Discrete Mathematics, Section 001, Fall 2016

Lecture 20: Chinese remainder theorem, Factoring

Zsolt Pajor-Gyulai
zsolt@cims.nyu.edu

Courant Institute of Mathematical Sciences

November 30, 2016

Outline

Solving two equations

We have seen how to solve one congruence and noted that there were an infinite number of solutions. Now we want to solve two congruences simultaneously.

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

We start with the example

$$x \equiv 1 \pmod{7}$$
$$x \equiv 4 \pmod{11}$$

Our task is to find all integers x that satisfies both equations.

Solving two equations

We start with the example

$$x \equiv 1 \pmod 7$$
$$x \equiv 4 \pmod{11}$$

By the first congruence, there is an integer k, such that

$$1 + 7k = x \equiv 4 \pmod{11} \qquad \Rightarrow \qquad 7k \equiv 3 \pmod{11}$$

We reduced it to a single equation!

Solution (Problem 1 on WS):

$$k = 2 + 11j, \qquad j \in \mathbb{Z},$$

and therefore

$$x = 1 + 7(2 + 11j) = 15 + 77j, \qquad j \in \mathbb{Z}.$$

Chinese remainder theorem

The pair of congruences where $gcd(m, n) = 1$,

$$x \equiv x_1 \pmod{m}, \qquad x \equiv x_2 \pmod{n}$$

has a unique solution x_0 with $0 \leq x_0 < mn$. Furthermore, every mutual solution to these congruences differs from x_0 by a multiple of mn.

WLOG assume $m < n$. From $x \equiv x_1 \pmod{m}$, we have $x = x_1 + km$ where $k \in \mathbb{Z}$. Plugging this into the other equation

$$x_1 + km \equiv x_2 \pmod{n} \qquad \rightarrow \qquad km \equiv x_2 - x_1 \pmod{\mathrm{n}}$$

Note that adding or subtracting a multiple of n from either side does not change this equation and therefore let

$$c = x_2 - x_1 \bmod n.$$

This yields the equation $km \equiv c \pmod{n}$ which is also

$$(k \bmod n) \otimes m = c, \qquad \text{in } \mathbb{Z}_n$$

[...]

Chinese remainder theorem

The pair of congruences

$$x \equiv x_1 \pmod{m}, \qquad x \equiv x_2 \pmod{n}$$

has a unique solution x_0 with $0 \leq x_0 < mn$. Furthermore, every mutual solution to these congruences differs from x_0 by a multiple of mn.

[...]

$$(k \bmod n) \otimes m = c, \qquad \text{in } \mathbb{Z}_n$$

Since $gcd(m, n) = 1$, m has a reciprocal m^{-1} in $\mathbb{Z}_n$. Then

$$(k \bmod n) = c \otimes m^{-1} =: d, \qquad \text{in } \mathbb{Z}_n.$$

This can be written as

$$k = d + jn, \qquad \text{for some } j \in \mathbb{Z}.$$

[...]

Chinese remainder theorem

The pair of congruences

$$x \equiv x_1 \pmod{m}, \qquad x \equiv x_2 \pmod{n}$$

has a unique solution x_0 with $0 \leq x_0 < mn$. Furthermore, every mutual solution to these congruences differs from x_0 by a multiple of mn.

[...]

$$k = d + jn, \qquad \text{for some } j \in \mathbb{Z}.$$

Plugging this back into $x = x_1 + km$, we get

$$x = x_1 + (d + jn)m = x_1 + dm + jnm$$

from which

$$x_0 = x_1 + dm \bmod nm$$

with $d = ((x_2 - x_1) \bmod n) \otimes m^{-1}$ where the reciprocal is taken in $\mathbb{Z}_n$.

Outline

1. Chinese remainder theorem
2. Factoring
3. Applications of the factorization theorem

Fundamental theorem of arithmetics

Theorem

Let n be a positive integer. Then n factors into a product of primes. Furthermore, this factorization is unique up to the order of the primes

In other words, for every positive integer n, there is $l \in \mathbb{N}$ and primes $p_1, \ldots, p_l$, such that

$$n = \prod_{i=1}^{l} p_i$$

and the only ambiguity lies in reidexing the p_i.

Believing this is true, do Problem 3 on the worksheet!

Auxilliary lemma 1

Lemma

Suppose $a, b, p \in \mathbb{Z}$ and p is a prime. If $p|ab$, then $p|a$ or $p|b$.

Proof

Suppose for the sake of contradiction that there are integers a, b, p such that $p|ab$ but p divides neither a nor b.

Since p is a prime, its only divisors are $\pm 1, \pm p$. We also know $p \nmid a$, and thus $gcd(a, p) = 1$. Similarly, $gcd(b, p) = 1$.

By two lectures before,

$$ax + py = 1, \qquad bz + pw = 1$$

for some integers x, y, z, w.
[...]

Auxiliary Lemma 1

Lemma

Suppose $a, b, p \in \mathbb{Z}$ and p is a prime. If $p|ab$, then $p|a$ or $p|b$.

Proof

[...]

By two lectures before,

$$ax + py = 1, \qquad bz + pw = 1$$

for some integers x, y, z, w. Multiplying these equations, we get

$$1 = (ax + py)(bz + pw) = abxz + pybz + paxw + p^2yw.$$

Since $p|ab$, all four terms are divisible by p and thus $p|1$.

