MTH314: Discrete Mathematics for Engineers

Lecture 9a: Public-Key Cryptography: Proofs

Dr Ewa Infeld

Ryerson University

Chinese Remainder Theorem

Theorem

Suppose that m, n are coprime. Then:
1. For all integers a, b the linear congruences

$$x \equiv a \ (mod \ \ m), \quad x \equiv b \ (mod \ \ n)$$

have a unique common solution c,

$$x \equiv c \ (mod \ \ m \cdot n)$$

Proof: The proof is *constructive* - just like with the Euclidean Algorithm, the fact that we always know how to find the result means the result always exists. We prove the uniqueness separately.

Chinese Remainder Theorem

Theorem

Suppose that m, n are coprime. Then:
1. For all integers a, b the linear congruences

$$x \equiv a \ (mod \ \ m), \quad x \equiv b \ (mod \ \ n)$$

have a unique common solution c,

$$x \equiv c \ (mod \ \ m \cdot n).$$

Proof: The proof is *constructive* - just like with the Euclidean Algorithm, the fact that we always know how to find the result means the result always exists. We'll prove the uniqueness separately. Let's recap:

Chinese Remainder Theorem

Proof of Chinese Remainder Theorem:
Suppose that m, n are coprime. We want to solve the system

$$x \equiv a \ (mod \ \ m), \quad x \equiv b \ (mod \ \ n)$$

by finding a common solution c,

$$x \equiv c \ (mod \ \ m \cdot n).$$

Chinese Remainder Theorem

Proof of Chinese Remainder Theorem:
Suppose that m, n are coprime. We want to solve the system

$$x \equiv a \ (mod \ \ m), \quad x \equiv b \ (mod \ \ n)$$

by finding a common solution c,

$$x \equiv c \ (mod \ \ m \cdot n).$$

Since $m, \ n$ are coprime we know that for some integers $q_1, \ q_2$ we have:

$$q_1 \cdot m + q_2 \cdot n = 1,$$

and we can find these integers using the Extended Euclidean Algorithm.

Proof of Chinese Remainder Theorem:
Suppose that m, n are coprime. We want to solve the system

$$x \equiv a \ (mod \ \ m), \quad x \equiv b \ (mod \ \ n)$$

by finding a common solution c,

$$x \equiv c \ (mod \ \ m \cdot n).$$

Since $m, \ n$ are coprime we know that for some integers $q_1, \ q_2$ we have:

$$q_1 \cdot m + q_2 \cdot n = 1,$$

and we can find these integers using the Extended Euclidean Algorithm. Then $c \equiv a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \ (mod \ \ n \cdot m)$ is a solution.

Chinese Remainder Theorem

We still need to

1. Veryfy that it really is a solution.
2. Prove that it's the only solution $mod\ m \cdot n$.

We still need to

1. Veryfy that it really is a solution.
2. Prove that it's the only solution $mod\ m \cdot n$.

We have $c \equiv a \cdot q_2 \cdot n + b \cdot q_1 \cdot m\ (mod\ n \cdot m)$, and want to verify that $c \equiv a\ (mod\ m)$ and $c \equiv b\ (mod\ n)$:

Chinese Remainder Theorem

We still need to

1. Veryfy that it really is a solution.
2. Prove that it's the only solution $mod\ m \cdot n$.

We have $c \equiv a \cdot q_2 \cdot n + b \cdot q_1 \cdot m\ (mod\ n \cdot m)$, and want to verify that $c \equiv a\ (mod\ m)$ and $c \equiv b\ (mod\ n)$:

$$a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \equiv a \cdot q_2 \cdot n\ (mod\ m)$$

Chinese Remainder Theorem

We still need to

1. Veryfy that it really is a solution.
2. Prove that it's the only solution $mod\ m \cdot n$.

We have $c \equiv a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \ (mod\ n \cdot m)$, and want to verify that $c \equiv a \ (mod\ m)$ and $c \equiv b \ (mod\ n)$:

$$a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \equiv a \cdot q_2 \cdot n \ (mod\ m)$$
$$a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \equiv a \cdot (1 - q_1 \cdot m) \ (mod\ m)$$

