Discrete Mathematics & Mathematical Reasoning
Multiplicative Inverses and Some Cryptography

Colin Stirling

Informatics
Multiplicative inverses

Every real number $x$, except $x = 0$, has a multiplicative inverse $y = \frac{1}{x}$; so $xy = 1$
Multiplicative inverses

- Every real number $x$, except $x = 0$, has a multiplicative inverse $y = \frac{1}{x}$; so $xy = 1$

- Similarly for $x \mod m$, except $x = 0$, we wish to find $y \mod m$ such that $xy \equiv 1 \pmod{m}$

$x = 8$ and $m = 15$. Then $x^2 = 16 \equiv 1 \pmod{15}$, so 2 is a multiplicative inverse of 8 (mod 15)

$x = 12$ and $m = 15$. The sequence \{ $x^a \pmod{m}$ | $a = 0, 1, 2, ...$ \} is periodic, and takes on the values \{ 0, 12, 9, 6, 3 \}. So, 12 has no multiplicative inverse mod 15

Notice $\gcd(8, 15) = 1$ whereas $\gcd(12, 15) = 3$. 

Colin Stirling (Informatics)  Discrete Mathematics (Chap 4)
Multiplicative inverses

- Every real number \( x \), except \( x = 0 \), has a multiplicative inverse \( y = \frac{1}{x} \); so \( xy = 1 \)

- Similarly for \( x \mod m \), except \( x = 0 \), we wish to find \( y \mod m \) such that \( xy \equiv 1 \pmod{m} \)

- \( x = 8 \) and \( m = 15 \). Then \( x \cdot 2 = 16 \equiv 1 \pmod{15} \), so 2 is a multiplicative inverse of 8 (mod 15)
Multiplicative inverses

- Every real number $x$, except $x = 0$, has a multiplicative inverse $y = \frac{1}{x}$; so $xy = 1$

- Similarly for $x \mod m$, except $x = 0$, we wish to find $y \mod m$ such that $xy \equiv 1 \pmod{m}$

- $x = 8$ and $m = 15$. Then $x \cdot 2 = 16 \equiv 1 \pmod{15}$, so 2 is a multiplicative inverse of 8 (mod 15)

- $x = 12$ and $m = 15$
Multiplicative inverses

- Every real number \( x \), except \( x = 0 \), has a multiplicative inverse \( y = \frac{1}{x} \); so \( xy = 1 \)

- Similarly for \( x \mod m \), except \( x = 0 \), we wish to find \( y \mod m \) such that \( xy \equiv 1 \pmod{m} \)

- \( x = 8 \) and \( m = 15 \). Then \( x 2 = 16 \equiv 1 \pmod{15} \), so 2 is a multiplicative inverse of 8 (mod 15)

- \( x = 12 \) and \( m = 15 \)
  The sequence \( \{xa \pmod{m} \mid a = 0, 1, 2, \ldots\} \) is periodic, and takes on the values \( \{0, 12, 9, 6, 3\} \). So, 12 has no multiplicative inverse mod 15

Notice \( \gcd(8, 15) = 1 \) whereas \( \gcd(12, 15) = 3 \).
Multiplicative inverses

- Every real number $x$, except $x = 0$, has a multiplicative inverse $y = \frac{1}{x}$; so $xy = 1$

- Similarly for $x \mod m$, except $x = 0$, we wish to find $y \mod m$ such that $xy \equiv 1 \pmod{m}$

- $x = 8$ and $m = 15$. Then $x \cdot 2 = 16 \equiv 1 \pmod{15}$, so 2 is a multiplicative inverse of 8 (mod 15)

- $x = 12$ and $m = 15$
  The sequence $\{xa \mod m | a = 0, 1, 2, ...\}$ is periodic, and takes on the values $\{0, 12, 9, 6, 3\}$. So, 12 has no multiplicative inverse mod 15

- Notice $\gcd(8, 15) = 1$ whereas $\gcd(12, 15) = 3$
Theorem

If \( m, x \) are positive integers and \( \gcd(m, x) = 1 \) then \( x \) has a multiplicative inverse mod \( m \) (and it is unique mod \( m \))

Proof.
By Bézout's theorem there are \( s \) and \( t \) such that
\[
s m + t x = 1 = \gcd(m, x)
\]
So,
\[
s m + t x \equiv 1 \pmod{m}
\]
As \( s m \equiv 0 \pmod{m} \), so \( t x \equiv 1 \pmod{m} \).