$\Rightarrow\Leftarrow$ $\square$

Auxiliary Lemma 2

Lemma

Suppoese $p, q_1, \ldots, q_t$ are prime numbers. If

$$p|(q_1 \ldots q_t),$$

then $p = q_i$ for some $1 \leq i \leq t$.

Proof

We prove this by induction on t.

The base case $t = 1$ is clear as if $p|q_1$ then since p and q_1 are primes, $p = q_1$.

Suppose this is true for $t = k$ and consider $p|(q_1 \ldots q_k q_{k+1})$. Let

$$a = q_1 \ldots q_k, \qquad b = q_{k+1}$$

Then $p|ab$ and by the previous lemma, either $p|a$ or $p|b$.

[...]

Auxiliary Lemma 2

Lemma

Suppoese $p, q_1, \dots, q_t$ are prime numbers. If

$$p|(q_1 \dots q_t),$$

then $p = q_i$ for some $1 \leq i \leq t$.

Proof

[...]

$$a = q_1 \dots q_k, \qquad b = q_{k+1}$$

Then $p|ab$ and by the previous lemma, either $p|a$ or $p|b$.

- If $p|a = q_1 \dots q_k$, then by the induction hypothesis, $p = q_i$ for some $1 \leq i \leq t$.
- If $p|b = q_{k+1}$ then $p = q_{k+1}$ as before.

In either case, the result is proven for $t = k + 1$ and therefore by induction the result holds for all t. □

Proof of existence of factorization

Suppose for the sake of contradiction, that not all positive integers factor into primes and let X be the set of these numbers.

- $1 = \prod_{i=1}^{0} p_i$ (empty product) and so $1 \notin X$.
- If p is a prime itself, then $p \notin X$.

By the WOP, let x be the least element of X. We have $x \neq 1$ and that x is not a prime. Therefore x is composite.

This means that there is an $a \in \mathbb{Z}$ with $1 < a < x$ such that $a|x$. Then there is a $b \in \mathbb{Z}$ such that $ab = x$ and clearly, $1 < b < x$.

Sice $a < x$ and $b < x$, they have a factorization, let's say given by

$$a = p_1 \dots p_s, \qquad b = q_1 \dots q_t$$

Then

$$x = ab = p_1 \dots p_s q_1 \dots q_t$$

is a factorization of x contradicting $x \in X$.$\Rightarrow\Leftarrow$.

Proof of Uniqueness of factorization

Suppose for the sake of contradiction that some positive integer can be factored into primes in two distinct ways and let Y be the set of these numbers.

- $1 \notin Y$ as the empty product is the only representation.

By the WOP, let y be the least element of Y. Thus y can be factored into primes in two distinct ways:

$$y = p_1 p_2 \dots p_s, \qquad y = q_1 q_2 \dots q_t$$

Note that $p_1 | y = q_1 q_2 \dots q_t$ and therefore by Aux Lemma 2, $p_1 = q_j$ for some j. Then

$$\frac{y}{p_1} = p_2 \dots p_j, \qquad \frac{y}{p_1} = \prod_{\substack{i=1 \\ i \neq j}}^{t} q_j.$$

But $\frac{y}{p_1} < y$ and it has two distinct factorization which contradict y being the smallest element of Y.$\Rightarrow\Leftarrow$.

Outline

Infinitely many primes

Theorem

There are infinitely many prime numbers

FTSC, assume that there are finitely many primes:

$$2, 3, 5, 7, \ldots, p.$$

Let $n = (2 \cdot 3 \cdot 5 \cdot \cdots \cdot p) + 1$.

- Is n a prime? Clearly, $n > p$ and therefore it is not, so n is composite.
- Let q be any prime and note

$$n = (2 \cdot 3 \cdot \cdots \cdot q \cdot \cdots \cdot p) + 1.$$

Then $n \bmod q = 1$ and $q \nmid n$. Since the choice of the prime q was arbitrary, there is no prime factorization of n.

$\Rightarrow\Leftarrow$

Formula for greatest common divisor

Theorem

Let *a* and *b* be positive integers with

$$a = 2^{e_2} \cdot 3^{e_3} \cdot 5^{e_2} \cdot 7^{e_7} \ldots, \qquad b = 2^{f_2} \cdot 3^{f_3} \cdot 5^{f_5} \cdot 7^{f_7} \cdot \ldots,$$

where e_i-s are naturals (possibly zero). Then

$$gcd(a, b) = 2^{min(e_2, f_2)} \cdot 3^{min(e_3, f_3)} \cdot 5^{min(e_5, f_5)} \cdot 7^{min(e_7, f_7)} \cdot \ldots$$

For example, if $a = 24$, $b = 30$,

$$24 = 2^3 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdot \ldots, \qquad 30 = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot \ldots$$

and

$$gcd(24, 30) = 2^1 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdot \cdots = 6.$$

Do Problem 4 on the worksheet!

Irrationality of $\sqrt{2}$

Do Problem 6 on the worksheet first!

Proposition

There is no rational number x such that $x^2 = 2$.

FTSC, suppose that there is a rational number $x = \frac{a}{b}$ where a and b are integers, such that $x^2 = 2$.
This implies $\left(\frac{a}{b}\right)^2 = 2$ which in turn implies $a^2 = 2b^2$. Consider the prime factorization of $n = a^2 = 2b^2$.

- 2 must appear in the factorization of $n = a^2$ an even number of times.
- 2 must appear in the factorization of $n = 2b^2$ an odd number of times.

$\Rightarrow\Leftarrow$ $\square$