Math 312, Lecture 8

Diophantine Equations

So far, lay down foundation: the integers

Today: linear equations in \( \mathbb{Z} \)

One variable: divisibility.

Can solve \( ax = b \) iff \( a \mid b \)

What about two variables?

Eq: \( 2x + y = 7 \)

Clearly has solutions: \( \{(x, 7-2x) : x \in \mathbb{Z}\} \)

\( 2x + 2y = 7 \)

Has no solutions. (LHS is always even, RHS always odd)

Eq: \( 2x + 3y = n \) (compare 4)

Bottom line: divisibility only obstacle to solutions
Two possibilities: (i) no solution for obvious reasons

\[ ax + by = c \]

(ii) 1-parameter family of solutions.

Then: The set of integral solutions to \( ax + by = c \) is:

(i) If \( a = b = 0 \), no solutions if \( c \neq 0 \) for all \( \mathbb{Z}^2 \) if \( c = 0 \).

(ii) Else, let \( d = \gcd(a, b) \).

(a) No solutions if \( ad,c \)

(b) If \( ad,c \) there are solutions, if \( (s, t) \) are such that \( as + bt = d \) then the general solution is

\[
\left\{ \left( \frac{sc}{d} + \frac{b}{d^2}, \frac{tc}{d} - \frac{a}{d^2} \right) \mid s, t \in \mathbb{Z} \right\}
\]

\[ a \cdot \frac{sc}{d} + b \cdot \frac{tc}{d} = c \]

particular solution

one-parameter family.
1. Key mental technique is: tell yourself a story.

2. "Solve equation": (i) find some solutions (ii) show these are all solutions.

"If (x,y) is a solution then ..." 

If (x,y) on list then it's a solution = "plugging into equation".

Examples: 5x + 11y = 7

Since (5,11) = 1 so guaranteed solutions.

How to find? 5·(-2) + 11·1 = 1

Note: (guaranteed by Bezout's thm)

must be 7; set 5·(-6) + 11·7 = 7.
to get other solutions, try
5 \cdot (-14 + x) + 11 \cdot (7 - 5k) = 7

need 5 \cdot \* = 11 \cdot \*
For this to work, need 11 \mid 5 \cdot \*
5 \mid 11 \cdot \*

so must have the solutions
5 \cdot (-14 + 11k) + 11 \cdot (7 - 5k) = 7
(add & subtract 55k)

so general solution is \( \{(-14 + 11k, 7 - 5k)\} \)

warning: we used (5, 11) = 1

notation: solutions are (-14, 7) + (11, -5) \cdot X

Example: 10x + 22y = 9
(10, 22) = 2 but 2 \mid 9, so no solutions.
Example: $10x + 22y = 14$

Again $(10, 22) = 2$, now all divisors are used to divide by $2$ to get $5x + 11y = 7$.

(see above)

(if have solutions can divide by gcd throughout)

---

**Pf of Thm:** We understand equations

$$0ax + 0by = c$$

$$ax + by = c, \text{ all } c$$

$d = \gcd(a, b)$

So only need to understand case

$$ax + by = c, \text{ all } c.$$

Equivalent equations

Then divide by $d$, get:

$$\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}$$

HW: $(\frac{a}{d}, \frac{b}{d}) = 1$
so enough to solve \( ax + by = c \) 
with \( (a,b) = 1 \).

(1) Existence: by Bezout's thin have \( s, t \) s.t. \( as + bt = 1 \) 
then \( a \cdot (cs) + b \cdot (ct) = c \) 
so \( (cs, ct) \) is a particular solution 
and \( (cs + bk, ct - ak), \ b \in \mathbb{Z} \) 
is also a solution:

\[
\begin{align*}
  a \cdot (cs + bk) + b \cdot (ct - ak) \\
  = a \cdot cs + a \cdot bk + b \cdot ct - b \cdot ak \\
  = a \cdot cs + b \cdot ct = c.
\end{align*}
\]

Conversely, suppose \( (x,y) \) is a solution: \( ax + by = c \)
also \( a \cdot cs + b \cdot ct = c \)
\[ a \cdot (x - cs) + b \cdot (y - ct) = 0 \]

or
\[ a \cdot (x - cs) = b \cdot (ct - y) \]

LHS is divisible by \( a \), RHS is divisible by \( b \), \( (a, b) = 1 \), so both sides are divisible by \( ab \), say have form \( a \cdot b \cdot k \), \( k \in \mathbb{Z} \)

then
\[ a \cdot (x - cs) = a \cdot b \cdot k = b \cdot (y - ct) \]

so
\[ x = cs + bk \]
\[ y = ct - ak \]