For uniqueness mod \( m \). Assume \( t x \equiv 1 \pmod{m} \) and \( u x \equiv 1 \pmod{m} \).
Therefore, \( t x \equiv u x \pmod{m} \).
Since \( \gcd(m, x) = 1 \) it follows that \( t \equiv u \pmod{m} \).

Compute the multiplicative inverse using extended Euclidean algorithm
**Theorem**

If $m, x$ are positive integers and $\gcd(m, x) = 1$ then $x$ has a multiplicative inverse mod $m$ (and it is unique mod $m$)

**Proof.**

By Bézout’s theorem there are $s$ and $t$ such that

$$sm + tx = 1 = \gcd(m, x)$$

So, $sm + tx \equiv 1 \pmod{m}$. As $sm \equiv 0 \pmod{m}$, so $tx \equiv 1 \pmod{m}$.

For uniqueness mod $m$. Assume $tx \equiv 1 \pmod{m}$ and $ux \equiv 1 \pmod{m}$. Therefore, $tx \equiv ux \pmod{m}$. Since $\gcd(m, x) = 1$ it follows that $t \equiv u \pmod{m}$. 

Compute the multiplicative inverse using extended euclidean algorithm
Itm, x are positive integers and gcd(m, x) = 1 then x has a multiplicative inverse mod m (and it is unique mod m)

Proof.
By Bézout’s theorem there are s and t such that

\[ sm + tx = 1 = \gcd(m, x) \]

So, \( sm + tx \equiv 1 \pmod{m} \). As \( sm \equiv 0 \pmod{m} \), so \( tx \equiv 1 \pmod{m} \).

For uniqueness mod m. Assume \( tx \equiv 1 \pmod{m} \) and \( ux \equiv 1 \pmod{m} \).

Therefore, \( tx \equiv ux \pmod{m} \). Since \( \gcd(m, x) = 1 \) it follows that \( t \equiv u \pmod{m} \).

Compute the multiplicative inverse using extended euclidean algorithm
**Theorem**

Let \( m_1, m_2, \ldots, m_n \) be pairwise relatively prime positive integers greater than 1 and \( a_1, a_2, \ldots, a_n \) be arbitrary integers. Then the system

\[
\begin{align*}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
& \vdots \\
x &\equiv a_n \pmod{m_n}
\end{align*}
\]

has a unique solution modulo \( m = m_1 m_2 \cdots m_n \).
Chinese remainder theorem

**Theorem**

Let \( m_1, m_2, \ldots, m_n \) be pairwise relatively prime positive integers greater than 1 and \( a_1, a_2, \ldots, a_n \) be arbitrary integers. Then the system

\[
\begin{align*}
  x &\equiv a_1 \pmod{m_1} \\
  x &\equiv a_2 \pmod{m_2} \\
  \vdots \\
  x &\equiv a_n \pmod{m_n}
\end{align*}
\]

has a unique solution modulo \( m = m_1 m_2 \cdots m_n \)

**Proof.**

In the book

[Colin Stirling (Informatics)](http://example.com) Discrete Mathematics (Chap 4)
Example

\[ x \equiv 2 \pmod{3} \]
\[ x \equiv 3 \pmod{5} \]
\[ x \equiv 5 \pmod{7} \]
Example

\[ x \equiv 2 \pmod{3} \]
\[ x \equiv 3 \pmod{5} \]
\[ x \equiv 5 \pmod{7} \]

\[ m = 3 \cdot 5 \cdot 7 = 105 \]
Example

\[ x \equiv 2 \pmod{3} \]
\[ x \equiv 3 \pmod{5} \]
\[ x \equiv 5 \pmod{7} \]

- \[ m = 3 \cdot 5 \cdot 7 = 105 \]
- \[ M_1 = 35 \text{ and } 2 \text{ is an inverse of } M_1 \mod 3 \]
Example

\[ x \equiv 2 \pmod{3} \]
\[ x \equiv 3 \pmod{5} \]
\[ x \equiv 5 \pmod{7} \]

