## Coprime integers \&

## SOME DIOPHANTINE EQUATIONS

## Euclid's algorithm - reviews from last Thursday

We want to compute $\operatorname{gcd}(600,-136)$.

## Euclid's algorithm - reviews from last Thursday

We want to compute $\operatorname{gcd}(600,-136)$.
Remember that if $a=b q+r$ then $\operatorname{gcd}(a, b)=\operatorname{gcd}(r+b q, b)=\operatorname{gcd}(r, b)=\operatorname{gcd}(b, r)$.

## Euclid's algorithm - reviews from last Thursday

We want to compute $\operatorname{gcd}(600,-136)$.
Remember that if $a=b q+r$ then $\operatorname{gcd}(a, b)=\operatorname{gcd}(r+b q, b)=\operatorname{gcd}(r, b)=\operatorname{gcd}(b, r)$.

|  |  |  |  |  |  |  | $\operatorname{gcd}(600,-136)$ |  | $\operatorname{gcd}(600,136)$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 600 | = | 136 | $\times$ | 4 | + | 56 | $\operatorname{gcd}(600,136)$ | $=$ | $\operatorname{gcd}(136,56)$ |
| 136 | $=$ | 56 | $\times$ | 2 | + | 24 | $\operatorname{gcd}(136,56)$ | = | $\operatorname{gcd}(56,24)$ |
| 56 | = | 24 | $\times$ | 2 | + | 8 | $\operatorname{gcd}(56,24)$ | $=$ | $\operatorname{gcd}(24,8)$ |
| 24 | $=$ | 8 | $\times$ | 3 | + | 0 | $\operatorname{gcd}(24,8)$ | $=$ | $\operatorname{gcd}(8,0)=8$ |

Hence $\operatorname{gcd}(600,-136)=8$.
Since the sequence of remainders is decreasing and non-negative, it reaches 0 after finitely many steps.

## Euclid's algorithm - reviews from last Thursday

We want to compute $\operatorname{gcd}(600,-136)$.
Remember that if $a=b q+r$ then $\operatorname{gcd}(a, b)=\operatorname{gcd}(r+b q, b)=\operatorname{gcd}(r, b)=\operatorname{gcd}(b, r)$.

|  |  |  |  |  |  |  | $\operatorname{gcd}(600,-136)$ | $=$ | $\operatorname{gcd}(600,136)$ |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 600 | $=$ | 136 | $\times$ | 4 | + | 56 | $\operatorname{gcd}(600,136)$ | = | $\operatorname{gcd}(136,56)$ |
| 136 | = | 56 | $\times$ | 2 | + | 24 | $\operatorname{gcd}(136,56)$ | = | $\operatorname{gcd}(56,24)$ |
| 56 | = | 24 | $\times$ | 2 | + | 8 | $\operatorname{gcd}(56,24)$ |  | $\operatorname{gcd}(24,8)$ |
| 24 | = | 8 | $\times$ | 3 | $+$ | 0 | $\operatorname{gcd}(24,8)$ | = | $\operatorname{gcd}(8,0)=8$ |

Hence $\operatorname{gcd}(600,-136)=8$.
Since the sequence of remainders is decreasing and non-negative, it reaches 0 after finitely many steps.

Then it is possible to obtain a suitable Bézout's identity going backward:

$$
\begin{array}{rrr}
8 & =56+24 \times(-2) & \text { since } 8=56-24 \times 2 \\
& =56+(136+56 \times(-2)) \times(-2) & \text { since } 24=136-56 \times 2 \\
& =136 \times(-2)+56 \times 5 & \\
& =136 \times(-2)+(600+136 \times(-4)) \times 5 & \text { since } 56=600-136 \times 4 \\
8 & =600 \times 5+(-136) \times 22 &
\end{array}
$$

## Coprime integers

## Definition

Let $a, b \in \mathbb{Z}$ not both zero. We say that $a$ and $b$ are coprime (or relatively prime) if $\operatorname{gcd}(a, b)=1$.

## Coprime integers

## Definition

Let $a, b \in \mathbb{Z}$ not both zero. We say that $a$ and $b$ are coprime (or relatively prime) if $\operatorname{gcd}(a, b)=1$.

