Last time:

Let $m, n \in \mathbb{Z}$ with $m \neq 0$. We say that m divides n if n is a multiple of m, i.e.

$$n = mk \quad \text{for some} \quad k \in \mathbb{Z}, \quad \text{written } m|n$$

If m does not divide n, then we write $m \nmid n$.

Last time:

Let $m, n \in \mathbb{Z}$ with $m \neq 0$. We say that m divides n if n is a multiple of m, i.e.

$$n = mk \quad \text{for some} \quad k \in \mathbb{Z}, \quad \text{written } m|n$$

If m does not divide n, then we write $m \nmid n$. When we list the divisors of $n \in \mathbb{Z}_{>0}$, we give the positive integers that divide n.

Example: the divisors of 28 are 1, 2, 4, 7, 14, and 28.

The greatest common divisor of $a, b \in \mathbb{Z}_{>0}$, denoted $\gcd(a, b)$ is largest number that divides both a and b.

Last time:

Let $m, n \in \mathbb{Z}$ with $m \neq 0$. We say that m divides n if n is a multiple of m, i.e.

$$n = mk \quad \text{for some} \quad k \in \mathbb{Z}, \quad \text{written } m|n$$

If m does not divide n, then we write $m \nmid n$. When we list the divisors of $n \in \mathbb{Z}_{>0}$, we give the positive integers that divide n.

Example: the divisors of 28 are 1, 2, 4, 7, 14, and 28.

The greatest common divisor of $a, b \in \mathbb{Z}_{>0}$, denoted $\gcd(a, b)$ is largest number that divides both a and b.

We calculate $\gcd(a, b)$ either by comparing the prime factorizations (for small a, b) or by using the Euclidean algorithm.

Euclidean algorithm

The division algorithm says for any $a, b \in \mathbb{Z}$ with $b \neq 0$, there are unique integers q and r satisfying

$$a = bq + r \qquad \text{and} \qquad 0 \leqslant r < |b|.$$

Think: "a divided by b is q with remainder r."

Euclidean algorithm

The division algorithm says for any $a, b \in \mathbb{Z}$ with $b \neq 0$, there are unique integers q and r satisfying

$$a = bq + r \qquad \text{and} \qquad 0 \leqslant r < |b|.$$

Think: "a divided by b is q with remainder r."
Repeatedly apply the division algorithm to find the GCD:

$$\begin{array}{ccccccl}
a & = & b * q_1 & + & r_1 & & \\
b & = & r_1 * q_2 & + & r_2 & & \\
r_1 & = & r_2 * q_3 & + & r_3 & & \\
 & \vdots & & & & & \\
r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} & & \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} & \leftarrow & \gcd(a, b) \\
r_{n-2} & = & r_{n-1} * q_n & + & 0 & \leftarrow & r_n
\end{array}$$

On the homework, you show:

For any positive integers a and b, there exist integers x and y satisfying $\gcd(a, b) = ax + by$.

We say $\gcd(a, b)$ is an integral combination of a and b.

On the homework, you show:

For any positive integers a and b, there exist integers x and y satisfying $\gcd(a, b) = ax + by$.

We say $\gcd(a, b)$ is an integral combination of a and b.

Example:

$$\gcd(35, 100) = 7 \quad \text{and} \quad (3)35 + (-1)100 = 5$$

On the homework, you show:

For any positive integers a and b, there exist integers x and y satisfying $\gcd(a,b) = ax + by$.

We say $\gcd(a,b)$ is an integral combination of a and b.

Example:

$$\gcd(35,100) = 7 \quad \text{and} \quad (3)35 + (-1)100 = 5$$
$$\gcd(7,5) = 1 \quad \text{and} \quad (3)7 + (-4)5 = 1$$

On the homework, you show:

For any positive integers a and b, there exist integers x and y satisfying $\gcd(a, b) = ax + by$.

