Discrete Math 37110 - Class 4 (2016-10-06)

Instructor: László Babai
Notes taken by Jacob Burroughs
Revised by instructor

4.1 Division vs. congruences

DO 4.1. If $m \mid ab$ and $\gcd(a, m) = 1$, then $m \mid b$

DO 4.2. If $\gcd(a, m) = 1$, then $\gcd(m, ab) = \gcd(m, b)$

DO 4.3. If $d \mid m$ and $a \equiv b \pmod{m}$ then $a \equiv b \pmod{d}$. (Uses transitivity of divisibility)

Example 4.4. If $a \equiv b \pmod{75}$ then $a \equiv b \pmod{5}$

DO 4.5. $a \equiv b \pmod{m} \implies ac \equiv bc \pmod{mc}$

The converse of this also holds.

DO 4.6. If $c \mid a, b, m$ and $a \equiv b \pmod{m}$, then $\frac{a}{c} \equiv \frac{b}{c} \pmod{\frac{m}{c}}$, assuming $c \neq 0$.

We have seen that $a \equiv b \pmod{m} \implies ac \equiv bc \pmod{m}$. The converse of this statement is false. For example, $2 \equiv 4 \mod 2$, but, dividing both sides with 2 we do not get a congruence: $1 \not\equiv 2 \mod 2$. However, the converse does hold under an additional assumption.

DO 4.7. Suppose $c \mid a$, $c \mid b$, $a \equiv b \pmod{m}$, and c, m are relatively prime. Then $\frac{a}{c} \equiv \frac{b}{c} \pmod{m}$.

Here is a stronger version of this statement.

DO 4.8. Suppose $c \mid a$, $c \mid b$, $c \neq 0$ and $a \equiv b \pmod{m}$. Then $\frac{a}{c} \equiv \frac{b}{c} \pmod{\frac{m}{d}}$ where $d = \gcd(c, m)$

4.2 Linear congruences

Definition 4.9. x is a *multiplicative inverse* of $a \mod m$ if $ax \equiv 1 \pmod{m}$

Proposition 4.10. *If there exists an inverse of* $a \pmod{m}$ *then the inverses form a residue class* mod$m$. *In other words, if* x_0 *is an inverse then* $(\forall x)(x$ *is an inverse* $\iff x \equiv x_0 \pmod{m})$.

Corollary 4.11. *The multiplicative inverse is unique* mod$m$. *This means that any two inverses must be congruent* $\mod m$.

Proof of Prop. 4.10.

$$\begin{aligned} ax \equiv 1 \pmod{m} &\iff ax \equiv ax_0 \pmod{m} \\ &\iff m \mid ax - ax_0 = a(x - x_0) \\ &\iff m \mid x - x_0 \quad (\text{because } \gcd(a, m) = 1) \\ &\iff x \equiv x_0 \mod m \end{aligned}$$

□

Proposition 4.12 (Linear congruence)**.** *Given a, b, m, a solution to $ax \equiv b \pmod{m}$ exists if and only if $\gcd(a, m) \mid b$.*

Proof of necessity. Let $d = \gcd(a, m)$. Then $ax \equiv b \pmod{m} \implies$
$ax \equiv b \pmod{d}$, and thus $0 \equiv b \pmod{d}$ since $a \equiv 0 \pmod{d}$. So $d \mid b$. □

DO 4.13. The sufficiency is left as an exercise. We assume $d \mid b$, and want to show that $\exists x$ such that $ax \equiv b \pmod{m}$.
Hint. Prove that this statement is equivalent to Bézout's lemma.

HW 4.14. Show that if $ax \equiv b \pmod{m}$ is solvable then the solutions form a residue class modulo $\frac{m}{d}$. What this means is the following. Suppose $ax_0 \equiv b \pmod{m}$. Then $(\forall x)(ax \equiv b \pmod{m}) \iff \left(x \equiv x_0 \pmod{\frac{m}{d}}\right)$, where $d = \gcd(a, m)$.

Remark. It follows that the solution is unique modulo m/d, i.e., every pair of solutions is congruent modulo m/d.

Method 4.15. We want to solve $ax \equiv b \pmod{m}$, assuming $d \mid b$ where $d = \gcd(a, m) \neq 0$. We can transform this into $\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{m}{d}$, in which case the coefficient and the modulus are relatively prime ($\gcd(a', m') = 1$, where $a' = a/d$ and $m' = m/d$). Let $b' = b/d$. Then $x = (a')^{-1}b' \pmod{m'}$ works; or we can directly use a method analogous to finding the multiplicative inverse.

