HKOI Training

$ami \sim wkc$

Last modified: March 8, 2010

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Euclidean algorithm

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Finding integer solutions for $\gcd$

Finding integers solutions to $123x + 9y = 3$.

Finding integer solutions for $\gcd$

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Finding integers solutions to $123x + 9y = 3$.

Remark. *Here, all the unknowns are assumed to be integers.*

Euclidean algorithm
Finding integer solutions
Solving modulus equation
End

Finding integer solutions for $\gcd$

Finding integers solutions to $123x + 9y = 3$.

Remark. *Here, all the unknowns are assumed to be integers.*

k	r_k	q_k	x_k	y_k	Formulae
0	123		1	0	
1	9		0	1	
2	6	13	1	-13	$123 = 9 \cdot 13 + 6$
3	3	1	-1	14	$9 = 6 \cdot 1 + 3$
4	0	2	3	-41	$6 = 3 \cdot 2 + 0$

To understand the euclidean algorithm for finding a pariturclar solution.

Finding integer solutions for $\gcd$

Euclidean algorithm

- Finding integer solutions
- Solving modulus equation

End

Finding integers solutions to $123x + 9y = 3$.

Remark. *Here, all the unknowns are assumed to be integers.*

k	r_k	q_k	x_k	y_k	Formulae
0	123		1	0	
1	9		0	1	
2	6	13	1	-13	$123 = 9 \cdot 13 + 6$
3	3	1	-1	14	$9 = 6 \cdot 1 + 3$
4	0	2	3	-41	$6 = 3 \cdot 2 + 0$

To understand the euclidean algorithm for finding a paritucular solution.

First, we have $123 = 9\,(13) + 6 \iff 123\,(1) + 9\,(-13) = 6$

Finding integer solutions for $\gcd$

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Finding integers solutions to $123x + 9y = 3$.

Remark. *Here, all the unknowns are assumed to be integers.*

k	r_k	q_k	x_k	y_k	Formulae
0	123		1	0	
1	9		0	1	
2	6	13	1	-13	$123 = 9 \cdot 13 + 6$
3	3	1	-1	14	$9 = 6 \cdot 1 + 3$
4	0	2	3	-41	$6 = 3 \cdot 2 + 0$

To understand the euclidean algorithm for finding a pariticular solution.

First, we have $123 = 9\,(13) + 6 \iff 123\,(1) + 9\,(-13) = 6$

From the second formulae, $9 = 6\,(1) + 3 \iff 9\,(1) - 6\,(1) = 3$

Finding integer solutions for $\gcd$

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Finding integers solutions to $123x + 9y = 3$.

Remark. *Here, all the unknowns are assumed to be integers.*

k	r_k	q_k	x_k	y_k	Formulae
0	123		1	0	
1	9		0	1	
2	6	13	1	-13	$123 = 9 \cdot 13 + 6$
3	3	1	-1	14	$9 = 6 \cdot 1 + 3$
4	0	2	3	-41	$6 = 3 \cdot 2 + 0$

To understand the euclidean algorithm for finding a parituclar solution.

First, we have $123 = 9\,(13) + 6 \iff 123\,(1) + 9\,(-13) = 6$

From the second formulae, $9 = 6\,(1) + 3 \iff 9\,(1) - 6\,(1) = 3$

i.e. $9\,(1) - (123\,(1) + 9\,(-13))\,(1) = 3 \iff 123\,(-1) + 9\,(14) = 3$

Finding integer solutions for gcd

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Finding integers solutions to $123x + 9y = 3$.

Remark. *Here, all the unknowns are assumed to be integers.*

k	r_k	q_k	x_k	y_k	Formulae
0	123		1	0	
1	9		0	1	
2	6	13	1	-13	$123 = 9 \cdot 13 + 6$
3	3	1	-1	14	$9 = 6 \cdot 1 + 3$
4	0	2	3	-41	$6 = 3 \cdot 2 + 0$

To understand the euclidean algorithm for finding a parituclar solution.

First, we have $123 = 9\,(13) + 6 \iff 123\,(1) + 9\,(-13) = 6$

From the second formulae, $9 = 6\,(1) + 3 \iff 9\,(1) - 6\,(1) = 3$

i.e. $9\,(1) - (123\,(1) + 9\,(-13))\,(1) = 3 \iff 123\,(-1) + 9\,(14) = 3$

Through this, you should know the new x_k and y_k are obtained

by $x_{k-2} - q_k x_{k-1}$ and $y_{k-2} - q_k y_{k-1}$.

Finding integer solutions for $\gcd$

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Finding integers solutions to $123x + 9y = 3$.

Remark. *Here, all the unknowns are assumed to be integers.*

k	r_k	q_k	x_k	y_k	Formulae
0	123		1	0	
1	9		0	1	
2	6	13	1	-13	$123 = 9 \cdot 13 + 6$
3	3	1	-1	14	$9 = 6 \cdot 1 + 3$
4	0	2	3	-41	$6 = 3 \cdot 2 + 0$

To understand the euclidean algorithm for finding a pariutuclar solution.