Chinese Remainder Theorem

We still need to

1. Veryfy that it really is a solution.
2. Prove that it's the only solution $mod\ m \cdot n$.

We have $c \equiv a \cdot q_2 \cdot n + b \cdot q_1 \cdot m\ (mod\ n \cdot m)$, and want to verify that $c \equiv a\ (mod\ m)$ and $c \equiv b\ (mod\ n)$:

$$a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \equiv a \cdot q_2 \cdot n\ (mod\ m)$$
$$a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \equiv a \cdot (1 - q_1 \cdot m)\ (mod\ m)$$
$$a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \equiv a\ (mod\ m)$$

Chinese Remainder Theorem

We still need to

1. Veryfy that it really is a solution.
2. Prove that it's the only solution *mod* $m \cdot n$.

We have $c \equiv a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \ (mod\ n \cdot m)$, and want to verify that $c \equiv a \ (mod\ m)$ and $c \equiv b \ (mod\ n)$:

$$a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \equiv a \cdot q_2 \cdot n \ (mod\ m)$$
$$a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \equiv a \cdot (1 - q_1 \cdot m) \ (mod\ m)$$
$$a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \equiv a \ (mod\ m)$$

$$a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \equiv b \cdot q_1 \cdot m \ (mod\ n)$$
$$a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \equiv b \cdot (1 - q_2 \cdot n) \ (mod\ n)$$
$$a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \equiv b \ (mod\ n)$$

Chinese Remainder Theorem

We still need to

1. Veryfy that it really is a solution.
2. Prove that it's the only solution $mod\ m \cdot n$.

We have $c \equiv a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \ (mod\ n \cdot m)$, and want to verify that $c \equiv a \ (mod\ m)$ and $c \equiv b \ (mod\ n)$:

$$a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \equiv a \cdot q_2 \cdot n \ (mod\ m)$$
$$a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \equiv a \cdot (1 - q_1 \cdot m) \ (mod\ m)$$
$$a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \equiv a \ (mod\ m)$$

$$a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \equiv b \cdot q_1 \cdot m \ (mod\ n)$$
$$a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \equiv b \cdot (1 - q_2 \cdot n) \ (mod\ n)$$
$$a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \equiv b \ (mod\ n)$$

So $c \equiv a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \ (mod\ n \cdot m)$ is indeed a solution.

Chinese Remainder Theorem

Is $c \equiv a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \ (mod \ n \cdot m)$ the unique congruence class solution to $x \equiv a \ (mod \ m), \quad x \equiv b \ (mod \ n)$?

Chinese Remainder Theorem

Is $c \equiv a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \ (mod \ n \cdot m)$ the unique congruence class solution mod $m \cdot n$ to $x \equiv a \ (mod \ m), \quad x \equiv b \ (mod \ n)$?

We know that $m, \ n$ are coprime. Suppose for cotradiction that another number x is a solution.

Chinese Remainder Theorem

Is $c \equiv a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \ (mod\ n \cdot m)$ the unique congruence class solution mod $m \cdot n$ to $x \equiv a \ (mod\ m), \quad x \equiv b \ (mod\ n)$?

We know that $m,\ n$ are coprime. Suppose for cotradiction that another number x is a solution. Then x is congruent to c both mod m and mod n. So $c - x$ must be a multiple of m and also a multiple of n.

Chinese Remainder Theorem

Is $c \equiv a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \ (mod \ n \cdot m)$ the unique congruence class solution mod $m \cdot n$ to $x \equiv a \ (mod \ m), \quad x \equiv b \ (mod \ n)$?

We know that $m, \ n$ are coprime. Suppose for cotradiction that another number x is a solution. Then x is congruent to c both mod m and mod n. So $c - x$ must be a multiple of m and also a multiple of n.

But since $m, \ n$ are coprime, that means that $c - x$ is a multiple of $m \cdot n$. So in fact $x \equiv c \ (mod \ m \cdot n)$, thus proving that c is in fact the unique solution mod $m \cdot n$.

Chinese Remainder Theorem

Is $c \equiv a \cdot q_2 \cdot n + b \cdot q_1 \cdot m \ (mod\ \ n \cdot m)$ the unique congruence class solution mod $m \cdot n$ to $x \equiv a \ (mod\ \ m), \quad x \equiv b \ (mod\ \ n)$?

