

VARIOUS TOPICS

MATH 372. FALL 2005. INSTRUCTOR: PROFESSOR AITKEN

Here is a brief summary of some of the recent topics covered in class.

1. LINEAR CONGRUENCES

Suppose you want to solve the congruence $ax \equiv b \pmod{m}$. In other words, suppose you want to solve the linear equation $\bar{a}x = \bar{b}$ in \mathbb{Z}_m . If $(a, m) = 1$ then \bar{a} is a unit and the equation has a unique solution:

Theorem 1. *Suppose $(a, m) = 1$. Then the equation $\bar{a}x = \bar{b}$ has a unique solution: $x = \bar{b}\bar{a}^{-1}$. In other words, the congruence $ax \equiv b \pmod{m}$ has a unique solution modulo m .*

Example 1. Suppose you want to solve $2x \equiv 7 \pmod{15}$. Since $\bar{2}^{-1} = \bar{8}$, we consider $\bar{7} \cdot \bar{8} = \bar{11}$. So the solution is $x \equiv 11 \pmod{15}$.

Technically there are an infinite number of solutions to the congruence: $-4, 11, 26, \dots$. However, they are all congruent modulo 15. In other words, the equation $\bar{2}x = \bar{7}$ has a unique solution.

What do you do if $(a, m) = d > 1$? In other words, what happens if \bar{a} is not a unit in U_m ? It turns out that there are either zero or d solutions to $\bar{a}x = \bar{b}$.

Theorem 2. *Suppose $(a, m) = d > 1$. Then $ax \equiv b \pmod{m}$ has a solution if and only if $d \mid b$. If it has a solution, then it has d distinct solutions modulo m . In other words, $\bar{a}x = \bar{b}$ has d solutions in \mathbb{Z}_m .*

Proof. Suppose that $ax_0 \equiv b \pmod{m}$. Then m divides $ax_0 - b$. Thus $ax_0 - b = km$ for some k . This means that $x_0a - km = b$. So b is a linear combination of a and m . By an earlier result, $d = (a, m)$ divides any linear combination of a and m . So $d \mid b$.

(I will skip the rest of the proof for now). □

How do you solve $ax \equiv b \pmod{m}$? First check to see if $d = (a, m)$ divides b . If not there are zero solutions by the above theorem. Otherwise, consider $a'x \equiv b' \pmod{m'}$ where $a' = a/d$ and $b' = b/d$ and $m' = m/d$. Find a solution x_0 to $a'x \equiv b' \pmod{m'}$. Now the d solutions are given by $x_0 + im'$ where $i = 0, 1, \dots, d - 1$. (I will skip the proof of this for now).

Example 2. Suppose you want to solve $6x \equiv 15 \pmod{33}$. Then $d = (6, 33) = 3$, and since 3 divides 15 there will be $d = 3$ solutions modulo 33.

First we divide everything by 3 giving us $2x \equiv 5 \pmod{11}$. The inverse of $\bar{2}$ is $\bar{6}$, so the solution is $5 \cdot 6 \equiv 8 \pmod{11}$. So the solutions are 8, $8 + 11$, and $8 + 2 \cdot 11$.

Final answer: 8, 19, and 30. Of course there are an infinite number of solutions (41 or 52 for example), but they are all congruent modulo 33 to the given three. Simply put, $\bar{6}x = \bar{15}$ has three solutions in \mathbb{Z}_{33} .

2. CRYPTOGRAPHY

A mathematical code requires two functions: an encryption function $E(x)$ and a decryption function $D(x)$. These two functions must be inverse functions: $D(x) = E^{-1}(x)$.

Before RSA, the functions used were such that if eavesdroppers found out $E(x)$, they could easily figure out $D(x)$. Public key systems such as RSA are important because $E(x)$ can be made public without $D(x)$ being discovered.

Example 3 (Non public key code). If $E(x) = \overline{3}x + \overline{21}$ is the encryption function $\mathbb{Z}_{25} \rightarrow \mathbb{Z}_{25}$, then

$$D(x) = E^{-1}(x) = (x - \overline{21})\overline{3}^{-1} = (x + \overline{4})\overline{17} = \overline{17}x + \overline{18}.$$

3. RSA

These codes use functions $U_n \rightarrow U_n$ given by formulas $E(x) = x^e$ and $D(x) = x^f$ where n is a large composite number. The numbers e and f are related by the formula $ef \equiv 1 \pmod{\phi(n)}$. The numbers e and n are public, so $E(x) = x^e$ is known to all. The number f is private, only the person (or computer) setting up the code knows $D(x) = x^f$. The factorization of n and the number $\phi(n)$ must also be kept private: if discovered by eavesdroppers then $D(x)$ can be figured out from $E(x)$.

