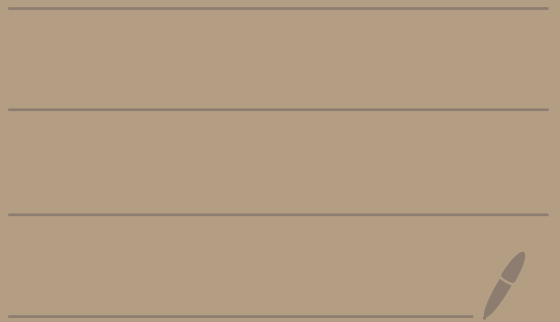


Math 4460

2/17/25



Super-duper prime theorem

Let a, b, p be integers where p is prime.

If $p | ab$, then $p | a$ or $p | b$.

Ex: $3 | 30 \rightarrow \underbrace{3}_p | \underbrace{3}_a \cdot \underbrace{10}_b$

$\rightarrow \underbrace{3}_p | 3$ note $p \nmid b$

Ex: $3 | 90 \rightarrow \underbrace{3}_p | \underbrace{3}_a \cdot \underbrace{30}_b$

$\rightarrow \underbrace{3}_p | 3$ and $\underbrace{3}_p | 30$

Proof:

Suppose $p|ab$ where p is prime.

Since p is prime, the positive divisors of p are 1 and p .

Then

$$\gcd(p, a) = 1$$

or

$$\gcd(p, a) = p.$$

Case 1: Suppose $\gcd(p, a) = 1$.

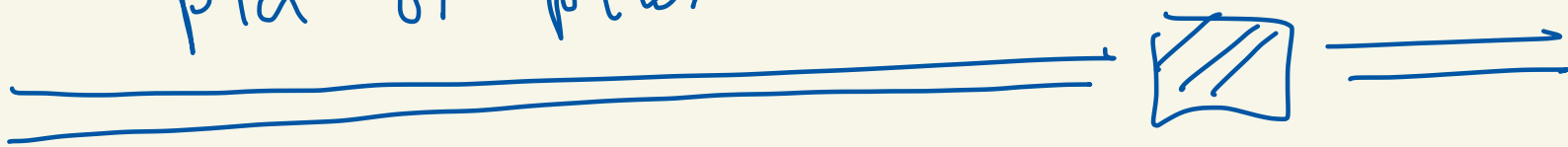
So, $\gcd(p, a) = 1$ and $p|ab$.

From Wed's theorem we get $p|b$.

Case 2: Suppose $\gcd(p, a) = p$.

Then, $p|a$.

Thus, in either case either
pla or plb.



One area of number theory
is called the study of
Diophantine equations

These are polynomials with one
or more variable with
integer coefficients.
You want to find integer solutions.

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 prime

$$x^2 - ny^2 = 1$$

$n > 1$, n is square free

← Pell-Fermat equation
you can solve it with continued fractions

$$x^n + y^n = z^n$$

$$n \geq 3$$

← Fermat's last theorem

Documentary on proof

"The proof"
NOVA PBS

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

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

Andrew Wiles
1995

For Diophantine equations
you'd ask: Are there any
integer solutions? If
there are, how many solutions?
Is there a formula for
the 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 $d \mid c$

integer
solutions
means
there
exist
 $x_0, y_0 \in \mathbb{Z}$
with
 $ax_0 + by_0 = c$

② If $ax+by=c$ has integer solutions and (x_0, y_0) is an integer solution, then every integer solution is of the form

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

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

where t is an integer.

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

Proof: On Weds. 

Ex: Consider

$$21x + 33y = 5 \leftarrow \boxed{ax + by = c}$$

Let

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

And

$$3 \nmid 5 \leftarrow \boxed{d \nmid c}$$

So

$$21x + 33y = 5$$

doesn't have integer solutions.

$$\left[21 \left(\frac{5}{21} \right) + 33(0) = 5 \right]$$

doesn't count not an integer

Ex: Consider

$$\underbrace{578x + 153y = 17}_{ax + by = c}$$

last week

We get

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

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

So there are integer solutions.

We found a solution using the Euclidean algorithm last week.

It was $x_0 = 4, y_0 = -15$.

By the theorem, every integer solution is of the form

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

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

That is

$$x = 4 - 9t$$

$$y = -15 + 34t$$

where $t \in \mathbb{Z}$

formula for
all integer
solutions to
 $578x + 153y = 17$

Some solutions are:

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

