MAT246H1-S – LEC0201/9201 Concepts in Abstract Mathematics

COPRIME INTEGERS & SOME DIOPHANTINE EQUATIONS



We want to compute gcd(600, -136).

We want to compute gcd(600, -136).

Remember that if a = bq + r then gcd(a, b) = gcd(r + bq, b) = gcd(r, b) = gcd(b, r).

We want to compute gcd(600, -136).

Remember that if a = bq + r then gcd(a, b) = gcd(r + bq, b) = gcd(r, b) = gcd(b, r).

							gcd(600, -136)	=	gcd(600, 136)
600	=	136	\times	4	+	56	gcd(600, 136)	=	gcd(136, 56)
136	=	56	\times	2	+	24	gcd(136, 56)	=	gcd(56, 24)
56	=	24	\times	2	+	8	gcd(56,24)	=	gcd(24, 8)
24	=	8	×	3	+	0	gcd(24, 8)	=	gcd(8,0) = 8

Hence gcd(600, -136) = 8.

Since the sequence of remainders is decreasing and non-negative, it reaches 0 after finitely many steps.

We want to compute gcd(600, -136).

Remember that if a = bq + r then gcd(a, b) = gcd(r + bq, b) = gcd(r, b) = gcd(b, r).

							gcd(600, -136)	=	gcd(600, 136)
600	=	136	\times	4	+	56	gcd(600, 136)	=	gcd(136, 56)
136	=	56	\times	2	+	24	gcd(136, 56)	=	gcd(56, 24)
56	=	24	\times	2	+	8	gcd(56,24)	=	gcd(24, 8)
24	=	8	×	3	+	0	gcd(24, 8)	=	gcd(8,0) = 8

Hence 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:

$8 = 56 + 24 \times (-2)$	since $8 = 56 - 24 \times 2$
$= 56 + (136 + 56 \times (-2)) \times (-2)$	since $24 = 136 - 56 \times 2$
$= 136 \times (-2) + 56 \times 5$	
$= 136 \times (-2) + (600 + 136 \times (-4)) \times 5$	since $56 = 600 - 136 \times 4$
$8 = 600 \times 5 + (-136) \times 22$	

Coprime integers

Definition

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

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

Coprime integers

Definition

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

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

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

Gauss' lemma

Gauss' lemma

$$\forall a, b, c \in \mathbb{Z}, \left\{ \begin{array}{c} \gcd(a, b) = 1\\ a|bc \end{array} \right. \implies a|c$$

Gauss' lemma

Gauss' lemma

$$\forall a, b, c \in \mathbb{Z}, \left\{ \begin{array}{c} \gcd(a, b) = 1\\ a|bc \end{array} \right. \implies a|c$$

Proof.

Let $a, b, c \in \mathbb{Z}$ such that gcd(a, b) = 1 and a|bc. Then there exists $k \in \mathbb{Z}$ such that bc = ka. By Bézout's identity, there exist $u, v \in \mathbb{Z}$ such that 1 = au + bv. Thus c = (au + bv)c = auc + bcv = auc + kav = a(uc + kv). Hence a|c.

Theorem

Let $a, b, c \in \mathbb{Z}$ with a and b not both zero.

Then the equation ax + by = c has an integer solution if and only if gcd(a, b)|c.

Theorem

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

Proof.

⇒: Assume that ax + by = c for some $(x, y) \in \mathbb{Z}^2$. Since gcd(a, b)|a and gcd(a, b)|b, we get that gcd(a, b)|ax + by = c. \Leftarrow : Assume that gcd(a, b)|c, then there exists $k \in \mathbb{Z}$ such that c = k gcd(a, b). By Bézout's identity, there exists $(u, v) \in \mathbb{Z}^2$ such that au + bv = gcd(a, b). Hence aku + bkv = k gcd(a, b) = c.

Therefore (ku, kv) is an integer solution of the equation.

Theorem

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

Proof.

⇒: Assume that ax + by = c for some $(x, y) \in \mathbb{Z}^2$. Since gcd(a, b)|a and gcd(a, b)|b, we get that gcd(a, b)|ax + by = c. \Leftarrow : Assume that gcd(a, b)|c, then there exists $k \in \mathbb{Z}$ such that c = k gcd(a, b). By Bézout's identity, there exists $(u, v) \in \mathbb{Z}^2$ such that au + bv = gcd(a, b). Hence aku + bkv = k gcd(a, b) = c. Therefore (ku, kv) 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).

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

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

- 1 Note that gcd(20, 16) = 4|500, hence this equation admits a solution. Moreover, dividing by 4, we get that $20x + 16y = 500 \Leftrightarrow 5x + 4y = 125$.
- 2 Let's find a first solution starting from a Bézout relation 5u + 4v = 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 5x + 4y = 125 and $5 \times 125 + 4 \times (-125) = 125$. Thus 5(x - 125) + 4(y + 125) = 0, so 4|5(x - 125). Since gcd(4, 5) = 1, by Gauss' lemma, 4|x - 125. So x = 4k + 125 for some $k \in \mathbb{Z}$. Then 5(4k) + 4(y + 125) = 0, i.e. 5k + y + 125 = 0, so that y = -5k - 125. Therefore (x, y) = (4k + 125, -5k - 125).

Conversely, (4k + 125, -5k - 125) is a solution for every k ∈ Z: indeed, 20x + 16y = 20(4k + 125) + 16(-5k - 125) = 500.

5 Conclusion: the solutions are $(4k + 125, -5k - 125), k \in \mathbb{Z}$.

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

either
$$\begin{cases} x - y = 1 \\ x + y = 401 \end{cases}$$
 or $\begin{cases} x - y = -1 \\ x + y = -401 \end{cases}$ or $\begin{cases} x - y = 401 \\ x + y = 1 \end{cases}$ or $\begin{cases} x - y = -401 \\ x + y = -1 \end{cases}$

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