We know that $m, \ n$ are coprime. Suppose for cotradiction that another number x is a solution. Then x is congruent to c both mod m and mod n. So $c - x$ must be a multiple of m and also a multiple of n.

But since $m, \ n$ are coprime, that means that $c - x$ is a multiple of $m \cdot n$. So in fact $x \equiv c \ (mod\ \ m \cdot n)$, thus proving that c is in fact the unique solution mod $m \cdot n$.

This completes the proof of the Chinese Remainder Theorem. $\square$

Fermat's Little Theorem

Theorem

Let a be any integer and p a prime number. If a, p are coprime, then:

$$a^{p-1} \equiv 1 \ (mod \ p).$$

Fermat's Little Theorem

Theorem

Let a be any integer and p a prime number. If a, p are coprime, then:

$$a^{p-1} \equiv 1 \ (mod \ p).$$

The proof is set up in stages:

1. $a \cdot 0,\ a \cdot 1,\ a \cdot 2, \ldots,\ a \cdot (p-1)$ all have different congruence classes mod p. There are p numbers here, so all congruence classes are taken. (It's a bijection.)
2. Then we must have:

$$(a \cdot 1) \cdot (a \cdot 2) \cdot \cdots \cdot (a \cdot (p-1)) \equiv (p-1)! \ (mod \ p)$$

3. From which we can derive the theorem.

Fermat's Little Theorem

Claim 1: $a \cdot 0,\ a \cdot 1,\ a \cdot 2, \ldots,\ a \cdot (p-1)$ all have different congruence classes mod p.

Suppose for contradiction that for some integers $i,\ j$, where $0 \leq i < j < p$ we have: $a \cdot i \equiv a \cdot j\ (mod\ p)$.

Fermat's Little Theorem

Claim 1: $a \cdot 0,\ a \cdot 1,\ a \cdot 2, \ldots,\ a \cdot (p-1)$ all have different congruence classes mod p.

Suppose for contradiction that for some integers $i,\ j$, where $0 \leq i < j < p$ we have: $a \cdot i \equiv a \cdot j \ (mod\ p)$.

Then $p | a \cdot (j - i)$.

Fermat's Little Theorem

Claim 1: $a \cdot 0,\ a \cdot 1,\ a \cdot 2, \ldots,\ a \cdot (p-1)$ all have different congruence classes mod p.

Suppose for contradiction that for some integers $i,\ j$, where $0 \leq i < j < p$ we have: $a \cdot i \equiv a \cdot j\ (mod\ p)$.

Then $p | a \cdot (j - i)$. But p is prime, so it would mean p either divides a, or $j - i$, or both. It can't divide $j - i$ since $0 \leq i < j < p$, and we assumed p, a are coprime. So we arrive at a contradiction. $\checkmark$

Fermat's Little Theorem

Claim 1: $a \cdot 0,\ a \cdot 1,\ a \cdot 2, \ldots,\ a \cdot (p-1)$ all have different congruence classes mod p.

Suppose for contradiction that for some integers $i,\ j$, where $0 \leq i < j < p$ we have: $a \cdot i \equiv a \cdot j\ (mod\ p)$.

Then $p | a \cdot (j-i)$. But p is prime, so it would mean p either divides a, or $j-i$, or both. It can't divide $j-i$ since $0 \leq i < j < p$, and we assumed p, a are coprime. So we arrive at a contradiction. $\checkmark$

Claim 2: $(a \cdot 1) \cdot (a \cdot 2) \cdot \cdots \cdot (a \cdot (p-1)) \equiv a^{p-1} \cdot (p-1)!\ (mod\ p)$. Notice that $a \cdot 0 \equiv 0\ (mod\ p)$, so in fact there's a bijection from $a \cdot 1,\ a \cdot 2, \ldots,\ a \cdot (p-1)$ to $1,\ 2,\ 3, dots,\ p-1$ defined by equivalence mod p.