Strategy: Take the Euclidean algorithm and solve for r_{n-1}, starting from the end...

$$\begin{array}{ccccc}
a & = & b * q_1 & + & r_1 \\
b & = & r_1 * q_2 & + & r_2 \\
r_1 & = & r_2 * q_3 & + & r_3 \\
 & \vdots & & & \\
r_{n-5} & = & r_{n-4} * q_{n-3} & + & r_{n-3} \\
r_{n-4} & = & r_{n-3} * q_{n-2} & + & r_{n-2} \\
r_{n-3} & = & r_{n-2} * q_{n-1} & + & r_{n-1} \quad \leftarrow \gcd(a, b) \\
r_{n-2} & = & r_{n-1} * q_n & + & 0
\end{array}$$

We "know": For any positive integers a and b, there exist integers x and y satisfying $\gcd(a, b) = ax + by$. (prove on homework).

We “know”: For any positive integers a and b, there exist integers x and y satisfying $\gcd(a,b) = ax + by$. (prove on homework).

Claim: The smallest positive integer combination of a and b is $\gcd(a,b)$.

We “know”: For any positive integers a and b, there exist integers x and y satisfying $\gcd(a, b) = ax + by$. (prove on homework).

Claim: The smallest positive integer combination of a and b is $\gcd(a, b)$.

Proof. We know that $\gcd(a, b)$ is some integer combination of a and b. Now we show that $\gcd(a, b)$ is the smallest .

We "know": For any positive integers a and b, there exist integers x and y satisfying $\gcd(a,b) = ax + by$. (prove on homework).

Claim: The smallest positive integer combination of a and b is $\gcd(a,b)$.

Proof. We know that $\gcd(a,b)$ is some integer combination of a and b. Now we show that $\gcd(a,b)$ is the smallest .

Let $m, n \in \mathbb{Z}$, and consider $ma + nb$.

We "know": For any positive integers a and b, there exist integers x and y satisfying $\gcd(a, b) = ax + by$. (prove on homework).

Claim: The smallest positive integer combination of a and b is $\gcd(a, b)$.

Proof. We know that $\gcd(a, b)$ is some integer combination of a and b. Now we show that $\gcd(a, b)$ is the smallest .

Let $m, n \in \mathbb{Z}$, and consider $ma + nb$.

(Similar technique as last time! Show that $\gcd(a, b)$ is a divisor of $ma + nb \ldots$)

We "know": For any positive integers a and b, there exist integers x and y satisfying $\gcd(a, b) = ax + by$. (prove on homework).

Claim: The smallest positive integer combination of a and b is $\gcd(a, b)$.

Proof. We know that $\gcd(a, b)$ is some integer combination of a and b. Now we show that $\gcd(a, b)$ is the smallest .

Let $m, n \in \mathbb{Z}$, and consider $ma + nb$.

(Similar technique as last time! Show that $\gcd(a, b)$ is a divisor of $ma + nb \ldots$)

Let $d = \gcd(a, b)$

We "know": For any positive integers a and b, there exist integers x and y satisfying $\gcd(a, b) = ax + by$. (prove on homework).

Claim: The smallest positive integer combination of a and b is $\gcd(a, b)$.

Proof. We know that $\gcd(a, b)$ is some integer combination of a and b. Now we show that $\gcd(a, b)$ is the smallest .

Let $m, n \in \mathbb{Z}$, and consider $ma + nb$.

(Similar technique as last time! Show that $\gcd(a, b)$ is a divisor of $ma + nb \ldots$)

Let $d = \gcd(a, b)$, so that

$$a = kd \text{ and } b = \ell d \text{ for some } k, \ell \in \mathbb{Z}.$$

We "know": For any positive integers a and b, there exist integers x and y satisfying $\gcd(a, b) = ax + by$. (prove on homework).

Claim: The smallest positive integer combination of a and b is $\gcd(a, b)$.

Proof. We know that $\gcd(a, b)$ is some integer combination of a and b. Now we show that $\gcd(a, b)$ is the smallest .

Let $m, n \in \mathbb{Z}$, and consider $ma + nb$.

(Similar technique as last time! Show that $\gcd(a, b)$ *is a divisor of* $ma + nb \ldots$*)*

Let $d = \gcd(a, b)$, so that

$$a = kd \text{ and } b = \ell d \text{ for some } k, \ell \in \mathbb{Z}.$$

So

$$ma + nb$$

We "know": For any positive integers a and b, there exist integers x and y satisfying $\gcd(a, b) = ax + by$. (prove on homework).

Claim: The smallest positive integer combination of a and b is $\gcd(a, b)$.