4.3 Systems of simultaneous congruences

Definition 4.16. A system of simultaneous congruences is a set of congruences which must be satisfied simultaneously.

DO 4.17. Consider the following system of simultaneous congruences.

$$\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ a_2 x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ a_k x &\equiv b_k \pmod{m_k} \end{aligned}$$

Prove: If each separate congruence is solvable and $(\forall i)(m_i \neq 0)$ then the system is equivalent to a system of the following form:

$$\begin{aligned} x &\equiv b'_1 \pmod{m'_1} \\ x &\equiv b'_2 \pmod{m'_2} \\ &\vdots \\ x &\equiv b'_k \pmod{m'_k} \end{aligned}$$

where $m'_i = m_i / \gcd(a_i, m_i)$. Determine the value of b'_i. (Two systems are *equivalent* if they have the same set of solutions.)

So we only need to deal with the case when each coefficient is 1.

Theorem 4.18. *Consider the following system of simultaneous congruences.*

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

If this system has a solution then the solution is unique modulo $\operatorname{lcm}(m_1, m_2, \ldots, m_k)$.

Proof. Suppose x_0 is a solution. Then x is a solution if and only if $(\forall i)(x \equiv x_0 \pmod{m_i})$, or equivalently, $x \equiv x_0 \mod \operatorname{lcm}(m_1, m_2, \ldots, m_k)$ □

DO 4.19. Show that $e_1 \mid a$ and $\ldots$ and $e_k \mid a$ if and only if $\operatorname{lcm}(e_1, \ldots, e_k) \mid a$

Example 4.20. A system with no solution:

$$\begin{aligned} x &\equiv 0 \pmod{2} \\ x &\equiv 1 \pmod{2} \end{aligned}$$

DO 4.21. Show that the system

$$\begin{aligned} x &\equiv 4 \pmod{75} \\ x &\equiv 17 \pmod{210} \end{aligned}$$

has no solution.
Hint: look at each congruence modulo 5.

Theorem 4.22. *The system*

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

is solvable if and only if $a_1 \equiv a_2 \pmod{d}$ *where* $d = \gcd(m_1, m_2)$.

Proof of necessity. $x \equiv a_i \pmod{m_i} \implies x \equiv a_i \pmod{d} \implies a_1 \equiv x \equiv a_2 \pmod{d}$ □

XC 4.23. Show that the condition is also sufficent: if $a_1 \equiv a_2 \pmod{d}$ then the system of congruences given in Theorem 4.22 has a solution.

Theorem 4.24 (Chinese Remainder Theorem (CRT))**.** *If* $(\forall i \neq j)(\gcd(m_i, m_j) = 1)$*, then*

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ &\vdots \\ x &\equiv c_k \pmod{m_k} \end{aligned}$$

has a solution.

DO 4.25. Prove that under the assumptions of the CRT, the solutions form a residue class modulo $m_1 \dots m_k$. In particular, the solution is unique modulo $m_1 \dots m_k$.

DO 4.26. Let $M = m_1 \cdots m_k$, and $P_i = \frac{M}{m_i} = \prod_{j \neq i} m_j$.
Show that $(\forall j)(\gcd(P_j, m_j) = 1)$.

Proof of CRT. Try to find x in the form $x = \sum_{i=1}^{k} x_i P_i$. Now x is a solution if and only if $\sum_{i=1}^{k} x_i P_i \equiv c_j \pmod{m_j}$ for each j. Let us note that $P_i \equiv 0 \pmod{m_j}$ if $i \neq j$. The above sum thus reduces to $x_j P_j \equiv c_j \pmod{m_j}$ (separation of the variables). So to solve our original system of simultaneous congruences, we just need to solve each congruence $x_j P_j \equiv c_j \pmod{m_j}$ separately. But this congruence is solvable because $\gcd(P_j, m_j) = 1$. □

CH 4.27. The system $x \equiv a_i \pmod{m_i}$ $(i = 1, \dots, k)$ is solvable if and only if every pair of congruences is solvable, i. e., $(\forall i \neq j)(a_i \equiv a_j \mod \gcd(m_i, m_j))$.