- \( m = 3 \cdot 5 \cdot 7 = 105 \)
- \( M_1 = 35 \) and 2 is an inverse of \( M_1 \pmod{3} \)
- \( M_2 = 21 \) and 1 is an inverse of \( M_2 \pmod{5} \)

\[ x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 5 \cdot 15 \cdot 1 = 140 + 63 + 75 = 278 \equiv 68 \pmod{105} \]
Example

\[ x \equiv 2 \pmod{3} \]
\[ x \equiv 3 \pmod{5} \]
\[ x \equiv 5 \pmod{7} \]

- \( m = 3 \cdot 5 \cdot 7 = 105 \)
- \( M_1 = 35 \) and 2 is an inverse of \( M_1 \mod 3 \)
- \( M_2 = 21 \) and 1 is an inverse of \( M_2 \mod 5 \)
- \( M_3 = 15 \) and 1 is an inverse of \( M_3 \mod 7 \)
Example

\[ x \equiv 2 \pmod{3} \]
\[ x \equiv 3 \pmod{5} \]
\[ x \equiv 5 \pmod{7} \]

- \( m = 3 \cdot 5 \cdot 7 = 105 \)
- \( M_1 = 35 \) and 2 is an inverse of \( M_1 \) mod 3
- \( M_2 = 21 \) and 1 is an inverse of \( M_2 \) mod 5
- \( M_3 = 15 \) and 1 is an inverse of \( M_3 \) mod 7
- \( x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 5 \cdot 15 \cdot 1 \)

\[ x \equiv 278 \pmod{105} \]
Example

\[ x \equiv 2 \pmod{3} \]
\[ x \equiv 3 \pmod{5} \]
\[ x \equiv 5 \pmod{7} \]

- \( m = 3 \cdot 5 \cdot 7 = 105 \)
- \( M_1 = 35 \) and 2 is an inverse of \( M_1 \) mod 3
- \( M_2 = 21 \) and 1 is an inverse of \( M_2 \) mod 5
- \( M_3 = 15 \) and 1 is an inverse of \( M_3 \) mod 7
- \( x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 5 \cdot 15 \cdot 1 \)
- \( x = 140 + 63 + 75 = 278 \equiv 68 \pmod{105} \)
Theorem

If \( p \) is prime and \( p \nmid a \), then \( a^{p-1} \equiv 1 \pmod{p} \). Furthermore, for every integer \( a \) we have \( a^p \equiv a \pmod{p} \).
Fermat's little theorem

**Theorem**

If \( p \) is prime and \( p \nmid a \), then \( a^{p-1} \equiv 1 \pmod{p} \). Furthermore, for every integer \( a \) we have \( a^p \equiv a \pmod{p} \).

**Proof.**

Assume \( p \nmid a \) and so, therefore, \( \gcd(p, a) = 1 \). Then \( a, 2a, \ldots, (p-1)a \) are not pairwise congruent modulo \( p \); if \( ia \equiv ja \pmod{p} \) because \( \gcd(p, a) = 1 \) then \( i \equiv j \pmod{p} \) which is impossible. Therefore, each element \( ja \mod p \) is a distinct element in the set \( \{1, \ldots, p - 1\} \). This means that the product \( a \cdot 2a \cdot \cdots (p-1)a \equiv 1 \cdot 2 \cdot \cdots p - 1 \pmod{p} \). Therefore, \( (p - 1)!a^{p-1} \equiv (p - 1)! \pmod{p} \). Now because \( \gcd(p, q) = 1 \) for \( 1 \leq q \leq p - 1 \) it follows that \( a^{p-1} \equiv 1 \pmod{p} \). Therefore, also \( a^p \equiv a \pmod{p} \) and when \( p\mid a \) then clearly \( a^p \equiv a \pmod{p} \).
Computing the remainders modulo prime $p$

Find $7^{222} \mod 11$

By Fermat's little theorem, we know that $7^{10} \equiv 1 \pmod{11}$, and so $(7^{10})^k \equiv 1 \pmod{11}$ for every positive integer $k$. Therefore, $7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} \cdot 7^2 \equiv 1^{22} \cdot 49 \equiv 5 \pmod{11}$. Hence, $7^{222} \mod 11 = 5\cdot 340 \equiv 1 \pmod{11}$ because $2^{10} \equiv 1 \pmod{11}$.
Computing the remainders modulo prime $p$