Proof. We know that $\gcd(a, b)$ is some integer combination of a and b. Now we show that $\gcd(a, b)$ is the smallest .

Let $m, n \in \mathbb{Z}$, and consider $ma + nb$.

(Similar technique as last time! Show that $\gcd(a, b)$ is a divisor of $ma + nb \ldots$)

Let $d = \gcd(a, b)$, so that

$$a = kd \text{ and } b = \ell d \text{ for some } k, \ell \in \mathbb{Z}.$$

So

$$ma + nb = m(kd) + n(\ell d)$$

We "know": For any positive integers a and b, there exist integers x and y satisfying $\gcd(a, b) = ax + by$. (prove on homework).

Claim: The smallest positive integer combination of a and b is $\gcd(a, b)$.

Proof. We know that $\gcd(a, b)$ is some integer combination of a and b. Now we show that $\gcd(a, b)$ is the smallest .

Let $m, n \in \mathbb{Z}$, and consider $ma + nb$.

(Similar technique as last time! Show that $\gcd(a, b)$ is a divisor of $ma + nb\ldots$)

Let $d = \gcd(a, b)$, so that

$$a = kd \text{ and } b = \ell d \text{ for some } k, \ell \in \mathbb{Z}.$$

So

$$ma + nb = m(kd) + n(\ell d) = \underbrace{(mk + n\ell)}_{\in \mathbb{Z}\ \checkmark} d.$$

We "know": For any positive integers a and b, there exist integers x and y satisfying $\gcd(a, b) = ax + by$. (prove on homework).

Claim: The smallest positive integer combination of a and b is $\gcd(a, b)$.

Proof. We know that $\gcd(a, b)$ is some integer combination of a and b. Now we show that $\gcd(a, b)$ is the smallest .

Let $m, n \in \mathbb{Z}$, and consider $ma + nb$.

(Similar technique as last time! Show that $\gcd(a, b)$ is a divisor of $ma + nb$...)

Let $d = \gcd(a, b)$, so that

$$a = kd \text{ and } b = \ell d \text{ for some } k, \ell \in \mathbb{Z}.$$

So

$$ma + nb = m(kd) + n(\ell d) = \underbrace{(mk + n\ell)}_{\in\mathbb{Z} \ \checkmark} d.$$

Thus $ma + nb$ is a multiple of $d = \gcd(a, b)$.

We "know": For any positive integers a and b, there exist integers x and y satisfying $\gcd(a, b) = ax + by$. (prove on homework).

Claim: The smallest positive integer combination of a and b is $\gcd(a, b)$.

Proof. We know that $\gcd(a, b)$ is some integer combination of a and b. Now we show that $\gcd(a, b)$ is the smallest .

Let $m, n \in \mathbb{Z}$, and consider $ma + nb$.

(Similar technique as last time! Show that $\gcd(a, b)$ is a divisor of $ma + nb\ldots$)

Let $d = \gcd(a, b)$, so that

$$a = kd \text{ and } b = \ell d \text{ for some } k, \ell \in \mathbb{Z}.$$

So

$$ma + nb = m(kd) + n(\ell d) = \underbrace{(mk + n\ell)}_{\in \mathbb{Z}\ \checkmark} d.$$

Thus $ma + nb$ is a multiple of $d = \gcd(a, b)$. Therefore $\gcd(a, b)$ is the smallest positive integer combination of a and b. $\square$

Example: Let $a = 9$, $b = 12$.

Example: Let $a = 9$, $b = 12$. We have $\gcd(9, 12) = 3$.

Example: Let $a = 9$, $b = 12$. We have $\gcd(9, 12) = 3$. One integer combination of 9 and 12 giving 3 is

$$(-1)9 + (1)12 = 3.$$

Example: Let $a = 9$, $b = 12$. We have $\gcd(9, 12) = 3$. One integer combination of 9 and 12 giving 3 is

$$(-1)9 + (1)12 = 3.$$

Are there more?

