MA341 Number Theory
Kalin Kostadinov

Lecture 2 (20 May 2010)

Small Tool, Great Use: The Language of Congruences

Equations without solutions. In the previous lecture we have seen that for Linear Diophantine equations there exists a simple criterion that distinguishes between the ones that have any solutions, and the ones that have not. Namely, the general LDE $a_0x_0 + a_1x_1 + \cdots + a_nx_n = b$ has a solution if and only if every number that divides all of the coefficients $a_0, a_1, \ldots, a_n$, divides b as well. Paraphrasing this criterion, we could say that a LDE has no solution if and only if there exists a number d which divides all of the coefficients $a_0, a_1, \ldots, a_n$, but does not divide b.
It is worth pausing here for a second and thinking about what it did: we had an equivalence, ("if and only if") and negated both sides. The universal quantifier in the first version – "every number" – became an existential quantifier when negated - "there exists". Such play with logic is very usual in mathematics texts, but may be hard to grasp when first encountered; mastering it to the point when it becomes intuitive is going to greatly improve both your reading and writing skills. A good exercise to this end is to go through a list of theorems from an arbitrary book, and negate every statement.
Going back to the LDE criterion, we look at the following example:

$$1255x + 70y + 425z = 37373$$

Does it has any solutions? You will not need to look at it for a second time to see that the answers is no. It is evident that 5 divides the coefficients on the left, and hence for any values of the variables x, y, z 5 divides the left hand side of the equation; but it does not divide the right hand side.
There are two points to be made here. One, we didn't really performed the division to get our conclusion (else, what is the quotient?), the only thing that we are immediately seeing despite the large numbers are the remainders. Or, to reiterate, the important information is in the remainders. So in the next and in the last sections we will introduce two ways to concentrate on this essential information.
The second point to be made is that it wasn't really significant that we have a LDE to get the 'no solutions' conclusion. The same conclusion is immediately valid for example about the non-linear equation $1255x^2+70y^3+425xyz = 37373$. We will generalize this to a necessary condition for existence of solutions for Diophantine equations in the next section, where we could write more concisely with the notations introduced there.

Congruences. We take a more formal approach now, and give a few rigorous definitions and then list some properties connecting them.

Definition. Let a and b be integers. We say that a *divides* b, and write $a|b$, if there exists an integer c, such that $b = ac$.

Definition. Given two arbitrary integers a, b and a positive integer m, we say that a *is congruent to* b *modulo* m, and write $a \equiv b \pmod{m}$ when $m|b-a$.

For example, $7|42$, since $42 = 7 \times 6$, and $23 \equiv 11 \pmod{6}$, since $23 - 11 = 12$ and $6|12$.
We next list a few elementary properties of congruences. Let a, b, c be arbitrary integers and let m, n be positive integers. Then

- $a \equiv a \pmod{m}$
- If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$
- If $a \equiv b \pmod{m}$, and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$
- If $a \equiv b \pmod{m}$, then $a + c \equiv b + c \pmod{m}$
- If $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{m}$
- If $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$
- If $a \equiv b \pmod{m}$, and $n|m$ then $a \equiv b \pmod{n}$

All of this are easy to prove, and we leave the proofs as an exercise.
One could also write congruences with an unknown variable to solve for.
For example, let us find all integers s, which are solutions of the congruence $7x^2 + 3x - 4 \equiv 0 \pmod{15}$, i.e. we need values $s_1, s_2, \ldots, s_k, \ldots$ such that

$$7x^2 + 3x - 4 \equiv 0 \pmod{15} \Rightarrow \exists i, \quad x \equiv s_i \pmod{m}$$

So we consecutively simplify

$$\begin{aligned} 7x^2 + 3x - 4 \equiv 0 \pmod{15} &\Leftrightarrow 14x^2 + 6x - 8 \equiv 0 \pmod{15} &\Leftrightarrow \\ -x^2 + 6x - 8 \equiv 0 \pmod{15} &\Leftrightarrow x^2 - 6x + 9 - 1 \equiv 0 \pmod{15} &\Leftrightarrow \\ (x-3)^2 \equiv 1 \pmod{15} & \end{aligned}$$

And since $1^2 \equiv 4^2 \equiv 11^2 \equiv 14^2 \equiv 1 \pmod{15}$ our list is $4, 7, 11, 17$.
Note that we could add others integers to the list of the solution, for example -4 or 2 are solutions, as one could easily check. But they are not really new solutions, since $-4 \equiv 11 \pmod{15}$ and $2 \equiv 17 \pmod{15}$. So when giving the solutions of a congruence, we list only the solutions that are pairwise non-congruent. Since there are only finitely many non-congruent integers for any fixed modulus (to be precise: there are only m non-congruent numbers modulo m - for example $0, 1, 2, \ldots, m-1$ give such a maximal system of representatives), one could always solve a congruence equation by an exhaustion methods - check all the finitely many non-congruent numbers in a system of representatives of the residues of the modulus, to see which of them are solutions.
As an illustration, we solve the congruence $x^3 + 2y^2 \equiv 3 \pmod{5}$. For a system of non-congruent numbers modulo 5 we choose $0, 1, 2, 3, 4$ and we have 25 pairs of possible solutions for (x, y). We summarize the results for $x^3 + 2y^4$ in the