Fermat's Little Theorem

We don't need to know which is equivalent to what to know that the product of the first set is congruent to the product of the second set. So indeed:

$$(a \cdot 1) \cdot (a \cdot 2) \cdot \cdots \cdot (a \cdot (p-1)) \equiv (p-1)! \ (mod \ p).$$

Fermat's Little Theorem

We don't need to know which is equivalent to what to know that the product of the first set is congruent to the product of the second set. So indeed:

$$(a \cdot 1) \cdot (a \cdot 2) \cdot \dots \cdot (a \cdot (p-1)) \equiv (p-1)! \ (mod \ p).$$

Claim 3: $a^{p-1} \equiv 1 \ (mod \ p)$.

Another way to write the above formula is:

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \ (mod \ p).$$

Fermat's Little Theorem

We don't need to know which is equivalent to what to know that the product of the first set is congruent to the product of the second set. So indeed:

$$(a \cdot 1) \cdot (a \cdot 2) \cdot \cdots \cdot (a \cdot (p-1)) \equiv (p-1)! \ (mod \ p).$$

Claim 3: $a^{p-1} \equiv 1 \ (mod \ p)$.

Another way to write the above formula is:

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \ (mod \ p).$$

So $p|(a^{p-1} - 1)(p-1)!$.

Fermat's Little Theorem

We don't need to know which is equivalent to what to know that the product of the first set is congruent to the product of the second set. So indeed:

$$(a \cdot 1) \cdot (a \cdot 2) \cdot \dots \cdot (a \cdot (p-1)) \equiv (p-1)! \ (mod \ p).$$

Claim 3: $a^{p-1} \equiv 1 \ (mod \ p)$.

Another way to write the above formula is:

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \ (mod \ p).$$

So $p|(a^{p-1}-1)(p-1)!$. But since p is prime, we have $GCD(p,(p-1)!) = 1$, so in fact $p|(a^{p-1}-1)$.

Fermat's Little Theorem

We don't need to know which is equivalent to what to know that the product of the first set is congruent to the product of the second set. So indeed:

$$(a \cdot 1) \cdot (a \cdot 2) \cdot \cdots \cdot (a \cdot (p-1)) \equiv (p-1)! \ (mod\ p).$$

Claim 3: $a^{p-1} \equiv 1 \ (mod\ p)$.

Another way to write the above formula is:

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \ (mod\ p).$$

So $p|(a^{p-1}-1)(p-1)!$. But since p is prime, we have $GCD(p,(p-1)!) = 1$, so in fact $p|(a^{p-1}-1)$. Which means the same thing $a^{p-1} \equiv 1 \ (mod\ p)$. This concludes the proof of Fermat's Little Theorem. $\square$

Correctness of the modular cipher

“Prove correctness of the cryptosystem” means ”prove that the message you get back is the one the sender intended.”

Correctness of the modular cipher

"Prove correctness of the cryptosystem" means "prove that the message you get back is the one the sender intended."

Recap: your public key is (p, e) where p is prime. Your secret key is d such that $e \cdot d \equiv 1 \ (mod \ p)$. If someone wants to send you a message $0 < M < p$, they send

$$C = M^e \ (mod \ p).$$

To read it decrypt it as

$$M' = C^d \ (mod \ p).$$

To prove *correctness*, we want to show that $M = M'$.

Correctness of the modular cipher

Want:

$$M' = M,$$

where M' is the congruence class of $(M^e)^d$ mod p.

Correctness of the modular cipher

Want:

$$M' = M,$$

where M' is the congruence class of $(M^e)^d$ mod p.

$(M^e)^d = M^{ed}$. We know that $ed \equiv 1\ (mod\ p)$, and so by Fermat's Little Theorem, for any $0 < M < p$:

$$M^{ed} \equiv M\ (mod\ p).$$

Therefore, since by definition of M', $M^{ed} \equiv M'\ (mod\ p)$ and $0 \geq M' < p$, we conclude that $M = M'$. $\square$

Corectness of RSA

RSA recap: take two big primes $p,\ q$. Then calculate $n = p \cdot q$ and $\varphi(n) = (p-1)(q-1)$. Find two numbers $e,\ d$ such that $e \cdot d \equiv 1\ (mod\ \varphi(n))$. Your public key is (n, e). Your secret key is d. If someone wants to send you a message $0 < M < n$, they encrypt it as

$$C = M^e\ (mod\ n)$$

and send that. You decrypt is as

$$C^d \equiv M'\ (mod\ n),$$

the concruence class of $(M^e)^d$ mod n. As before, we would like to prove the *correctness* of RSA, i.e. that

$$M' = M.$$

Corectness of RSA

Proof: we have $(M^e)^d = M^{e \cdot d} \equiv M' \ (mod \ n)$, where $0 < M, M' < n$ and we would like to show that $M = M'$.