Example: Let $a = 9$, $b = 12$. We have $\gcd(9, 12) = 3$. One integer combination of 9 and 12 giving 3 is

$$(-1)9 + (1)12 = 3.$$

Are there more?

a=	9	b=	12								
	-5	-4	-3	-2	-1	0	1	2	3	4	5
-5	-105	-96	-87	-78	-69	-60	-51	-42	-33	-24	-15
-4	-93	-84	-75	-66	-57	-48	-39	-30	-21	-12	-3
-3	-81	-72	-63	-54	-45	-36	-27	-18	-9	0	9
-2	-69	-60	-51	-42	-33	-24	-15	-6	3	12	21
-1	-57	-48	-39	-30	-21	-12	-3	6	15	24	33
0	-45	-36	-27	-18	-9	0	9	18	27	36	45
1	-33	-24	-15	-6	3	12	21	30	39	48	57
2	-21	-12	-3	6	15	24	33	42	51	60	69
3	-9	0	9	18	27	36	45	54	63	72	81
4	3	12	21	30	39	48	57	66	75	84	93
5	15	24	33	42	51	60	69	78	87	96	105

Example: Let $a = 9$, $b = 12$. We have $\gcd(9, 12) = 3$. One integer combination of 9 and 12 giving 3 is

$$(-1)9 + (1)12 = 3.$$

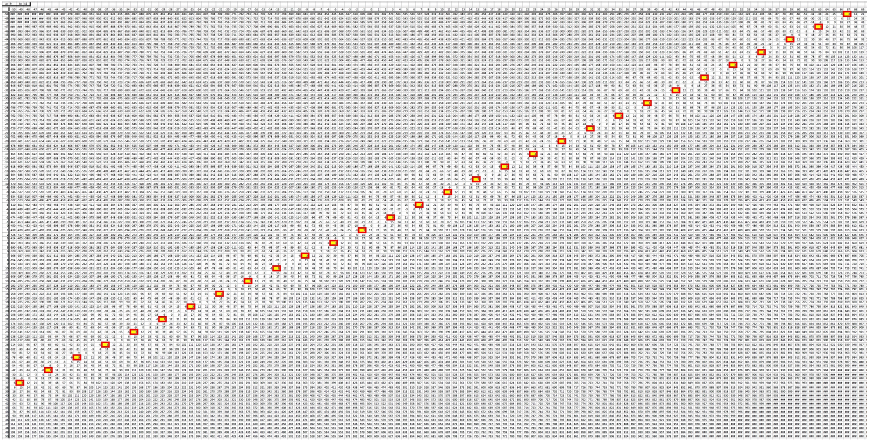
Are there more?

a= 9	b= 12																					
	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10	11
-10	-210	-201	-192	-183	-174	-165	-156	-147	-138	-129	-120	-111	-102	-93	-84	-75	-66	-57	-48	-39	-30	-21
-9	-198	-189	-180	-171	-162	-153	-144	-135	-126	-117	-108	-99	-90	-81	-72	-63	-54	-45	-36	-27	-18	-9
-8	-186	-177	-168	-159	-150	-141	-132	-123	-114	-105	-96	-87	-78	-69	-60	-51	-42	-33	-24	-15	-6	3
-7	-174	-165	-156	-147	-138	-129	-120	-111	-102	-93	-84	-75	-66	-57	-48	-39	-30	-21	-12	-3	6	15
-6	-162	-153	-144	-135	-126	-117	-108	-99	-90	-81	-72	-63	-54	-45	-36	-27	-18	-9	0	9	18	27
-5	-150	-141	-132	-123	-114	-105	-96	-87	-78	-69	-60	-51	-42	-33	-24	-15	-6	3	12	21	30	39
-4	-138	-129	-120	-111	-102	-93	-84	-75	-66	-57	-48	-39	-30	-21	-12	-3	6	15	24	33	42	51
-3	-126	-117	-108	-99	-90	-81	-72	-63	-54	-45	-36	-27	-18	-9	0	9	18	27	36	45	54	63
-2	-114	-105	-96	-87	-78	-69	-60	-51	-42	-33	-24	-15	-6	3	12	21	30	39	48	57	66	75
-1	-102	-93	-84	-75	-66	-57	-48	-39	-30	-21	-12	-3	6	15	24	33	42	51	60	69	78	87
0	-90	-81	-72	-63	-54	-45	-36	-27	-18	-9	0	9	18	27	36	45	54	63	72	81	90	99
1	-78	-69	-60	-51	-42	-33	-24	-15	-6	3	12	21	30	39	48	57	66	75	84	93	102	111
2	-66	-57	-48	-39	-30	-21	-12	-3	6	15	24	33	42	51	60	69	78	87	96	105	114	123
3	-54	-45	-36	-27	-18	-9	0	9	18	27	36	45	54	63	72	81	90	99	108	117	126	135
4	-42	-33	-24	-15	-6	3	12	21	30	39	48	57	66	75	84	93	102	111	120	129	138	147
5	-30	-21	-12	-3	6	15	24	33	42	51	60	69	78	87	96	105	114	123	132	141	150	159
6	-18	-9	0	9	18	27	36	45	54	63	72	81	90	99	108	117	126	135	144	153	162	171
7	-6	3	12	21	30	39	48	57	66	75	84	93	102	111	120	129	138	147	156	165	174	183
8	6	15	24	33	42	51	60	69	78	87	96	105	114	123	132	141	150	159	168	177	186	195
9	18	27	36	45	54	63	72	81	90	99	108	117	126	135	144	153	162	171	180	189	198	207
10	30	39	48	57	66	75	84	93	102	111	120	129	138	147	156	165	174	183	192	201	210	219