following table:

x:y	0	1	2	3	4
0	0	2	3	3	2
1	1	3	4	4	3
2	3	0	1	1	0
3	2	4	0	0	4
4	4	1	2	2	1

So we see that all the solutions are
$x \equiv 0 \pmod 5, y \equiv 2 \pmod 5$, or $x \equiv 0 \pmod 5, y \equiv 3 \pmod 5$, or
$x \equiv 1 \pmod 5, y \equiv 1 \pmod 5$, or $x \equiv 1 \pmod 5, y \equiv 4 \pmod 5$, or
$x \equiv 2 \pmod 5, y \equiv 0 \pmod 5$.
The following simple observation leads to an important necessary condition for existence of solutions of diophantine equations:
Let the diophantine equations $f(x_1, x_2, \ldots, x_k) = 0$ has at least one solution. Then for any positive integer m, the congruence $f(x_1, x_2, \ldots, x_k) \equiv 0 \pmod m$ also has a solution.
Therefore, if we could find a modulus m, for which the congruence has no solutions, we can conclude that the original diophantine equation has no solutions as well.
Example: Consider the equation $15x^3 - y^6 = 32$, and take $m = 7$. The congruence $15x^3 - y^6 \equiv 32 \pmod 7$ is equivalent to $x^3 - y^6 \equiv 4 \pmod 7$ and the last one has no solutions, as $x^3 \equiv 0, 1, 6 \pmod 7$ and $y^6 \equiv 0, 1 \pmod 7$ so $x^3 - y^6$ could be congruent to $0, 1, 5, 6$ modulo 7, but never 4 (mod 7). Hence $x^3 - y^6 \equiv 4 \pmod 7$ has no solutions, and neither does the equivalent congruence $15x^3 - y^6 \equiv 32 \pmod 7$.
Therefore the original equation, $15x^3 - y^6 = 32$ has no integral solutions.

The Chinese Remainders Theorem. A lot of problems lead to two or three linear congruences that have to be solved together. Consider for example the following riddle. A poor fellow had three daughters, and a small fortune of x golden coins. Once it was time to marry the first one, he threw a big party, which cost him 2 coins, and split the leftover of his fortune into equal parts between his three daughters, his wife and himself. Three years later, with hard work he managed to accumulate as much gold as he had prior to the marriage of his first daughter, and threw a second party, to marry his second daughter. This time the party cost him 3 golden coins (inflation was known even to people in the ancient times), and afterwards he split the remaining money equally between himself, his wife, and his two daughters. Two more years passed before he managed to recover from the spending and bring his fortune back to x golden coins again. Then he threw a third party, which cost him 5 golden coins, and split the leftover of his fortune between himself, his wife, and his last daughter. What was the fortune he had to begin with?
Reading again carefully, we find out that all we know about the number of

golden pieces, x, is that it satisfies the following three congruences:

$$\begin{aligned} x &\equiv 2 \pmod 5 \\ x &\equiv 3 \pmod 4 \\ x &\equiv 4 \pmod 3 \end{aligned}$$

With some trial and error guessing, we find out that a possible solution is $x = 7$. The following statement, known as the Chinese Remainder Theorem, gives us a condition when such systems are solvable, and a bound of the minimal solution.

Theorem. *Let k be any natural number. Given arbitrary integers $c_1, c_2, \ldots, c_k$ and positive integers $m_1, m_2, \ldots m_k$ which are pairwise relatively prime, the system of linear congruences*

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\cdots \\ x &\equiv c_k \pmod{m_k} \end{aligned}$$

has a unique solution $x \equiv x_0 \pmod{m_1 m_2 \ldots m_k}$

There are various algorithms how to solve such systems of congruences, which help to reduce the amount of guessing necessary. A fast and still a simple one is to first find numbers $x_1, x_2, \ldots, x_k$ such that

$$\begin{array}{lllllll} x_1 \equiv 1 \pmod{m_1} & x_2 \equiv 0 \pmod{m_1} & \cdots & x_k \equiv 0 \pmod{m_1} \\ x_1 \equiv 0 \pmod{m_2} & x_2 \equiv 1 \pmod{m_2} & \cdots & x_k \equiv 0 \pmod{m_2} \\ \cdots & & \cdots\cdots & \cdots \\ x_1 \equiv 0 \pmod{m_k} & x_2 \equiv 0 \pmod{m_k} & \cdots & x_k \equiv 1 \pmod{m_k} \end{array}$$

Then the solution is $x_0 = c_1 x_1 + c_2 x_2 + \ldots c_k x_k$. For example, in the golden coins case we easily find $x_1 = 36$ (a multiple of 12, one greater than a multiple of 5), $x_2 = 45$ and $x_3 = 40$, so that
$x \equiv 2 * 36 + 3 * 45 + 4 * 40 \pmod{60} \Leftrightarrow x \equiv 367 \pmod{60} \Leftrightarrow x \equiv 7 \pmod{60}$.