- Find $7^{222} \mod 11$

By Fermat’s little theorem, we know that $7^{10} \equiv 1 \pmod{11}$, and so $(7^{10})^k \equiv 1 \pmod{11}$ for every positive integer $k$. Therefore, $7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} \cdot 7^2 \equiv 1^{22} \cdot 49 \equiv 5 \pmod{11}$. Hence, $7^{222} \mod 11 = 5$
Computing the remainders modulo prime $p$

- Find $7^{222} \mod 11$

- By Fermat’s little theorem, we know that $7^{10} \equiv 1 \pmod{11}$, and so $(7^{10})^k \equiv 1 \pmod{11}$ for every positive integer $k$. Therefore, $7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} \cdot 7^2 \equiv 1^{22} \cdot 49 \equiv 5 \pmod{11}$. Hence, $7^{222} \mod 11 = 5$

- $2^{340} \equiv 1 \pmod{11}$ because $2^{10} \equiv 1 \pmod{11}$
Private key cryptography

- Bob wants to send Alice a secret message M

Alice sends Bob a private key $E_n$ (which has an inverse $D_n$)

Bob encrypts $M$ and sends Alice $E_n(M)$

Alice decrypts $E_n(M)$, $D_n(En(M))$

Important property $D_n(En(M)) = M$

Alice and Bob share a secret which could be intercepted by a third party

Example use $E_n(p) = (p + 3) \mod 26$
Private key cryptography

- Bob wants to send Alice a secret message M
- Alice sends Bob a private key En (which has an inverse De)

\[
\text{Bob encrypts } M \text{ and sends } Alice \text{ En}(M)
\]

\[
\text{Alice decrypts } En(M), \text{ De}(En(M))
\]

Important property: \(\text{De}(\text{En}(M)) = M\)

Alice and Bob share a secret which could be intercepted by a third party

Example use \(\text{En}(p) = (p + 3) \mod 26\)

What is WKLV LV D VHFSHW?
Bob wants to send Alice a secret message $M$

Alice sends Bob a private key $E_n$ (which has an inverse $D_e$)

Bob encrypts $M$ and sends Alice $E_n(M)$

Alice decrypts $E_n(M)$, $D_e(E_n(M))$

Important property $D_e(E_n(M)) = M$

Alice and Bob share a secret which could be intercepted by a third party

Example use $E_n(p) = (p + 3) \mod 26$
Private key cryptography

- Bob wants to send Alice a secret message M
- Alice sends Bob a private key $E_n$ (which has an inverse $D_n$)
- Bob encrypts $M$ and sends Alice $E_n(M)$
- Alice decrypts $E_n(M)$, $D_n(E_n(M))$

Important property $D_n(E_n(M)) = M$

Alice and Bob share a secret which could be intercepted by a third party

Example use $E_n(p) = (p + 3) \mod 26$

What is $WKLV$ LV $D\ VHFSHW$ ?
Private key cryptography

- Bob wants to send Alice a secret message $M$
- Alice sends Bob a private key $E_n$ (which has an inverse $D_n$)
- Bob encrypts $M$ and sends Alice $E_n(M)$
- Alice decrypts $E_n(M)$, $D_n(E_n(M))$
- Important property $D_n(E_n(M)) = M$

Example use $E_n(p) = (p + 3) \mod 26$
Private key cryptography

- Bob wants to send Alice a secret message M
- Alice sends Bob a private key $E_n$ (which has an inverse $D_n$)
- Bob encrypts M and sends Alice $E_n(M)$
- Alice decrypts $E_n(M)$, $D_n(E_n(M))$
- Important property $D_n(E_n(M)) = M$
- Alice and Bob share a secret which could be intercepted by a third party

Example use $E_n(p) = (p + 3) \mod 26$
Private key cryptography

- Bob wants to send Alice a secret message M
- Alice sends Bob a private key $E_n$ (which has an inverse $D_e$)
- Bob encrypts M and sends Alice $E_n(M)$
- Alice decrypts $E_n(M)$, $D_e(E_n(M))$
- Important property $D_e(E_n(M)) = M$
- Alice and Bob share a secret which could be intercepted by a third party
- Example use $E_n(p) = (p + 3) \mod 26$
Private key cryptography