Example: Let $a = 9$, $b = 12$. We have $\gcd(9, 12) = 3$. One integer combination of 9 and 12 giving 3 is

$$(-1)9 + (1)12 = 3.$$

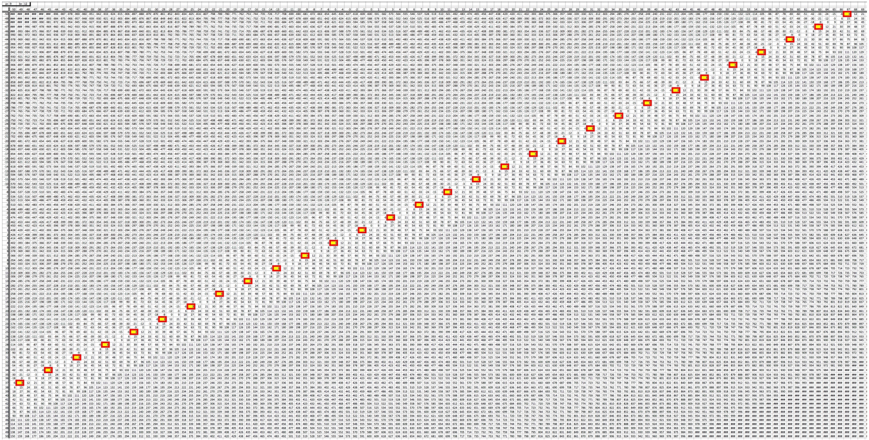
Are there more?



Example: Let $a = 9$, $b = 12$. We have $\gcd(9, 12) = 3$. One integer combination of 9 and 12 giving 3 is

$$(-1)9 + (1)12 = 3.$$

Are there more?

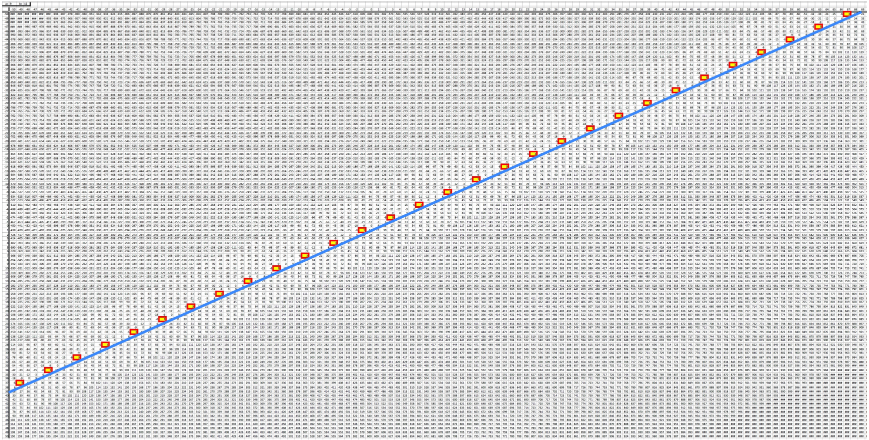


Infinitely many?

