Lecture 2

Congruence equation

Solve for $2x \equiv 3 \mod 5$

Trial & Error:

$x \equiv 0 \mod 5$, $2x \equiv 0 \mod 5$

$x \equiv 1 \mod 5$, $2x \equiv 2 \mod 5$

$x \equiv 3 \mod 5$, $2x \equiv 1 \mod 5$

$x \equiv 4 \mod 5$, $2x \equiv 3 \mod 5$

Tedious !

In this case, one can do

$$x = [3]_5 \times [2]_5^{-1},$$

but this is not possible when 5 is replaced by a non-prime number

Prob 3: $a, n \in \mathbb{N}$ & $d \in \mathbb{Z}$. The equation $ax \equiv d \mod n$ is solvable iff $GCD(a, n) \mid d$.

Ex: The previous example: $GCD(2,5) = 1$ & $1 \mid 3$.

Proof

Let $\exists x$ s.t.

$$ax \equiv d \mod n$$

$\Leftrightarrow n \mid ax - d \Leftrightarrow \exists q \in \mathbb{Z}$

s.t. $ax + qn = d$.

$\Leftrightarrow GCD(a, n) \mid d$.

Prop 2
last week

Ex: Solve $6x \equiv 5 \mod 4$.

Not solvable as $GCD(6,4) = 2 \nmid 5$

Ex: Solve $6x \equiv 2 \mod 4$.

solvable as $gcd(6, 4) = 2 \mid 4$.

To find the solution we need to find q s.t. $6x + 4q = 2$

$\Leftrightarrow 3x + 2q = 1 \Leftrightarrow 3x \equiv 1 \mod 2$

$\Rightarrow x = [3]_2^{-1} = 1$.

The Chinese Remainder theorem

What about a system of congruence equation? e.g. $5x \equiv 3 \mod 9$

$6x \equiv 5 \mod 7$

what's the general way to determine whether the above system is solvable

Theorem (CRT for 2 equations)

Let $GCD(m, n) = 1$. Then there is a solution to $a, b \in \mathbb{Z}$

$x \equiv a \mod m$

$x \equiv b \mod n$

The solution is unique mod mn.

Proof: (Constructive proof)

As $GCD(m, n) = 1$, $\exists\ r, s$ s.t.

$mr + ns = 1$

Note that $mr \equiv 1 \mod n$

$ns \equiv 1 \mod m$

Let $x = mr\ell + nsa$. Then

$$x \equiv nsa \mod m$$
$$\equiv 1 \cdot a \equiv a \mod m$$

similarly, $x \equiv b \mod n$.

To check uniqueness, let x & y are solutions to the above system.

Then $\left.\begin{array}{l} x \equiv a \mod m \\ y \equiv a \mod m \end{array}\right\} \Rightarrow x \equiv y \mod m$

$\Downarrow$

$m \mid x-y$

similarly, $n \mid x-y$.

Using the following exercise we check that $mn \mid x-y$ as $GCD(m,n)=1$

$\Rightarrow x \equiv y \mod mn$

Exercise: Let $GCD(m,n) = 1$ and $a \in \mathbb{Z}$. If $m \mid a$ & $n \mid a$, then $mn \mid a$

Hint: Use fundamental theorem of arithmetic.

More generally, we have

Theorem (Non-examinable proof)

Let $n_1, n_2, \ldots, n_r \in \mathbb{N}$ s.t.

$\text{GCD}(n_i, n_j) = 1 \quad \forall\ 1 \le i \ne j \le r.$

Let $a_i \in \mathbb{Z}$. Then $\exists\ x$ unique up to modulo $n_1 \times \cdots \times n_r$ s.t.

$$x \equiv a_i \mod n_i.$$

Non ad-hoc:

$$\left.\begin{aligned} x &\equiv a \mod m \\ x &\equiv b \mod n \end{aligned}\right\} \text{re-write}$$

$q_1, q_2 \in \mathbb{Z}$,

$$x = a + q_1 m = b + q_2 n$$

$$q_1 m - q_2 n = b - a$$

solvable as $\text{GCD}(m, n) = 1 \mid b - a$

Not always true if $\text{GCD}(m,n)$ is not 1.

$$x \equiv 2 \mod 4 \quad \text{has no sol}^n.$$
$$x \equiv 3 \mod 6$$

If $4 \mid x - 2 \Rightarrow x = 2 + 4q_1 \Rightarrow x$ is even

If $6 \mid x-3 \Rightarrow x = 3 + 6q_2 \Rightarrow x$ is odd.

Exercise : Solve

$$x \equiv 1 \mod 2$$
$$x \equiv 4 \mod 5$$
$$x \equiv -2 \mod 7$$

CRT for first two eq^{n}s. :

$$2 \times 3 + (-1) \times 5 = 1$$

So $x = 2 \times 3 \times 4 + (-1) \times 5 \times 1$

$= 24 - 5 = 19$

Any $x \equiv 19$ satisfies first two eq^{n}s.

For the third evaluation we solve

$$x \equiv 19 \mod 10$$
$$x \equiv -2 \mod 7$$

We have $10 \times (-2) + 7 \times 3 = 1$

So $x = 10 \times (-2) \times (-2) + 7 \times 3 \times 19$

$= 40 + 399 = 439.$

Theorem: $\exists$ infinitely many prime numbers $p \equiv -1 \mod 4$

Pf: Let $\exists$ finitely many $p_1, \ldots, p_k$ that are $\equiv -1 \mod 4$.

Consider $N = 4 p_1 \times \cdots \times p_k - 1$

Note: 1) $N \equiv -1 \mod 4 \Rightarrow 2 \nmid N$

2) $p_i \nmid N \quad \forall\ 1 \le i \le k$

So if N is a prime then we arrive at a contradiction.

Let N be not a prime. By FTA

$N = q_1 \times \cdots \times q_n$, q_i prime.

By the above q_i must be $\equiv 1 \mod 4$

as $q_i \nmid 2 \Rightarrow$ odd

$q_i \not\equiv -1 \mod 4$

But then $N \equiv 1 \mod 4$. Contradiction.

Remark: Try to prove similarly that $\exists$ infinitely many prime $\equiv 1 \mod 4$.

Digression (Non-exam)

1) One needs deep mathematics (complex analysis) to see that $\exists$ infinitely many primes of the form $p \equiv a \bmod q$ with $\gcd(a, q) = 1$.

Google : Dirichlet theorem on primes in arithmetic progression

2) $\exists$ infinitely many primes.

$$\#\{p : p \le x\} \approx \frac{x}{\log x}$$

OTOH there is slight bias in the counts

$$\#\{p \le x : p \equiv 1 \bmod 4\}$$

$$\#\{p \le x : p \equiv -1 \bmod 4\}$$

Difference of the above $\approx \frac{\sqrt{x}}{\log x} \log\log\log x$

Exercise

The goal is to show that $\exists$ infinitely many primes that are $(-1) \bmod 4$

1) Assume p_i, for $1 \le i \le k$, are primes s.t. $p_i \equiv -1 \bmod 4$

Let $N = 4 p_1 \times p_2 \times \cdots \times p_k - 1$

show that if p is a prime factor of N then $p \equiv 1 \bmod 4$

2) Assume $\exists$ only finitely many primes that are $\equiv -1 \bmod 4$. Using (1) arrive at a contradiction

3) Can you prove similarly that there are infinitely many primes $\equiv 1 \bmod 4$?

4) Use the same argument to prove there are infinite by many primes, but not using (2).