COMS10003 Lecture 8.

Julian Gough 2014-11-16

Preface

These are outline notes for lecture 8; they are based on *Number Theory with Computer Applications* by Ramanujachary Kumanduri and Cristina Romero. This is an excellent book, but the material can be found in many number theory and discrete mathematics books. A manicule (☜ or ☞) is used to indicate that a proof, derivation or piece of material has been omitted from the lecture but will be covered in the workshop.

Modular arithmetic

The idea behind modular arithmetic is to use remainders and so on to make an actual arithmetic system. It relies on *congruence*. If a, b and c are integers, we say that a *is congruent to* b *modulo* m if $m|(a-b)$. This is written $a \equiv b \pmod{m}$ and sometimes people say a is equivalent to b modulo m or even a is equal to b modulo m.

There are different ways of thinking about this, we could say a is the same as b up to a multiple of m, or we could use the language of remainders we developed above and say $a \equiv b \pmod{m}$ is $(a \bmod m) = (b \bmod m)$. Note the way the use of mod differs, if $r = a \bmod m$ then r is the remainder and $0 \leq r < m$ whereas if $a \equiv b \pmod{m}$ then a and b are conjugate, neither has to be less than m.

As an example the integers $n \equiv 3 \pmod{8}$ are $n = 3 + 8m$ where m is an integers, so they include -5, 3, 11 and so on.

Congruence is an example of an *equivalence relation*, an equivalence relation is any relationship between pairs of elements in a set that satisfies reflexivity, symmetry and transitivity. So, for a set X the relationship $\sim$ is an equivalence relationship if

1. Reflexivity: if $x \in X$ then $x \sim x$.
2. Symmetry: if x and y are in X and $x \sim y$ then $y \sim x$.
3. Transitivity: if x, y and z are in X and $x \sim y$ and $y \sim z$ then $x \sim z$.

Verifying that congruence is an equivalence relation is just a matter of checking each of those three properties.☜

☞This lemma gives some of the properties of congruences

Lemma. If a, b, c, d are integers and m a positive integer then

1. $a \equiv b \pmod{m}$ implies $ac \equiv bc \pmod{m}$.
2. $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ implies $a + c \equiv b + d \pmod{m}$.

3. $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ implies $ac \equiv bd \pmod{m}$.

4. $a \equiv b \pmod{m}$ implies $a^k \equiv b^k \pmod{m}$ for positive integers k.

5. $a \equiv b \pmod{m}$ and $d|m$ for some d a positive integer then $a \equiv b \pmod{d}$.

6. $ac \equiv bc \pmod{m}$ implies $a \equiv b \pmod{n}$ where $n = m/(c, m)$.

This means for example that $2^{4k} \equiv 1 \pmod{5}$ because $2^{4k} = 16^k$ and $16 \equiv 1 \pmod{5}$.

Another lemma shows that we can study congruence modulo composite numbers by looking at congruences modulo the factors.

Lemma. If $(m, n) = 1$ then $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$ if and only if $a \equiv b \pmod{mn}$.

Proof: If $m|(a - b)$ then $a - b = km$ for some k, now $n|(a - b)$ with $(m, n) = 1$ so $n|k$ and hence $nm|(a - b)$ or $a \equiv b \pmod{mn}$. Conversely, if $a \equiv b \pmod{mn}$ then $a \equiv b \pmod{d}$ for any divisor d of mn including m and n.□

Modular inverses

Modular arithmetic is an example of a mathematical system where we have taken ideas from somewhere else, in this case, ordinary arithmetic and changed the rules slightly, in this case, by being interested in conguence instead of equality. Modular arithmetic has addition and multiplication based on the addition and multiplication in ordinary arithmetic, but it turns out to have different properties. The most striking difference might be related to multiplicative inverses. Integers don't have integer multiplicative inverses, so $1/5 \cdot 5 = 1$ but $1/5$ isn't an integer. However $3 \cdot 5 \equiv 1 \pmod{7}$ so five does have an inverse modulo seven.

A number a^{-1} is called the *inverse of a modulo m* if and only if $aa^{-1} \equiv 1 \pmod{m}$. Sometimes this exists, for example $5^{-1} = 5 \pmod{3}$ since $5 \cdot 5 = 25 \equiv 1 \pmod{3}$, sometimes they don't exist; for example, consider four modulo six; $2 \cdot 4 = 8 \equiv 2 \pmod{6}$, $3 \cdot 4 = 12 \equiv 0 \pmod{6}$, $4^2 = 16 \equiv 4 \pmod{6}$ and $5 \cdot 4 = 20 \equiv 2 \pmod{6}$, and that exhausts all possible inverses. In fact if a and m have a common factor then a has no inverse modulo m; if $ab \equiv 1 \pmod{m}$ then $m|(ab - 1)$ but if $(a, m) = d$ then $d|m$ then $d|(ab - 1)$. Now $d|a$ so $d|1$ which only happens if $d = 1$. In fact, there is a stronger result

Theorem. An integer a is invertible modulo m if and only if $(a, m) = 1$.

Proof: If a has an inverse a^{-1} then $aa^{-1} \equiv 1 \pmod{m}$, so $aa^{-1} - 1 = km$ for some k. This implies the greatest common divisor $(a, m)|1$ because it divides the other two terms, hence $(a, m) = 1$. Conversely, if $(a, m) = 1$ then there exist x and y such that $ax + my = 1$, hence $ax \equiv 1 \pmod{m}$ and $a^{-1} = x$ is the inverse.□.

It can also be proved that if there is an inverse it is unique, so if $ax \equiv 1 \pmod{m}$ and $ay \equiv 1 \pmod{m}$ then $x \equiv y \pmod{m}$. The proof of the theorem above also shows how a modular inverse might be calculated: by using the Euclid algorithm to express $(a, m) = 1$ in the form $(a, m) = xa + ym$. Take, for example, the problem of finding $11^{-1} \pmod{31}$. Now, we know $(31, 11) = 1$, this follows trivially from the primality of 31 and 11, but applying the Euclid algorithm will give us x and y so that $1 = 31x + 11y$. So

$$31 = 2 \cdot 11 + 9 \tag{1}$$

and

$$11 = 9 + 2 \tag{2}$$

and

$$9 = 4 \cdot 2 + 1 \tag{3}$$

so following this backwards we have

$$1 = 9 - 4 \cdot 2 = 9 - 4 \cdot (11 - 9) = 5 \cdot 9 - 4 \cdot 11 \tag{4}$$

and so

$$1 = 5 \cdot 9 - 4 \cdot 11 = 5 \cdot (31 - 2 \cdot 11) - 4 \cdot 11 = 5 \cdot 31 - 14 \cdot 11 \tag{5}$$

Hence $1 = 5 \cdot 31 - 14 \cdot 11$ and, since $5 \cdot 31 \equiv 0 \pmod{31}$ this means $11^{-1} \equiv -14 \equiv 17 \pmod{31}$.