Discrete Mathematics & Mathematical Reasoning
Multiplicative Inverses and Some Cryptography

Colin Stirling

Informatics

Some slides based on ones by Myrto Arapinis

Multiplicative inverses

Theorem

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

Multiplicative inverses

Theorem

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

Proof.

Consider the sequence of m numbers $0, x, 2x, ..., (m-1)x$. We first show that these are all distinct modulo m.

To verify the above claim, suppose that $ax \bmod m = bx \bmod m$ for two distinct values a, b in the range $0 \leq a, b \leq m-1$. Then we would have $(a-b)x \equiv 0 (\text{mod } m)$, or equivalently, $(a-b)x = km$ for some integer k. But since x and m are relatively prime, it follows that $a-b$ must be an integer multiple of m. This is not possible since a,b are distinct non-negative integers less than m.

Now, since there are only m distinct values modulo m, it must then be the case that $ax \equiv 1 (\text{mod } m)$ for exactly one a (modulo m). This a is the unique multiplicative inverse. □

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

$$\begin{aligned} x &\equiv a_1 \ (mod\ m_1) \\ x &\equiv a_2 \ (mod\ m_2) \\ &\vdots \\ x &\equiv a_n \ (mod\ m_n) \end{aligned}$$

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

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

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

Proof.

In the book $\square$

Example

$$
\begin{aligned}
x &\equiv 2 \pmod{3} \\
x &\equiv 3 \pmod{5} \\
x &\equiv 5 \pmod{7}
\end{aligned}
$$

Example

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 5 \pmod{7}$$

- $m = 3 \cdot 5 \cdot 7 = 105$

Example

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 5 \pmod{7}$$

- $m = 3 \cdot 5 \cdot 7 = 105$
- $M_1 = 35$ and 2 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 mod 3
- $M_2 = 21$ and 1 is an inverse of M_2 mod 5

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
- $x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 5 \cdot 15 \cdot 1$

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

Fermat's little theorem

Theorem

If p is prime and $p \not| a$, 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 $p \not| a$, then $a^{p-1} \equiv 1 \pmod{p}$. Furthermore, for every integer a we have $a^p \equiv a \pmod{p}$

Proof.

Assume $p \not| a$ and so, therefore, $\gcd(p, a) = 1$. Then $a, 2a, \ldots, (p-1)a$ are not pairwise congruent modulo p; if $ia \equiv ja \pmod{p}$ then $(i-j)a = pm$ for some m which is impossible (as then $i \equiv j \pmod{p}$ using last result from slides of Lecture 11). Therefore, each element $ja \bmod p$ is a distinct element in the set $\{1, \ldots, p-1\}$. This means that the product $a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots p-1 \pmod{p}$. 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 $p|a$ then clearly $a^p \equiv a \pmod{p}$. $\square$

Computing the remainders modulo prime p

- Find 7^{222} mod 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, $7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22}\, 7^2 \equiv 1^{22} 49 \equiv 5 \pmod{11}$. Hence, $7^{222} \bmod 11 = 5$

Computing the remainders modulo prime p

- Find $7^{222} \bmod 11$
- 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, $7^{222} = 7^{22\cdot 10+2} = (7^{10})^{22}\, 7^2 \equiv 1^{22} 49 \equiv 5 \pmod{11}$. Hence, $7^{222} \bmod 11 = 5$
- $2^{340} \equiv 1 \pmod{11}$ because $2^{10} \equiv 1 \pmod{11}$

Private key cryptography

- Bob wants to send Alice a secret message M

Private key cryptography

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

Private key cryptography

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

Private key cryptography

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

Private key cryptography

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

Private key cryptography

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

Private key cryptography

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

Private key cryptography

- Bob wants to send Alice a secret message M
- Alice sends Bob a private key En (which has an inverse De)
- Bob encrypts M and sends Alice En(M)
- Alice decrypts En(M), De(En(M))
- Important property De(En(M)) $=$ M
- Alice and Bob share a secret which could be intercepted by a third party
- Example use En(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 En (and keeps her inverse private key De secret from everyone including Bob)

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 En (and keeps her inverse private key De secret from everyone including Bob)
- Bob encrypts M and sends Alice En(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 En (and keeps her inverse private key De secret from everyone including Bob)
- Bob encrypts M and sends Alice En(M)
- Alice decrypts En(M), De(En(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 En (and keeps her inverse private key De secret from everyone including Bob)
- Bob encrypts M and sends Alice En(M)
- Alice decrypts En(M), De(En(M))
- Important property De(En(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 En (and keeps her inverse private key De secret from everyone including Bob)
- Bob encrypts M and sends Alice En(M)
- Alice decrypts En(M), De(En(M))
- Important property De(En(M)) $=$ M
- The challenge: De can't be feasibly computed from En; and given $En(M)$ one can't feasibly compute M

RSA Cryptosystem

- Named after 3 researchers: Rivest, Shamir and Adleman

RSA Cryptosystem

- Named after 3 researchers: Rivest, Shamir and Adleman
- There are quick algorithms for testing whether a large integer is prime

RSA Cryptosystem

- Named after 3 researchers: Rivest, Shamir and Adleman
- There are quick algorithms for testing whether a large integer is prime
- There is no known quick algorithm that can factorise a large integer

RSA Cryptosystem

- Named after 3 researchers: Rivest, Shamir and Adleman
- There are quick algorithms for testing whether a large integer is prime
- There is no known quick algorithm that can factorise a large integer
- Very significant open problem: how hard is it to factorise integers?

RSA: key generation

- 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 secret

Encryption If Bob wishes to send message M to Alice.

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

Decryption Alice can recover m from c by

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

Unrealistic example

- $n = 43 \cdot 59 = 2537$

Unrealistic example

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

Unrealistic 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 $(2537, 937)$

Unrealistic 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)

Unrealistic 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)
- So, 1819^{13} mod 2537 = 2081 and 1415^{13} mod 2537 = 2182

Unrealistic 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)
- So, 1819^{13} mod 2537 = 2081 and 1415^{13} mod 2537 = 2182
- So encrypted message is 2081 2182

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
$m^{ed} = m^{h(p-1)(q-1)}m = (m^{p-1})^{h(q-1)}m \equiv 1^{h(q-1)}m \equiv m \pmod{p}$ (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 $c^d = m^{ed} \equiv m \pmod{n}$