, p, q) \) where \( p \) and \( q \) are large primes (\( \approx 10^{100} \)) and \( e \) is coprime (has no factors in common) to \( (p - 1)(q - 1) \).

Let \( n = pq \). Then \( e \) and \( n \) are made public and only the owner of the system knows \( p \) and \( q \).

To encrypt the message:
1. Convert the message into a stream of decimal digits (the method for doing this is not secret, indeed it must be known).

2. Cut the stream into blocks of equal length and convert these to decimal numbers \( m_1, m_2, \ldots \), where \( m_i < n \).

3. Raise each number \( m_i \) to the power \( e \) and replace \( m_i^e \) by its remainder \( r_i \) (mod \( n \)) (so \( m_i^e \equiv r_i \) (mod \( n \)) in mathematical notation).

4. The encrypted message is then the stream \( r_1 r_2 r_3 \ldots \)

To decrypt the message.

1. Let \( d \) be the number that has the property

\[
ed \equiv 1 \pmod{(p-1)(q-1)}
\]

(this is not too hard to compute, it can be done by using Euclid’s algorithm, and can be worked out once and for all and saved).

2. Then

\[
r_i^d \equiv (m_i^e)^d \equiv m_i^{ed} \equiv m_i^{\varphi(n) \cdot 1} \equiv m_i \pmod{n}
\]

by the Euler-Fermat theorem, and the decrypted message is \( m_1 m_2 m_3 \ldots \)

(c) Factorising 253 gives \( n = 11 \times 23 = 253 \). So \( p = 11 \), \( q = 23 \). So \( \varphi(n) = 10 \times 22 = 220 \). The public key exponent is \( e = 139 \). Hence the decryption key \( d \) is the solution to \( 139d \equiv 1 \pmod{220} \).

Using Euclid’s algorithm (for example)

\[
220 = 1 \times 139 + 81
\]
\[139 = 1 \times 81 + 58\]
\[81 = 1 \times 58 + 23\]
\[58 = 2 \times 23 + 12\]
\[23 = 2 \times 12 - 1\]

So \[1 = 2 \times 12 - 23 = 2 \times (58 - 2 \times 23) - 23 = 2 \times 58 - 5 \times 23\]
\[= 2 \times 58 - 5 \times (81 - 58) = 7 \times 58 - 5 \times 81\]
\[= 7 \times (139 - 81) - 5 \times 81 = 7 \times 139 - 12 \times 81\]
\[= 7 \times 139 - 12 \times (220 - 139) = 19 \times 139 - 12 \times 220\]

Hence \[19 \times 139 \equiv 1 \pmod{220}\] so \(d = 19\).

[Or can use modular arithmetic and Euler-Fermat theorem to work out \(139^{\phi(m)} - 1 \pmod{m}\) in a similar way, since we know that \(139^{\phi(m)} = 1 \pmod{m}\).]