Math 4460

2/15/23

Corollary: Let $a, b, p \in \mathbb{Z}$ where p is prime.
If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Ex: $p = 7$

$7 \mid 140$

$7 \mid (14)(10)$ — a, b

$7 \mid 14$ here but $7 \nmid 10$

$p \mid a$
$p \nmid b$

Ex: $p = 5$

$\left.\begin{array}{l} 5 \mid 50 \\ 5 \mid \underset{a}{5} \cdot \underset{b}{10} \end{array}\right\}$ here $5 \mid 5$ and $5 \mid 10$

$p \mid a$
$p \mid b$

proof: Suppose $p \mid ab$ where p is prime

Since p is prime we know its

only positive divisors are
1 and p.

Thus,
$gcd(p,a)=1$ or $gcd(p,a)=p$.

<u>case 1:</u> Suppose $gcd(p,a)=1$.
We know $gcd(p,a)=1$ and $p|ab$.
Thus from Monday's theorem
we know $p|b$.

<u>case 2:</u> Suppose $gcd(p,a)=p$.
Then, $p|a$.

So, in either case $p|a$ or $p|b$. $\blacksquare$

One area of number theory is called the study of <u>Diophantine equations</u>. These are polynomials in one or more variables whose coefficients are integers.

$\boxed{\text{Examples of Diophantine equations:}}$

$$578x + 153y = 17$$

linear equation
2 unknowns

$$x^2 + y^2 = z^2$$

Pythagorean equation

$$5 = x^2 + y^2$$

$p = x^2 + y^2$
p is prime

$$x^2 - ny^2 = 1$$ ← Pell-Fermat equation

$\left(\begin{array}{l} n>1 \text{ and } n \\ \text{is squarefree} \end{array}\right)$

can solve using continued fractions

ex: $x^2 - 5y^2 = 1$

$$x^n + y^n = z^n, \; n \geq 3$$ ← Fermat's last theorem

$x^3 + y^3 = z^3$

$x^4 + y^4 = z^4$

$\vdots \qquad \vdots$

Fermat claimed these equations have no non-trivial solutions (ie where you don't set one of them to be 0).

Fermat wrote in one of his books he had a proof but it can't fit in the margin.

It was proven in 1995 by Andrew Wiles.

NOVA PBS show "The proof"

For Diophantine equations you want "integer solutions". That is, solutions where the variables are integers.

<u>Questions</u>: Are there any integer solutions? If there are how many are there? Is there a formula for the integer solutions?

Theorem: Let $a,b,c \in \mathbb{Z}$ with a,b are not both zero.
Let $d = \gcd(a,b)$.

① $ax+by=c$ has integer solutions if and only if $d \mid c$.

has integer solutions means $\exists\, x,y \in \mathbb{Z}$ where $ax+by=c$

② If $ax+by=c$ has integer solutions and (x_0,y_0) is an integer solution [that is, $ax_0+by_0=c$] then the formula

$$x = x_0 - t\left(\frac{b}{d}\right)$$

$$y = y_0 + t\left(\frac{a}{d}\right)$$

gives all the integer solutions where t ranges over all integers.

(3) So either $ax+by=c$ has no solutions or infinitely many.

Ex: Consider

$$21x + 33y = 5$$

$\boxed{ax+by=c}$

$\boxed{c}$

Does this equation have integer solutions?

$$d = \gcd(a,b) = \gcd(21,33) = 3$$

$$3 \nmid 5$$

$\boxed{d \nmid c}$

No integer solutions by theorem

Doesn't count:

$$21\underbrace{\left(\frac{5}{21}\right)}_{\text{not an integer}}+33(0)=5$$

Ex: Consider

$$\boxed{578x+153y=17}$$

c = 17

$d=\gcd(578,153)=17$

$17 \mid 17$ ✓ $\leftarrow$ $\boxed{d \mid c}$

So the theorem says there are integer solutions.

We found one on Monday
it was $x_0 = 4$, $y_0 = -15$.