- Bob wants to send Alice a secret message $M$
- Alice sends Bob a private key $E_n$ (which has an inverse $D_e$)
- Bob encrypts $M$ and sends Alice $E_n(M)$
- Alice decrypts $E_n(M)$, $D_e(E_n(M))$
- Important property $D_e(E_n(M)) = M$
- Alice and Bob share a secret which could be intercepted by a third party
- Example use $E_n(p) = (p + 3) \mod 26$
- What is $WKLV \ LV \ D \ VHFSHW$?
Public key cryptography

- Bob wants to send Alice a secret message $M$
Public key cryptography

- Bob wants to send Alice a secret message $M$
- Without Alice and Bob sharing a secret
Public key cryptography

- Bob wants to send Alice a secret message $M$
- Without Alice and Bob sharing a secret
- Alice sends Bob a public key $E_n$ (and keeps her inverse private key $D_e$ secret from everyone including Bob)

Important property $D_e(E_n(M)) = M$

The challenge: $D_e$ can't be feasibly computed from $E_n$; and given $E_n(M)$ one can't feasibly compute $M$
Bob wants to send Alice a secret message $M$

Without Alice and Bob sharing a secret

Alice sends Bob a public key $E_n$ (and keeps her inverse private key $D_e$ secret from everyone including Bob)

Bob encrypts $M$ and sends Alice $E_n(M)$

Important property $D_e(E_n(M)) = M$

The challenge: $D_e$ can't be feasibly computed from $E_n$; and given $E_n(M)$ one can't feasibly compute $M$
Bob wants to send Alice a secret message $M$

Without Alice and Bob sharing a secret

Alice sends Bob a public key $E_n$ (and keeps her inverse private key $D_e$ secret from everyone including Bob)

Bob encrypts $M$ and sends Alice $E_n(M)$

Alice decrypts $E_n(M)$, $D_e(E_n(M))$
Public key cryptography

- Bob wants to send Alice a secret message $M$
- **Without Alice and Bob sharing a secret**
- Alice sends Bob a public key $E_n$ (and keeps her inverse private key $D_e$ secret from everyone including Bob)
- Bob encrypts $M$ and sends Alice $E_n(M)$
- Alice decrypts $E_n(M)$, $D_e(E_n(M))$
- Important property $D_e(E_n(M)) = M$
Public key cryptography

- Bob wants to send Alice a secret message M
- Without Alice and Bob sharing a secret
- Alice sends Bob a public key $E_n$ (and keeps her inverse private key $D_e$ secret from everyone including Bob)
- Bob encrypts M and sends Alice $E_n(M)$
- Alice decrypts $E_n(M)$, $D_e(E_n(M))$
- Important property $D_e(E_n(M)) = M$
- The challenge: $D_e$ can’t be feasibly computed from $E_n$; and given $E_n(M)$ one can’t feasibly compute M
Choose two distinct prime numbers \( p \) and \( q \)

Let \( n = pq \) and \( k = (p - 1)(q - 1) \)

Choose integer \( e \) where \( 1 < e < k \) and \( \gcd(e, k) = 1 \)

\( (n, e) \) is released as the public key

Let \( d \) be the multiplicative inverse of \( e \) modulo \( k \), so \( de \equiv 1 \pmod{k} \)

\( (n, d) \) is the private key and kept secret
RSA: encryption and decryption

Alice transmits her public key \((n, e)\) to Bob and keeps the private key \((n, d)\) secret
RSA: encryption and decryption

Alice transmits her public key \((n, e)\) to Bob and keeps the private key \((n, d)\) secret

**Encryption** Bob wishes to send message \(M\) to Alice
RSA: encryption and decryption

Alice transmits her public key \((n, e)\) to Bob and keeps the private key \((n, d)\) secret

**Encryption** Bob wishes to send message \(M\) to Alice

1. He turns \(M\) into integer \(m, 0 \leq m < n\), using an agreed-upon reversible protocol known as a padding scheme
RSA: encryption and decryption

Alice transmits her public key \((n, e)\) to Bob and keeps the private key \((n, d)\) secret