## Proposition: the converse of Bézout's identity holds for coprime numbers

Let $a, b \in \mathbb{Z}$ not both zero. Then

$$
\operatorname{gcd}(a, b)=1 \Leftrightarrow \exists u, v \in \mathbb{Z}, a u+b v=1
$$

## Coprime integers

## Definition

Let $a, b \in \mathbb{Z}$ not both zero. We say that $a$ and $b$ are coprime (or relatively prime) if $\operatorname{gcd}(a, b)=1$.

## Proposition: the converse of Bézout's identity holds for coprime numbers

Let $a, b \in \mathbb{Z}$ not both zero. Then

$$
\operatorname{gcd}(a, b)=1 \Leftrightarrow \exists u, v \in \mathbb{Z}, a u+b v=1
$$

Proof.
$\Rightarrow$ : it is simply Bézout's identity.
$\Leftarrow$ let $a, b \in \mathbb{Z}$ not both zero. Assume that $a u+b v=1$ for some $u, v \in \mathbb{Z}$.
Set $d=\operatorname{gcd}(a, b)$. Then $d \mid a$ and $d \mid b$, hence $d \mid(a u+b v)=1$.
Therefore $|d|=1$.
But since $d \in \mathbb{N}$, we get that $d=1$.

## Gauss' lemma

## Gauss' lemma

$\forall a, b, c \in \mathbb{Z},\left\{\left.\begin{array}{l}\operatorname{gcd}(a, b)=1 \\ a \mid b c\end{array} \Longrightarrow a \right\rvert\, c\right.$

## Gauss' lemma

## Gauss' lemma

$\forall a, b, c \in \mathbb{Z},\left\{\left.\begin{array}{l}\operatorname{gcd}(a, b)=1 \\ a \mid b c\end{array} \Longrightarrow a \right\rvert\, c\right.$

## Proof.

Let $a, b, c \in \mathbb{Z}$ such that $\operatorname{gcd}(a, b)=1$ and $a \mid b c$.
Then there exists $k \in \mathbb{Z}$ such that $b c=k a$.
By Bézout's identity, there exist $u, v \in \mathbb{Z}$ such that $1=a u+b v$.
Thus $c=(a u+b v) c=a u c+b c v=a u c+k a v=a(u c+k v)$.
Hence $a \mid c$.

## Affine diophantine equation: $a x+b y=c-1$

## Theorem

Let $a, b, c \in \mathbb{Z}$ with $a$ and $b$ not both zero.
Then the equation $a x+b y=c$ has an integer solution if and only if $\operatorname{gcd}(a, b) \mid c$.

## Affine diophantine equation: $a x+b y=c-1$

## Theorem

Let $a, b, c \in \mathbb{Z}$ with $a$ and $b$ not both zero.
Then the equation $a x+b y=c$ has an integer solution if and only if $\operatorname{gcd}(a, b) \mid c$.

## Proof.

$\Rightarrow$ : Assume that $a x+b y=c$ for some $(x, y) \in \mathbb{Z}^{2}$.
Since $\operatorname{gcd}(a, b) \mid a$ and $\operatorname{gcd}(a, b) \mid b$, we get that $\operatorname{gcd}(a, b) \mid a x+b y=c$.
$\Leftarrow$ : Assume that $\operatorname{gcd}(a, b) \mid c$, then there exists $k \in \mathbb{Z}$ such that $c=k \operatorname{gcd}(a, b)$.
By Bézout's identity, there exists $(u, v) \in \mathbb{Z}^{2}$ such that $a u+b v=\operatorname{gcd}(a, b)$.
Hence $a k u+b k v=k \operatorname{gcd}(a, b)=c$.
Therefore ( $k u, k v$ ) is an integer solution of the equation.

## Affine diophantine equation: $a x+b y=c-1$

## Theorem

Let $a, b, c \in \mathbb{Z}$ with $a$ and $b$ not both zero.
Then the equation $a x+b y=c$ has an integer solution if and only if $\operatorname{gcd}(a, b) \mid c$.