The theorem says that <u>all</u>
solutions are of the form

$$x = x_0 - t\left(\frac{b}{d}\right) = 4 - t\left(\frac{153}{17}\right) = 4 - 9t$$

$$y = y_0 + t\left(\frac{a}{d}\right) = -15 + t\left(\frac{578}{17}\right) = -15 + 34t$$

$$\left[\begin{array}{l} a = 578, b = 153, d = 17 \\ ax + by = c \end{array}\right]$$

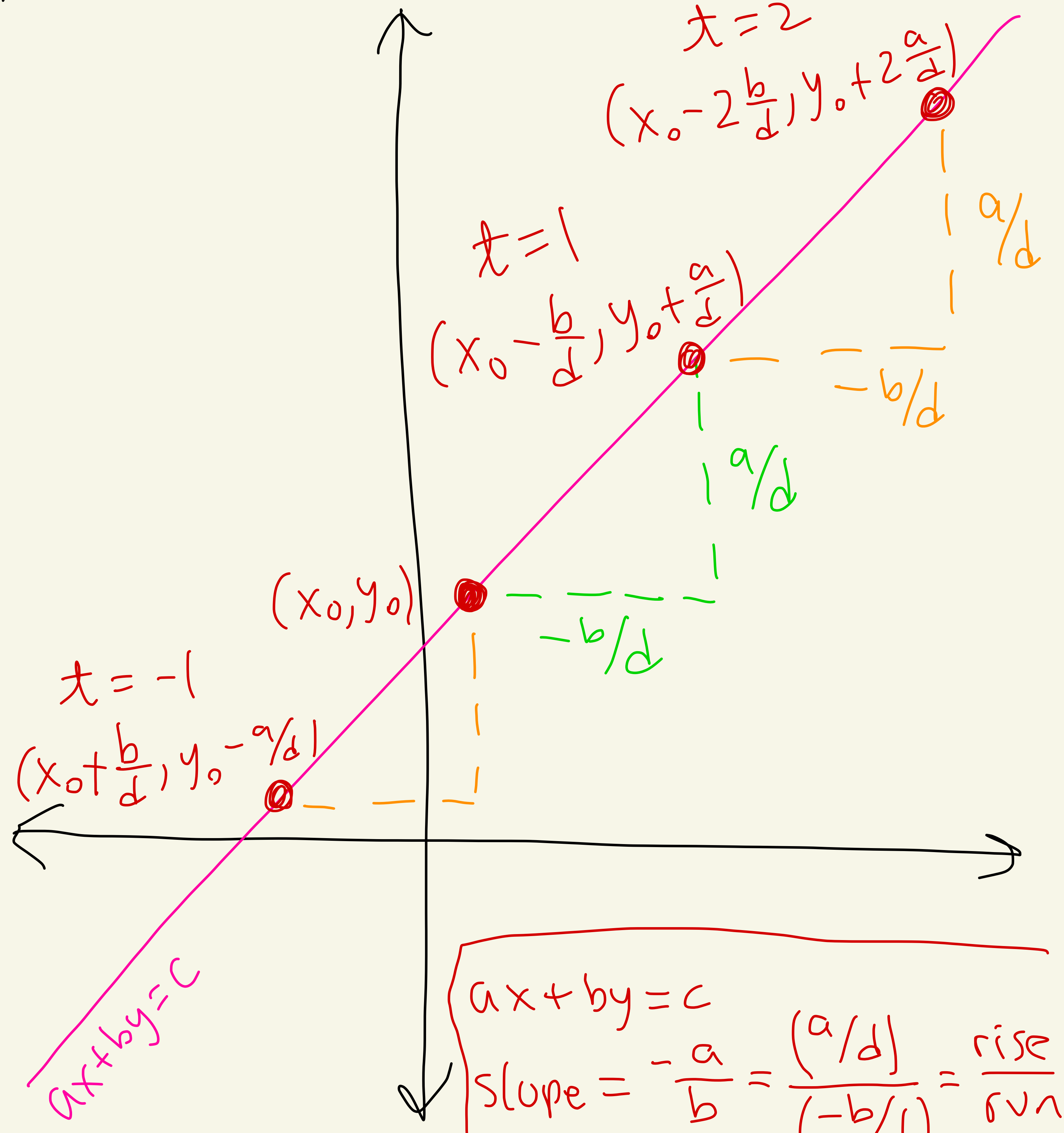
Some particular
solutions

are

t	$x=4-9t$	$y=-15+34t$
0	4	-15
1	-5	19
-1	13	-49
2	-14	53
-2	22	-83
⋮	⋮	⋮

$$ax + by = c \qquad x = x_0 - \left(\frac{b}{d}\right)t$$

$$a > 0,\ b < 0 \qquad y = y_0 + \left(\frac{a}{d}\right)t$$



$$ax + by = c$$

$$\text{slope} = -\frac{a}{b} = \frac{(a/d)}{(-b/d)} = \frac{\text{rise}}{\text{run}}$$