**Encryption** Bob wishes to send message \(M\) to Alice

1. He turns \(M\) into integer \(m, 0 \leq m < n\), using an agreed-upon reversible protocol known as a padding scheme
2. He computes the ciphertext \(c\) corresponding to \(c = m^e \mod n\). (This can be done quickly)
RSA: encryption and decryption

Alice transmits her public key \((n, e)\) to Bob and keeps the private key \((n, d)\) secret

Encryption
Bob wishes to send message \(M\) to Alice

1. He turns \(M\) into integer \(m, 0 \leq m < n\), using an agreed-upon reversible protocol known as a padding scheme
2. He computes the ciphertext \(c\) corresponding to \(c = m^e \mod n\). (This can be done quickly)
3. Bob transmits \(c\) to Alice.
RSA: encryption and decryption

Alice transmits her public key \((n, e)\) to Bob and keeps the private key \((n, d)\) secret

**Encryption** Bob wishes to send message \(M\) to Alice

1. He turns \(M\) into integer \(m, 0 \leq m < n\), using an agreed-upon reversible protocol known as a padding scheme
2. He computes the ciphertext \(c\) corresponding to \(c = m^e \mod n\). (This can be done quickly)
3. Bob transmits \(c\) to Alice.

**Decryption** Alice can recover \(m\) from \(c\)
RSA: encryption and decryption

Alice transmits her public key \((n, e)\) to Bob and keeps the private key \((n, d)\) secret.

**Encryption** Bob wishes to send message \(M\) to Alice

1. He turns \(M\) into integer \(m, 0 \leq m < n\), using an agreed-upon reversible protocol known as a padding scheme.
2. He computes the ciphertext \(c\) corresponding to \(c = m^e \mod n\). (This can be done quickly)
3. Bob transmits \(c\) to Alice.

**Decryption** Alice can recover \(m\) from \(c\)

1. Using her private key exponent \(d\) via computing \(m = c^d \mod n\)
RSA: encryption and decryption

Alice transmits her public key \((n, e)\) to Bob and keeps the private key \((n, d)\) secret

**Encryption** Bob wishes to send message \(M\) to Alice

1. He turns \(M\) into integer \(m, 0 \leq m < n\), using an agreed-upon reversible protocol known as a padding scheme
2. He computes the ciphertext \(c\) corresponding to \(c = m^e \mod n\). (This can be done quickly)
3. Bob transmits \(c\) to Alice.

**Decryption** Alice can recover \(m\) from \(c\)

1. Using her private key exponent \(d\) via computing \(m = c^d \mod n\)
2. Given \(m\), she can recover the original message \(M\) by reversing the padding scheme
Example

\[ n = 43 \cdot 59 = 2537 \]
Example

- \( n = 43 \cdot 59 = 2537 \)
- \( \gcd(13, 42 \cdot 58) = 1 \), so public key is \((2537, 13)\)
Example

- \( n = 43 \cdot 59 = 2537 \)
- \( \gcd(13, 42 \cdot 58) = 1 \), so public key is \((2537, 13)\)
- \( d = 937 \) is inverse of 13 modulo 2436 = 42 \cdot 58; private key \((2537, 937)\)
Example

- \( n = 43 \cdot 59 = 2537 \)
- \( \gcd(13, 42 \cdot 58) = 1 \), so public key is \((2537, 13)\)
- \( d = 937 \) is inverse of 13 modulo \( 2436 = 42 \cdot 58 \); private key \((2537, 937)\)
- Encrypt STOP as two blocks 1819 for ST and 1415 for OP
  (padding scheme: position in alphabet - 1)

  - So, \( 1819 \mod 2537 = 2081 \) and \( 1415 \mod 2537 = 2182 \)
  - So encrypted message is 2081 2182

  - Receive message 0981 0461: decrypt it
    - \( 0981 \mod 2537 = 0704 \) and \( 0461 \mod 2537 = 1115 \)
    - So decrypted message is HELP
Example

- \( n = 43 \cdot 59 = 2537 \)
- \( \text{gcd}(13, 42 \cdot 58) = 1 \), so public key is \((2537, 13)\)
- \( d = 937 \) is inverse of 13 modulo \( 2436 = 42 \cdot 58 \); private key \((2537, 937)\)
- Encrypt STOP as two blocks 1819 for ST and 1415 for OP (padding scheme: position in alphabet - 1)
- So, \( 1819^{13} \mod 2537 = 2081 \) and \( 1415^{13} \mod 2537 = 2182 \)
Example