Example 4. Suppose Alice wants to set up an RSA code. She needs to choose two large prime numbers. She chooses the following:

$$p_1 = 1957343243 \quad q_1 = 97034897.$$

(you need a computer program in order to generate large primes. The `isprime` command in Maple can be used to help generate large primes.) The product is

$$n_1 = p_1q_1 = 189930599978150971.$$

Even this 18 digit number is too small with current technology. For internet transactions the number should close to 2^{128} (a 39 digit number) and for the highest security close to 2^{1024} (a 309 digit number).

Next she figures out $\phi(n_1)$ as follows:

$$\phi(n_1) = \phi(p_1)\phi(q_1) = (p_1 - 1)(q_1 - 1) = 189930597923772832.$$

She must now choose an exponent e_1 which is relatively prime to $\phi(n_1)$. She chooses the number $e_1 = 11311351$ and checks that $(e_1, \phi(n_1)) = 1$ using the Euclidean algorithm.¹ In fact, using Maple's extended Euclidean algorithm function called `igcdex` she can quickly find u and v such that

$$11311351u + 189930597923772832v = 1.$$

The given u leads to an inverse to e_1 modulo $\phi(n_1)$. This inverse is found to be $f_1 = 187854724768504455$. So $e_1f_1 \equiv 1 \pmod{n_1}$.

Alice now has all the information she needs for her code.

Public information (public key): $n_1 = 189930599978150971$ and $e_1 := 11311351$.

¹One popular method for choosing e_1 is to choose a reasonably sized prime number that does not divide $\phi(n_1)$. Such a number is automatically relatively prime to $\phi(n_1)$.

Private information (private key):² $f_1 = 187854724768504455$ (although $p_1, q_1, \phi(n_1)$ are not needed any more, they must be kept private as well since knowing any of them can allow others to calculate f_1 using the Euclidean algorithm.)

Others can now send her secret information using $E(x) = x^{e_1}$ considered as a function $U_{n_1} \rightarrow U_{n_1}$, and she can decode it using $D(x) = x^{f_1}$ considered as a function $U_{n_1} \rightarrow U_{n_1}$.

She can receive messages now. However, for her to send messages back, others must give her their public information (public keys).

Example 5. Alice gives Bob her public information. Now Bob can send messages to Alice. However, to get messages back, Bob has to develop his own code.

He chooses

$$p_2 = 4150371209 \quad q_2 = 10007032897.$$

The product is

$$n_2 = p_2 q_2 = 41532901223224662473,$$

and

$$\phi(n_2) = \phi(p_2)\phi(q_2) = (p_2 - 1)(q_2 - 1) = 41532901209067258368.$$

He chooses $e_2 = 781721$ and checks that $(e_2, \phi(n_2)) = 1$ using Maple's extended Euclidean algorithm function called `igcdex` which also gives him values of u and v such that

$$781721u + 41532901209067258368v = 1.$$

This u leads to the inverse $f_2 = 21560771902702873769$.

Public information (public key): $n_2 = 41532901223224662473$ and $e_2 := 781721$.

Private information (private key): $f_2 = 21560771902702873769$ (although $p_2, q_2, \phi(n_2)$ are not needed any more, they must be kept private as well.)

Example 6. Now Bob wants to send Alice a secret message “the treasure is under the elm tree”. First they need to both agree on how to translate text into numbers. Suppose that they choose the following method (which can be made public): they split the message into blocks of three letters (in the real world, larger blocks should be used), and convert to integers by using 01 for ‘a’, using 02 for ‘b’, . . . , 26 for ‘z’. Other two digit combinations can be used for punctuation: for example they decide on 55 for space and 99 for end of message.

So the message “the treasure is under the elm tree” would be written as the following 12 numbers³

200805 552018 50119 211805 550919 552114 40518 552008 55505 121355 201805 55599

Now Bob wants to make sure that Alice knows the message came from him, so he signs it as follows. He first takes his name ‘bob’ written as numbers 021502 = 21502 and modifies it in way that only he can do: he computes $D_2(21502) \equiv 21502^{f_2} \pmod{n_2}$.

Now he sends his message to Alice. Recall $E_1(x) = x^{e_1}$ is computed modulo n_1 . He sends the numbers

$$E_1(200805) \ E_1(552018) \ E_1(50119) \ E_1(211805) \ E_1(550919) \ E_1(552114) \ E_1(40518) \\ E_1(552008) \ E_1(55505) \ E_1(121355) \ E_1(201805) \ E_1(55599) \ D_2(21502)$$

²Many people prefer d_1 to f_1 since d stands for “decryption” just as e stands for “encryption”.

³These numbers are considered in U_{n_1} so they must be relatively prime to n_1 . Since the numbers are less than p_1 and q_1 , the only primes dividing n_1 , they are automatically relatively prime to n_1 .

