Modular Arithmetic

$a \equiv b \mod n \iff n \mid a-b.$

Div. algorithm says for any $a \in \mathbb{Z}$, $\exists q, r$ w/ $a = nq + r$, $0 \leq r \leq n-1$.

So $a \equiv 0, 1, \ldots, n-1 \mod n$ are the only possibilities

These correspond to sets

$$\{\ldots, -n, 0, n, 2n, \ldots\} = [0]$$

$$\{\ldots, -n+1, 1, n+1, 2n+1, \ldots\} = [1]$$

$$\vdots \qquad\qquad \vdots$$

$$\{\ldots, -2n+1, n-1, 2n-1, \ldots\} = [n-1]$$

Congruence Classes mod n

$$\mathbb{Z}/n\mathbb{Z} = \{[0], \ldots, [n-1]\}$$

Modular arithmetic has all the properties you would want:

$a \equiv b \mod n \qquad c \equiv d \mod n$

$$a + c \equiv b + d \mod n$$
$$ac \equiv bd \mod n$$

Linear equations mod n:

$$ax \equiv b \mod n$$

Looking for solutions mod n to

equations like the above.

$ax \equiv b \bmod n \iff ax = b + nk$ for some k

$\iff$ Solutions to

$$ax + ny = b$$

<u>Thm:</u> $ax \equiv b \bmod n$ has a sol^n iff $(a,n) = d \mid b$.

If $x_0 \bmod n$ is one solution, then we have exactly $d-1$ solutions mod n, and they are

$$x_0 \bmod n,\ x_0 + \frac{n}{d} \bmod n,\ \dots,\ x_0 + (d-1)\frac{n}{d} \bmod n$$

<u>Cor:</u> $ax \equiv 1 \bmod n$ has a sol^n

$\Leftrightarrow (a,n) = 1$, and it has a unique sol^n.

we call the solution to $ax \equiv 1 \mod n$ the <u>inverse</u> of a mod n,

we write $a^{-1} \mod n$.

Constrast this with $\mathbb{Z}$, where

$$ax = 1 \quad \Rightarrow \quad a = x = \pm 1.$$

<u>Ex:</u> Solve $10x \equiv 34 \mod 42$

$(10, 42) = 2$. $\quad 2 \mid 34$

the theorem says that there are 2 solutions mod 42.

How to find initial solution?

$10x \equiv 34 \mod 42$

$10x = 34 + 42k$ for some k.

$5x = 17 + 21k$ for some k.

$5x + 21y = 17.$

$21 - 5 \cdot 4 = 1$

$\Rightarrow \quad 5 \cdot (-68) + 21 \cdot 17 = 17$

$\Rightarrow \quad 10 \cdot (-68) + 21 \cdot 34 = 34$

$\Rightarrow \quad 10 \cdot (-68) \equiv 34 \mod 42$

So $x_0 \equiv -68 \equiv 16 \mod 42$

is one solution, and the

other solution is

$$16 + 21 \equiv 37 \mod 42.$$

So $\quad x \equiv 16, 37 \mod 42.$

Miscellaneous Problems

Prove that none of

$1, 11, 111, 1111, \ldots$ are perfect

squares except the first term.

Proof: the n^{th} term in the

Sequence is

$a_n = \frac{10^n - 1}{9}$. If $a_n = k^2$ for some n and some k,

then $a_n \equiv k^2 \bmod 4$.

The only squares mod 4 are 0, 1.

$$\frac{10^n - 1}{9} \equiv 10^n - 1 \mod 4$$

b/c $9 \equiv 1 \bmod 4$

and $10^n - 1 \equiv -1 \equiv 3 \bmod 4$

for $n \geq 2$ b/c $4 \mid 10^n$ for $n \geq 2$.

So for $n \geq 2$,

$a_n \equiv 3 \bmod 4$, so $a_n \neq \square$.

$a_1 = 1$ is a square $\square$

Prove that $15x^2 - 7y^2 = 9$ has no integer solutions.

<u>Proof:</u>

Sufficient to find an n s.t.

$15x^2 - 7y^2 \equiv 9 \mod n$ has <u>no</u> solution.

Note that $3 \mid 15x^2$, and $3 \mid 9$

$\Rightarrow \quad 3 \mid 7y^2, \Rightarrow 3 \mid y.$

$y = 3y_1$

$15x^2 - 7 \cdot 9 y_1^2 = 9$

$9 \mid 63y_1^2$

$9 \mid 9$

$\Rightarrow 9 \mid 15x^2$

$\Rightarrow 3 \mid x.$

$x = 3x_1$

$15 \cdot 9 x_1^2 - 7 \cdot 9 y_1^2 = 9$

$15x_1^2 - 7y_1^2 = 1.$

So we've shown a soln to

$15x^2 - 7y^2 = 9$ gives a soln to

$15x^2 - 7y^2 = 1.$

Reducing mod 3,

$-7y^2 \equiv 1 \mod 3$

$$2y^2 \equiv 1 \mod 3$$

$$\Rightarrow \quad y^2 \equiv 2 \mod 3.$$

this has no sol^n, b/c only squares mod 3 are 0,1.

$\Rightarrow$ $15x^2 - 7y^2 = 1$ has no sol^n $\Rightarrow$ $15x^2 - 7y^2 = 9$ has no sol^n $\boxtimes$

Prove that no integer of the form $7+8k$ is a sum of

3 Squares.

Proof. A soln to

$x^2+y^2+z^2 = 7+8k$

gives a soln to

$x^2+y^2+z^2 \equiv 7 \mod 8$

the only squares mod 8

are 0, 1, 4.

So $x^2, y^2, z^2 \in \{0,1,4\}$.

Brute force to check that none of the 27 possibilities work