Note that there may be questions that ask us to use the CRT to solve them; don't use this instead.

4.4 GCD of a set of integers

Definition 4.28 (Greatest common divisior of a set of numbers)**.** Let $S \subseteq \mathbb{Z}$. We say that d is a gcd of S if d is a common divisor (i.e., $(\forall s \in S)(d \mid s)$) and d is a multiple of all common divisors (i.e., $(\forall e)$(if $(\forall s \in S)(e \mid s)$ then $e \mid d$))

Note that in this definition, S is permitted to be an infinite set, or the empty set.

DO 4.29. Find a, b, c such that $\gcd(a, b, c) = 1$ but $\gcd(a, b) \neq 1$ and $\gcd(a, c) \neq 1$ and $\gcd(b, c) \neq 1$.

DO 4.30. Show that the gcd exists and "Bézout's Lemma" holds: the gcd can be written in the form

$$\gcd = \sum_{s_i \in S} x_i s_i$$

Here the sum must be finite even if S is infinite; in other words, all but a finite number of the coefficients x_i must be zero.

DO 4.31. (a) What is $\gcd(\emptyset)$? (b) What is $\gcd(\mathbb{Z})$?

DO 4.32. Prove: $\text{lcm}(a, b)$ is the gcd of all common multiples of a and b. (Note: this is an infinite set.)

DO 4.33. Using the notation from the proof of CRT above, prove that $\gcd(P_1, \ldots, P_k) = 1$.

DO 4.34 (No-risk strategy)**.** In the proof of CRT, we were looking for solutions of a particular form, namely, linear combinations of the P_i. Prove that there was no risk to this approach: every integer can be written as a linear combination of the P_i.

4.5 Reducing composite moduli to prime power moduli

DO 4.35. Prove: $a \equiv b \pmod{600} \iff$ the following congruences hold simultaneously.

$$\begin{aligned} a &\equiv b \pmod 8 \\ a &\equiv b \pmod 3 \\ a &\equiv b \pmod{25} \end{aligned}$$

DO 4.36. Let $m = \prod p_i^{k_i}$ be the prime factorization of m (the p_i are distinct primes). Then $a \equiv b \pmod m \iff (\forall i)(a \equiv b \pmod{p_i^{k_i}})$.

Example 4.37. Consider the quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{600}.$$

This is equivalent to the following set of simultaneous congruences.

$$\begin{aligned} ax^2 + bx + c &\equiv 0 \pmod 8 \\ ax^2 + bx + c &\equiv 0 \pmod 3 \\ ax^2 + bx + c &\equiv 0 \pmod{25} \end{aligned}$$

If we have a way of handling such congruences modulo 8, 3, and 2 (and modulo prime powers in general) then the solutions can then be combined using the CRT to obtain the solutions modulo 600.

HW 4.38. Given a prime p, prove that

$$x^2 \equiv 1 \pmod p \iff x \equiv \pm 1 \pmod p$$

Clearly state, exactly what property of p you are using.

XC 4.39. Given a pair of distinct odd primes, $p \neq q$, prove that

$$x^2 \equiv 1 \pmod{pq} \not\Longrightarrow x \equiv \pm 1 \pmod{pq}$$

Warning: you have to show that this inference is false for every pair (p, q) of distinct odd primes. Giving a counterexample for a particular pair such as $(3, 5)$ will not do.

Note: This problem was previously erroneously posted as "HW." It was meant to be "XC."

4.6 An amusing exercise: decimal is special!

The instructor's mother, a grade school teacher, tried to teach her slow-witted son the multiplication table. I had especially great difficulty remembering $7 \cdot 8$. Mother noticed the following helpful mnemonic.

$$56 = 7 \cdot 8.$$

Are there other entries in the multiplication table that obey a similar rule? Sure,

$$12 = 3 \cdot 4.$$

AMUX 4.40 (Instructor's mother's rule)**.** Show that the instructor's mother's rule occurs in the decimal system only. In other words, consider four consecutive digits, $k, \ldots, k+3$, in base b. So $0 \leq k \leq b-4$. Now if $(k+2)(k+3)$ is the two-digit number $\overline{k\ (k+1)}_b$, i.e., $(k+2)(k+3) = bk + (k+1)$, then $b = 10$ and $k = 1$ or 5.

(Enjoy this exercise, do not hand it in.)