Each one of these numbers is large (about the size of n_1) so I haven't displayed them in their full glory (or "full gory").⁴

If an eavesdropper intercepts these numbers, no damage is done since it is almost impossible for an eavesdropper to figure out $D_1(x)$ and use it to decode it.

Now Alice takes these numbers and applies $D_1(x) = x^{f_1}$ (modulo n_1) to each number. So she converts the encrypted $E_1(200805)$ into $D_1(E_1(200805)) = 200805$. Remember that $D_1(x) = E_1^{-1}(x)$ so D_1 and E_1 cancel each other out. She recovers the numbers

200805 552018 50119 211805 550919 552114 40518 552008 55505 121355 201805 55599

and converts it into the message "the treasure is under the elm tree". She realizes that $D_2(21502)$ is a signature. To check that it really uses $D_2(x)$, which only Bob knows, she applies $E_2(x)$ to it (which everyone knows). Since $E_2(D_2(21502)) = 21502$ is 'Bob' she recognizes that the signature must have used $D_2(x)$ and so the message had to have come from Bob.

What makes this system work? First of all, factoring large numbers takes more time than is computationally feasible if the number n is large enough. Also, it is infeasible to find $\phi(n)$ if you cannot factor n . Finally, finding an inverse f to e modulo $\phi(n)$ is infeasible if you do not know what $\phi(n)$ is.

You might have observed that the RSA relies on raising x to a large power. This is feasible as long as it is done in stages, and you reduce mod n after each stage. Second of all it relies on the following fact:

Lemma 1. *Suppose that $ef \equiv 1 \pmod{\phi(n)}$. Consider $E(x) = x^e$ and $D(x) = x^f$ as functions $U_n \rightarrow U_n$. Then $E(x)$ and $D(x)$ are inverse functions.*

Proof. According to the definition of *inverse function*, we must show that $D(E(\bar{a})) = \bar{a}$ and $E(D(\bar{a})) = \bar{a}$ for all $\bar{a} \in U_n$.

So let $\bar{a} \in U_n$ be given. Since $ef \equiv 1 \pmod{\phi(n)}$ we know that $ef - 1 = k\phi(n)$ for some k . Thus $ef = 1 + k\phi(n)$. So

$$E(D(\bar{a})) = E(\bar{a}^f) = (\bar{a}^f)^e = \bar{a}^{ef} = \bar{a}^{1+k\phi(n)} = \bar{a} \cdot (\bar{a}^k)^{\phi(n)} = \bar{a} \cdot \bar{1} = \bar{a}$$

using the fact that $(\bar{a}^k)^{\phi(n)} = \bar{1}$ by Euler's theorem. Similarly

$$D(E(\bar{a})) = D(\bar{a}^e) = (\bar{a}^e)^f = \bar{a}^{ef} = \bar{a}^{1+k\phi(n)} = \bar{a} \cdot (\bar{a}^k)^{\phi(n)} = \bar{a} \cdot \bar{1} = \bar{a}.$$

□

4. EXAMPLES OF EULER'S CRITERIA

Recall that determining if the diophantine equation $aX^2 + bY^2 + cZ^2 = 0$ has a solution comes down to Euler's criteria. We assume that a, b, c are square-free, non-zero, and pairwise relatively prime.

⁴If Bob doesn't want anyone but Alice to read his signature, he should probably split $D_2(21502)$ into small numbers and apply $E_1(x)$ to the pieces before sending it to Alice. That way only Alice can have access to his signature. (The purpose for splitting up $D_2(21502)$ is to make sure that it is smaller and relatively prime to n_1 .)

Theorem 3 (Euler's Criteria. Fully proved by Legendre). *Suppose that a, b, c are square-free, non-zero, and pairwise relatively prime integers. Then $aX^2 + bY^2 + cZ^2 = 0$ has a non-trivial integral solution if and only if (i) the integers $a, b,$ and c do not all have the same sign, (ii) $-ab$ is a square modulo $|c|$, (iii) $-ac$ is a square modulo $|b|$, and (iv) $-bc$ is a square modulo $|a|$.*

Thus if *any* of the criteria fail then the equation has no non-trivial solutions.

Example 7. The diophantine equation $5X^2 + 6Y^2 + 22Z^2 = 0$ has no solution since it fails criterion (i): all the signs are equal.

Example 8. The diophantine equation $5X^2 + 6Y^2 - 11Z^2 = 0$ obviously has a non-trivial solution (just look at $(1, 1, 1)$). However, let's see if we can use Euler's criterion to derive this fact.

We first check to see if $5, 6, -11$ have the same sign. Observe that two are positive, and one is negative. So the first criterion checks out.

Next we see if $-5 \cdot 6 = -30$ is a square modulo 11. We use the Legendre Symbol:

$$\left(\frac{-30}{11}\right) = \left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1.$$

So $-5 \cdot 6$ is a square modulo 11.

