• Basics of congruences (continued)
  – Do you know how congruences behave when we do division? Do you know when “cancel- 
cellation” is allowed? Can you make use of these properties of congruences to help 
make calculation of least residues simpler?
  – Suggested problems:
    1. Prove that 17 does not divide $5n^2 + 15$ for any integer $n$.
    2. If $n$ is an integer not divisible by 2 or 3, show that $n^2 \equiv 1 \pmod{24}$.

• Finding the day of the week
  – Given the day and the month of a particular year, can you find out which day of the 
week it is? (You will be given the month table in exams.)
  – Suggested problems: Pick any date after 1752. You can check your answer online – 
there are many websites that have the day of the week calculator, just do a google 
search.

• The theorems of Fermat and Euler
  – What does Fermat’s Little theorem say?
  – Can you state the definition of the Euler $\phi$-function? Given an integer $m$, do you know 
what $\phi(m)$ is? How can prime factorization help?
  – What is the definition of a reduced residue system modulo $m$? How many elements are 
there in a reduced residue system? Can you give a few examples of reduced residue 
systems modulo $m$?
  – Euler generalized Fermat’s Little theorem. What does his result say?
  – Do you know how to use the theorems of Fermat and Euler to help simplify calculations 
of least residues?
  – Suggested problems:
    1. Find a reduced residue system modulo 7 composed entirely of multiplies of 3.
    2. Show that the numbers 5, $5^2$, $5^3$, $5^4$, $5^5$, $5^6$ form a reduced residue system modulo 
18.
    3. If $p$ is an odd prime and $p \not| a$, show that $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$.
    4. Give an example to show that the result of the above exercise is not necessarily 
true if $p$ is replaced by an arbitrary positive $n$ with $\gcd(a, n) = 1$.
    5. If $p$ and $q$ are distinct primes, prove that $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

• Linear congruences
  – What is a linear congruence? What do we mean by a solution to a linear congruence?
  Given the linear congruence $ax \equiv b \pmod{m}$ and an integer $x'$, do you know how to 
check whether $x'$ is a solution to the given congruence?
  – What is the relationship between linear congruence and linear Diophantine equation?
  – What is the criterion for a linear congruence to have solution(s)? If it is solvable, how 
many incongruent solutions are there?
  – There are multiple ways to find one solution to a linear congruence. For example, trial-
and-error, Euclidean algorithm, multiplying and simplifying trick, and Euler’s Theorem.
  – What is the definition of a multiplicative inverse of $a$ modulo $m$? Does every integer 
have an inverse modulo $m$? Can an integer has two inverses modulo $m$? If $a$ has an 
inverse modulo $m$, do you know how to find it?
  – Can you state Wilson’s Theorem? Are you familiar with how to use Wilson’s Theorem?
  – Suggested problems:
    1. Solve the following linear congruences:
       (i) $25x \equiv 4 \pmod{11}$
(ii) \(15x \equiv 3 \pmod{9}\)
(iii) \(34x \equiv 60 \pmod{98}\)
(iv) \(35x \equiv 15 \pmod{182}\)

2. Use Euler’s Theorem to solve \(77x \equiv 28 \pmod{36}\) and \(77x \equiv 14 \pmod{105}\).

- Application: Cryptography
  - Do you know what a Caesar cipher is? A generalized Caesar cipher? Is there any constraint on the multiplier or shift constant for a generalized Caesar cipher?
  - Do you know how to encrypt and decrypt messages with a (generalized) Caesar cipher?
  - Can you break a cipher?
  - Suggested problems: See lecture notes on cryptography.

- Chinese Remainder Theorem
  - What does the Chinese Remainder Theorem say?
  - Do you know how to use the Chinese Remainder Theorem to solve a (system) of linear congruence(s)?
  - Suggested problems:
    1. Find the least positive integer that leaves remainders of 2, 3 and 2 when divided by 3, 5 and 7 respectively.
    2. Find the integer \(x\) such that \(-2310 \leq x \leq 2310\) and
       \[
       x \equiv 1 \pmod{21},
       x \equiv 2 \pmod{20},
       x \equiv 3 \pmod{11}.
       \]
    3. Find the solution to the system
       \[
       3x \equiv 7 \pmod{5},
       x \equiv 1 \pmod{4},
       5x \equiv 2 \pmod{11}.
       \]