## Proof.

$\Rightarrow$ : Assume that $a x+b y=c$ for some $(x, y) \in \mathbb{Z}^{2}$.
Since $\operatorname{gcd}(a, b) \mid a$ and $\operatorname{gcd}(a, b) \mid b$, we get that $\operatorname{gcd}(a, b) \mid a x+b y=c$.
$\Leftrightarrow$ : Assume that $\operatorname{gcd}(a, b) \mid c$, then there exists $k \in \mathbb{Z}$ such that $c=k \operatorname{gcd}(a, b)$.
By Bézout's identity, there exists $(u, v) \in \mathbb{Z}^{2}$ such that $a u+b v=\operatorname{gcd}(a, b)$.
Hence $a k u+b k v=k \operatorname{gcd}(a, b)=c$.
Therefore ( $k u, k v$ ) is an integer solution of the equation.
In the next slide, I am going to solve an example of such a diophantine equation. The general "recipe" is in the lecture notes (see §8 of Chapter 2).

## Affine diophantine equation: $a x+b y=c-2$

We want to solve $20 x+16 y=500$ for $(x, y) \in \mathbb{Z}$.

## Affine diophantine equation: $a x+b y=c-2$

We want to solve $20 x+16 y=500$ for $(x, y) \in \mathbb{Z}$.
(1) Note that $\operatorname{gcd}(20,16)=4 \mid 500$, hence this equation admits a solution. Moreover, dividing by 4 , we get that $20 x+16 y=500 \Leftrightarrow 5 x+4 y=125$.
(2) Let's find a first solution starting from a Bézout relation $5 u+4 v=1$. In this example, there is an obvious Bézout relation: $5 \times 1+4 \times(-1)=1$. (otherwise, we can use Euclid's algorithm to find one) Hence $5 \times 125+4 \times(-125)=125$. So $(125,-125)$ is a solution
(3) Let's find all the solutions.

Let $(x, y)$ be a solution then $5 x+4 y=125$ and $5 \times 125+4 \times(-125)=125$.
Thus $5(x-125)+4(y+125)=0$, so $4 \mid 5(x-125)$.
Since $\operatorname{gcd}(4,5)=1$, by Gauss' lemma, $4 \mid x-125$. So $x=4 k+125$ for some $k \in \mathbb{Z}$.
Then $5(4 k)+4(y+125)=0$, i.e. $5 k+y+125=0$, so that $y=-5 k-125$.
Therefore $(x, y)=(4 k+125,-5 k-125)$.
(4) Conversely, $(4 k+125,-5 k-125)$ is a solution for every $k \in \mathbb{Z}$ : indeed, $20 x+16 y=20(4 k+125)+16(-5 k-125)=500$.
(5) Conclusion: the solutions are $(4 k+125,-5 k-125), k \in \mathbb{Z}$.

## Another diophantine equation

For general diophantine equations, there are no recipes (Fermat's Last Theorem is about some diophantine equations and took 4 centuries to be solved).

## Another diophantine equation

For general diophantine equations, there are no recipes (Fermat's Last Theorem is about some diophantine equations and took 4 centuries to be solved).

We want to find integer solutions of $x^{2}-y^{2}=401$.

## Another diophantine equation

For general diophantine equations, there are no recipes (Fermat's Last Theorem is about some diophantine equations and took 4 centuries to be solved).

We want to find integer solutions of $x^{2}-y^{2}=401$.
Note that $x^{2}-y^{2}=401 \Leftrightarrow(x-y)(x+y)=401$.
Since 401 is a prime number (I am sure you can look in the future for next Thursday lecture), then

$$
\text { either }\left\{\begin{array} { l } 
{ x - y = 1 } \\
{ x + y = 4 0 1 }
\end{array} \text { or } \left\{\begin{array} { l } 
{ x - y = - 1 } \\
{ x + y = - 4 0 1 }
\end{array} \text { or } \left\{\begin{array} { l } 
{ x - y = 4 0 1 } \\
{ x + y = 1 }
\end{array} \text { or } \left\{\begin{array}{l}
x-y=-401 \\
x+y=-1
\end{array}\right.\right.\right.\right.
$$

So either $(x, y)=(201,200)$, or $(x, y)=(-201,-200)$ or $(x, y)=(201,-200)$ or $(x, y)=(-201,200)$.