Next we see if $-5 \cdot (-11) = 55$ is a square modulo 6. We cannot use the Legendre Symbol since 6 is not an odd prime. However, we can get by just fine without the bloody Legendre Symbol! We just observe that $55 \equiv 1 \pmod{6}$, and 1 is a square modulo 6. So $-5 \cdot (-11)$ is a square modulo 6.

Finally we see if $-(6) \cdot (-11) = 66$ is a square modulo 5.

$$\left(\frac{66}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

So $-(6) \cdot (-11)$ is a square modulo 5.

We conclude that $5X^2 + 6Y^2 - 11Z^2 = 0$ has a solution.

Example 9. Consider the diophantine equation $5X^2 + Y^2 = 3Z^2$. Does this equation have a non-trivial integral solution? First convert to $5X^2 + Y^2 - 3Z^2 = 0$.

We first check to see if $5, 1, -3$ have the same sign. Observe that two are positive, and one is negative. So the first criterion checks out.

Next we see if $-5 \cdot 1 = -5$ is a square modulo 3. We use the Legendre Symbol:

$$\left(\frac{-5}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

So $-5 \cdot 1$ is a square modulo 3.

Next we see if $-5 \cdot (-3)$ is a square modulo 1. Everything is congruent to 0 modulo 1, and 0 is a square, so everything is a square modulo 1. In particular, $-5 \cdot (-3)$ is a square modulo 1.

Finally we see if $-1 \cdot (-3) = 3$ is a square modulo 5:

$$\left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

So $-1 \cdot (-3)$ is *not* a square modulo 5.

Since one of the criteria fails, $5X^2 + Y^2 = 3Z^2$ does not have a non-trivial solution.

Example 10 (Optional). Is it possible to show that the above equation $5X^2 + Y^2 = 3Z^2$ has no non-trivial solution without resorting to Euler's criteria? The answer is yes. Since Euler's criterion failed modulo 5, let's try to generate a contradiction using 5 as a modulus.

Suppose that $5X^2 + Y^2 = 3Z^2$ has a solution, and suppose that (x_0, y_0, z_0) is a primitive solution. So $5x_0^2 + y_0^2 = 3z_0^2$. Modulo 5 this equation becomes $y_0^2 \equiv 3z_0^2 \pmod{5}$. Now the squares modulo 5 are found to be 0, 1, or 4. If $z_0^2 \equiv 1 \pmod{5}$ then $y_0^2 \equiv 3z_0^2 \equiv 3 \pmod{5}$ which cannot happen since 3 is not a square modulo 5. Similarly, if $z_0^2 \equiv 4 \pmod{5}$ then $y_0^2 \equiv 3z_0^2 \equiv 12 \equiv 2 \pmod{5}$ which cannot happen since 2 is not a square modulo 5. This leaves $z_0^2 \equiv 0 \pmod{5}$. In this case, $y_0^2 \equiv 3z_0^2 \equiv 0 \pmod{5}$.

So 5 divides both y_0^2 and z_0^2 . This means 5 divides y_0 and z_0 . So really, 25 must divide y_0^2 and z_0^2 . Since $5x_0^2 = 3z_0^2 - y_0^2$, we conclude that 25 divides $5x_0^2$. So 5 divides x_0^2 . Thus 5 divides x_0 .

Therefore, 5 divides x_0 , y_0 , and z_0 . Thus (x_0, y_0, z_0) is not primitive, a contradiction.

Example 11. Does $2X^2 - 103Y^2 - Z^2 = 0$ have a non-trivial integral solution?

We first check to see if 2, -103, -1 have the same sign. Observe that one is positive, and two are negative. So the first criterion checks out.

Next we see if $-2 \cdot (-103)$ is a square modulo 1. Everything is congruent to 0 modulo 1, and 0 is a square, so everything is a square modulo 1. In particular, $-2 \cdot (-103)$ is a square modulo 1.

Next we see if $-2 \cdot (-1) = 2$ is a square modulo 103. We use the Legendre Symbol:

$$\left(\frac{2}{103}\right) = 1$$

since $103 \equiv 7 \pmod{8}$. So $-2 \cdot (-1)$ is a square modulo 103.

Finally we see if $-(-103) \cdot (-1) = -103$ is a square modulo 2. We cannot use the Legendre Symbol since 2 is not an odd prime. However, we can precede as follows: $-103 \equiv 1 \pmod{2}$ and 1 is a square modulo 2, so $-(-103) \cdot (-1)$ is a square modulo 2.

Since all of the criteria succeed: $2X^2 - 103Y^2 - Z^2 = 0$ has a non-trivial solution.⁵

DR. WAYNE AITKEN, CAL. STATE, SAN MARCOS, CA 92096, USA
E-mail address: waitken@csusm.edu

⁵A solution turns out to be (8, 1, 5).