Example: Let $a = 9$, $b = 12$. We have $\gcd(9, 12) = 3$. One integer combination of 9 and 12 giving 3 is

$$(-1)9 + (1)12 = 3.$$

Are there more?



Infinitely many? (Looks like a *line* of them)

Example: Let $a = 9$, $b = 12$. We have $\gcd(9, 12) = 3$. One integer combination of 9 and 12 giving 3 is

$$(-1)9 + (1)12 = 3.$$

Are there more?

	-5	-4	-3	-2	-1	0	1	2	3	4	5
-5	-105	-96	-87	-78	-69	-60	-51	-42	-33	-24	-15
-4	-93	-84	-75	-66	-57	-48	-39	-30	-21	-12	-3
-3	-81	-72	-63	-54	-45	-36	-27	-18	-9	0	9
-2	-69	-60	-51	-42	-33	-24	-15	-6	3	12	21
-1	-57	-48	-39	-30	-21	-12	-3	6	15	24	33
0	-45	-36	-27	-18	-9	0	9	18	27	36	45
1	-33	-24	-15	-6	3	12	21	30	39	48	57
2	-21	-12	-3	6	15	24	33	42	51	60	69
3	-9	0	9	18	27	36	45	54	63	72	81
4	3	12	21	30	39	48	57	66	75	84	93
5	15	24	33	42	51	60	69	78	87	96	105

Infinitely many? (Looks like a *line* of them, with slope $-3/4$)

Example: Let $a = 9$, $b = 12$. We have $\gcd(9, 12) = 3$. One integer combination of 9 and 12 giving 3 is

$$(-1)9 + (1)12 = 3.$$

Are there more?

	-5	-4	-3	-2	-1	0	1	2	3	4	5
-5	-105	-96	-87	-78	-69	-60	-51	-42	-33	-24	-15
-4	-93	-84	-75	-66	-57	-48	-39	-30	-21	-12	-3
-3	-81	-72	-63	-54	-45	-36	-27	-18	-9	0	9
-2	-69	-60	-51	-42	-33	-24	-15	-6	3	12	21
-1	-57	-48	-39	-30	-21	-12	-3	6	15	24	33
0	-45	-36	-27	-18	-9	0	9	18	27	36	45
1	-33	-24	-15	-6	3	12	21	30	39	48	57
2	-21	-12	-3	6	15	24	33	42	51	60	69
3	-9	0	9	18	27	36	45	54	63	72	81
4	3	12	21	30	39	48	57	66	75	84	93
5	15	24	33	42	51	60	69	78	87	96	105

Infinitely many? (Looks like a *line* of them, with slope $-3/4 = -9/12$)

Lemma. For $a, b, x, y \in \mathbb{Z}$,

$$ax + by = a(x + bt) + b(y - at), \quad \text{for any } t \in \mathbb{Q}.$$

Lemma. For $a, b, x, y \in \mathbb{Z}$,

$$ax + by = a(x + bt) + b(y - at), \quad \text{for any } t \in \mathbb{Q}.$$

[Note: this is true for any t... real, complex, indeterminate, whatever. But the only hope that we have that $x + bt$ and $y - at$ could be integers is if t is at least rational.]

Lemma. For $a, b, x, y \in \mathbb{Z}$,

$$ax + by = a(x + bt) + b(y - at), \quad \text{for any } t \in \mathbb{Q}.$$

[Note: this is true for any t... real, complex, indeterminate, whatever. But the only hope that we have that $x + bt$ and $y - at$ could be integers is if t is at least rational.]

Now, given some $x, y \in \mathbb{Z}$ satisfying

$$ax + by = \gcd(a, b),$$

how do we generate more *integer solutions* x' and y' to $ax' + by' = \gcd(a, b)$?

Lemma. For $a, b, x, y \in \mathbb{Z}$,

$$ax + by = a(x + bt) + b(y - at), \quad \text{for any } t \in \mathbb{Q}.$$

[Note: this is true for any t... real, complex, indeterminate, whatever. But the only hope that we have that $x + bt$ and $y - at$ could be integers is if t is at least rational.]