Corectness of RSA

Proof: we have $(M^e)^d = M^{e \cdot d} \equiv M' \ (mod\ n)$, where $0 < M, M' < n$ and we would like to show that $M = M'$.

We know that $e \cdot d \equiv 1 \ (mod\ (p-1)(q-1))$. So $e \cdot d = 1 + m \cdot (p-1) \cdot (q-1)$ for some integer m.

Corectness of RSA

Proof: we have $(M^e)^d = M^{e \cdot d} \equiv M' \ (mod \ n)$, where $0 < M, M' < n$ and we would like to show that $M = M'$.

We know that $e \cdot d \equiv 1 \ (mod \ (p-1)(q-1))$. So $e \cdot d = 1 + m \cdot (p-1) \cdot (q-1)$ for some integer m. Then in particular:

$e \cdot d \equiv 1 \ (mod \ p-1)$
$e \cdot d \equiv 1 \ (mod \ q-1)$.

Corectness of RSA

Proof: we have $(M^e)^d = M^{e \cdot d} \equiv M' \ (mod\ n)$, where $0 < M, M' < n$ and we would like to show that $M = M'$.

We know that $e \cdot d \equiv 1 \ (mod\ (p-1)(q-1))$. So $e \cdot d = 1 + m \cdot (p-1) \cdot (q-1)$ for some integer m. Then in particular:

$e \cdot d \equiv 1 \ (mod\ p-1)$
$e \cdot d \equiv 1 \ (mod\ q-1)$.

So by Fermat's Little Theorem,
$M^{e \cdot d} \equiv M \ (mod\ p)$
$M^{e \cdot d} \equiv M \ (mod\ q)$

Corectness of RSA

Proof: we have $(M^e)^d = M^{e \cdot d} \equiv M' \ (mod \ n)$, where $0 < M, M' < n$ and we would like to show that $M = M'$.

We know that $e \cdot d \equiv 1 \ (mod \ (p-1)(q-1))$. So $e \cdot d = 1 + m \cdot (p-1) \cdot (q-1)$ for some integer m. Then in particular:

$e \cdot d \equiv 1 \ (mod \ p-1)$
$e \cdot d \equiv 1 \ (mod \ q-1)$.

So by Fermat's Little Theorem,
$M^{e \cdot d} \equiv M \ (mod \ p)$
$M^{e \cdot d} \equiv M \ (mod \ q)$

So we know that $M' \equiv M \ (mod \ p)$ and $' \equiv M \ (mod \ q)$. Since $p, \ q$ are coprime, and $0 \leq M', M < p \cdot q$ by Chinese Remainder Theorem we know that there is only one such number.

Corectness of RSA

Proof: we have $(M^e)^d = M^{e \cdot d} \equiv M' \ (mod \ n)$, where $0 < M, M' < n$ and we would like to show that $M = M'$.

We know that $e \cdot d \equiv 1 \ (mod \ (p-1)(q-1))$. So $e \cdot d = 1 + m \cdot (p-1) \cdot (q-1)$ for some integer m. Then in particular:

$e \cdot d \equiv 1 \ (mod \ p-1)$
$e \cdot d \equiv 1 \ (mod \ q-1)$.

So by Fermat's Little Theorem,
$M^{e \cdot d} \equiv M \ (mod \ p)$
$M^{e \cdot d} \equiv M \ (mod \ q)$

So we know that $M' \equiv M \ (mod \ p)$ and $' \equiv M \ (mod \ q)$. Since $p, \ q$ are coprime, and $0 \leq M', M < p \cdot q$ by Chinese Remainder Theorem we know that there is only one such number. M is such a number, so $M' = M$. This proves *correctness* of RSA.