- $n = 43 \cdot 59 = 2537$
- $\gcd(13, 42 \cdot 58) = 1$, so public key is $(2537, 13)$
- $d = 937$ is inverse of $13$ modulo $2436 = 42 \cdot 58$; private key $(2537, 937)$
- Encrypt STOP as two blocks $1819$ for ST and $1415$ for OP (padding scheme: position in alphabet - 1)
- So, $1819^{13} \mod 2537 = 2081$ and $1415^{13} \mod 2537 = 2182$
- So encrypted message is $2081 \ 2182$
Example

- \( n = 43 \cdot 59 = 2537 \)
- \( \text{gcd}(13, 42 \cdot 58) = 1 \), so public key is \((2537, 13)\)
- \( d = 937 \) is inverse of 13 modulo \( 2436 = 42 \cdot 58 \); private key \((2537, 937)\)
- Encrypt STOP as two blocks 1819 for ST and 1415 for OP (padding scheme: position in alphabet - 1)
- So, \( 1819^{13} \mod 2537 = 2081 \) and \( 1415^{13} \mod 2537 = 2182 \)
- So encrypted message is 2081 2182
- Receive message 0981 0461: decrypt it
- \( 0981 \mod 2537 = 0704 \) and \( 0461 \mod 2537 = 1115 \)
- So decrypted message is HELP
Example

- \( n = 43 \cdot 59 = 2537 \)
- \( \gcd(13, 42 \cdot 58) = 1 \), so public key is \((2537, 13)\)
- \( d = 937 \) is inverse of 13 modulo \( 2436 = 42 \cdot 58 \); private key \((2537, 937)\)
- Encrypt STOP as two blocks 1819 for ST and 1415 for OP (padding scheme: position in alphabet - 1)
- So, \( 1819^{13} \mod 2537 = 2081 \) and \( 1415^{13} \mod 2537 = 2182 \)
- So encrypted message is \( 2081 \ 2182 \)
- Receive message 0981 0461: decrypt it
- \( 0981^{937} \mod 2537 = 0704 \) and \( 0461^{937} \mod 2537 = 1115 \)
Example

- \( n = 43 \cdot 59 = 2537 \)
- \( \gcd(13, 42 \cdot 58) = 1 \), so public key is \((2537, 13)\)
- \( d = 937 \) is inverse of 13 modulo 2436 = 42 \cdot 58; private key \((2537, 937)\)
- Encrypt STOP as two blocks 1819 for ST and 1415 for OP (padding scheme: position in alphabet - 1)
- So, 1819\(^{13} \) mod 2537 = 2081 and 1415\(^{13} \) mod 2537 = 2182
- So encrypted message is 2081 2182
- Receive message 0981 0461: decrypt it
- 0981\(^{937} \) mod 2537 = 0704 and 0461\(^{937} \) mod 2537 = 1115
- So decrypted message is HELP
RSA: correctness of decryption

Given that \( c = m^e \mod n \), is \( m = c^d \mod n \)?

\[
c^d = (m^e)^d \equiv m^{ed} \pmod{n}
\]

By construction, \( d \) and \( e \) are each others multiplicative inverses modulo \( k \), i.e. \( ed \equiv 1 \pmod{k} \). Also \( k = (p - 1)(q - 1) \). Thus \( ed - 1 = h(p - 1)(q - 1) \) for some integer \( h \). We consider \( m^{ed} \mod p \)

If \( p \nmid m \) then

\[
m^{ed} = m^{h(p-1)(q-1)}m = (m^{p-1})^{h(q-1)}m \equiv 1^{h(q-1)}m \equiv m \pmod{p} \quad \text{(by Fermat’s little theorem)}
\]

Otherwise \( m^{ed} \equiv 0 \equiv m \pmod{p} \)

Symmetrically, \( m^{ed} \equiv m \pmod{q} \)

Since \( p, q \) are distinct primes, we have \( m^{ed} \equiv m \pmod{pq} \). Since \( n = pq \), we have \( c^d = m^{ed} \equiv m \pmod{n} \)