Now, given some $x, y \in \mathbb{Z}$ satisfying

$$ax + by = \gcd(a, b),$$

how do we generate more *integer solutions* x' and y' to $ax' + by' = \gcd(a, b)$? Namely,

when are $\quad x + bt \quad$ and $\quad y - at \quad$ both integers (for the same t)?

Lemma. For $a, b, x, y \in \mathbb{Z}$,

$$ax + by = a(x + bt) + b(y - at), \quad \text{for any } t \in \mathbb{Q}.$$

[Note: this is true for any t... real, complex, indeterminate, whatever. But the only hope that we have that $x + bt$ and $y - at$ could be integers is if t is at least rational.]

Now, given some $x, y \in \mathbb{Z}$ satisfying

$$ax + by = \gcd(a, b),$$

how do we generate more *integer solutions* x' and y' to $ax' + by' = \gcd(a, b)$? Namely,

when are $x + bt$ and $y - at$ both integers (for the same t)?

This happens exactly whenever

bt and at are both integers (for the same t). (∗)

Lemma. For $a, b, x, y \in \mathbb{Z}$,

$$ax + by = a(x + bt) + b(y - at), \quad \text{for any } t \in \mathbb{Q}.$$

[Note: this is true for any t... real, complex, indeterminate, whatever. But the only hope that we have that $x + bt$ and $y - at$ could be integers is if t is at least rational.]

Now, given some $x, y \in \mathbb{Z}$ satisfying

$$ax + by = \gcd(a, b),$$

how do we generate more *integer solutions* x' and y' to $ax' + by' = \gcd(a, b)$? Namely,

when are $x + bt$ and $y - at$ both integers (for the same t)?

This happens exactly whenever

$$bt \text{ and } at \text{ are both integers (for the same } t). \qquad (*)$$

1. $t \in \mathbb{Q}$

Lemma. For $a, b, x, y \in \mathbb{Z}$,

$$ax + by = a(x + bt) + b(y - at), \quad \text{for any } t \in \mathbb{Q}.$$

[Note: this is true for any t... real, complex, indeterminate, whatever. But the only hope that we have that $x + bt$ and $y - at$ could be integers is if t is at least rational.]

Now, given some $x, y \in \mathbb{Z}$ satisfying

$$ax + by = \gcd(a, b),$$

how do we generate more *integer solutions* x' and y' to $ax' + by' = \gcd(a, b)$? Namely,

when are $x + bt$ and $y - at$ both integers (for the same t)?

This happens exactly whenever

bt and at are both integers (for the same t). (∗)

1. $t \in \mathbb{Q}$
2. If $t = n/m$ in lowest terms, then (∗) if and only if $m|a$ and $m|b$.

Lemma. For $a, b, x, y \in \mathbb{Z}$,

$$ax + by = a(x + bt) + b(y - at), \quad \text{for any } t \in \mathbb{Q}.$$

[Note: this is true for any t... real, complex, indeterminate, whatever. But the only hope that we have that $x + bt$ and $y - at$ could be integers is if t is at least rational.]

Now, given some $x, y \in \mathbb{Z}$ satisfying

$$ax + by = \gcd(a, b),$$

how do we generate more *integer solutions* x' and y' to $ax' + by' = \gcd(a, b)$? Namely,

when are $x + bt$ and $y - at$ both integers (for the same t)?

This happens exactly whenever

$$bt \text{ and } at \text{ are both integers (for the same } t). \qquad (*)$$

1. $t \in \mathbb{Q}$
2. If $t = n/m$ in lowest terms, then $(*)$ if and only if $m|a$ and $m|b$.

So $\boxed{t = k/\gcd(a, b)}$ for any $k \in \mathbb{Z}$ works!

Theorem

Let a and b be nonzero integers, and let $g = \gcd(a, b)$.

(1) *If $ax + by = z$ for $x, y \in \mathbb{Z}$, then $g|z$. (homework)*

(2) *The equation $ax_1 + by_1 = g$ always has at least one integer solution, which can be found via the Euclidean algorithm.*

(3) *The integers solutions to $g = ax + by$ are given by*

$$x = x_1 + \frac{kb}{g} \quad \text{and} \quad y = y_1 - \frac{ka}{g}, \quad k \in \mathbb{Z}.$$