First, we have $123 = 9\,(13) + 6 \iff 123\,(1) + 9\,(-13) = 6$

From the second formulae, $9 = 6\,(1) + 3 \iff 9\,(1) - 6\,(1) = 3$

i.e. $9\,(1) - (123\,(1) + 9\,(-13))\,(1) = 3 \iff 123\,(-1) + 9\,(14) = 3$

Through this, you should know the new x_k and y_k are obtained

by $x_{k-2} - q_k x_{k-1}$ and $y_{k-2} - q_k y_{k-1}$.

Remark. *Remember that, we always read the last but one row to find a solution.*

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Finding integer solutions for any integer

Finding integers solutions to $12x + 5y = 3$.

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Finding integer solutions for any integer

Finding integers solutions to $12x + 5y = 3$.

k	r_k	q_k	x_k	y_k	Formulae
0	12		1	0	
1	5		0	1	
2	2	2	1	-2	$12 = 5 \cdot 2 + 2$
3	1	2	-2	5	$5 = 2 \cdot 2 + 1$
4	0	2	5	-12	$2 = 1 \cdot 2 + 0$

Finding integer solutions for any integer

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Finding integers solutions to $12x + 5y = 3$.

k	r_k	q_k	x_k	y_k	Formulae
0	12		1	0	
1	5		0	1	
2	2	2	1	-2	$12 = 5 \cdot 2 + 2$
3	1	2	-2	5	$5 = 2 \cdot 2 + 1$
4	0	2	5	-12	$2 = 1 \cdot 2 + 0$

This time, we let $m = 12$ and $n = 5$.

First, we have $m = n\,(2) + 2 \iff m\,(1) + n\,(-2) = 2$

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Finding integer solutions for any integer

Finding integers solutions to $12x + 5y = 3$.

k	r_k	q_k	x_k	y_k	Formulae
0	12		1	0	
1	5		0	1	
2	2	2	1	-2	$12 = 5 \cdot 2 + 2$
3	1	2	-2	5	$5 = 2 \cdot 2 + 1$
4	0	2	5	-12	$2 = 1 \cdot 2 + 0$

This time, we let $m = 12$ and $n = 5$.

First, we have $m = n\,(2) + 2 \iff m\,(1) + n\,(-2) = 2$

From the second formulae, $n = 2\,(2) + 1 \iff n\,(1) - 2\,(2) = 1$

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Finding integer solutions for any integer

Finding integers solutions to $12x + 5y = 3$.

k	r_k	q_k	x_k	y_k	Formulae
0	12		1	0	
1	5		0	1	
2	2	2	1	-2	$12 = 5 \cdot 2 + 2$
3	1	2	-2	5	$5 = 2 \cdot 2 + 1$
4	0	2	5	-12	$2 = 1 \cdot 2 + 0$

This time, we let $m = 12$ and $n = 5$.

First, we have $m = n\,(2) + 2 \iff m\,(1) + n\,(-2) = 2$

From the second formulae, $n = 2\,(2) + 1 \iff n\,(1) - 2\,(2) = 1$

i.e. $n\,(1) - (m\,(1) + n\,(-2))\,(2) = 1 \iff m\,(-2) + n\,(5) = 1$

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Finding integer solutions for any integer

Finding integers solutions to $12x + 5y = 3$.

k	r_k	q_k	x_k	y_k	Formulae
0	12		1	0	
1	5		0	1	
2	2	2	1	-2	$12 = 5 \cdot 2 + 2$
3	1	2	-2	5	$5 = 2 \cdot 2 + 1$
4	0	2	5	-12	$2 = 1 \cdot 2 + 0$

This time, we let $m = 12$ and $n = 5$.

First, we have $m = n(2) + 2 \iff m(1) + n(-2) = 2$

From the second formulae, $n = 2(2) + 1 \iff n(1) - 2(2) = 1$

i.e. $n(1) - (m(1) + n(-2))(2) = 1 \iff m(-2) + n(5) = 1$

Hence, $3(m(-2) + n(5)) = 3 \iff m(-6) + n(15) = 3$

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Finding integer solutions for any integer

Finding integers solutions to $12x + 5y = 3$.

k	r_k	q_k	x_k	y_k	Formulae
0	12		1	0	
1	5		0	1	
2	2	2	1	-2	$12 = 5 \cdot 2 + 2$
3	1	2	-2	5	$5 = 2 \cdot 2 + 1$
4	0	2	5	-12	$2 = 1 \cdot 2 + 0$

This time, we let $m = 12$ and $n = 5$.

First, we have $m = n(2) + 2 \iff m(1) + n(-2) = 2$

From the second formulae, $n = 2(2) + 1 \iff n(1) - 2(2) = 1$

i.e. $n(1) - (m(1) + n(-2))(2) = 1 \iff m(-2) + n(5) = 1$

Hence, $3(m(-2) + n(5)) = 3 \iff m(-6) + n(15) = 3$

$(x, y) = (-6, 15)$ is a solution.

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Solving modulus equation

Find all integers x such that $7x \bmod 13 = 1$.

Solving modulus equation

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Find all integers x such that $7x \bmod 13 = 1$.

Proof. The remainder is 1 means that $7x$ is the sum of a multiple of 13 and 1.

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Solving modulus equation

Find all integers x such that $7x \bmod 13 = 1$.

Proof. The remainder is 1 means that $7x$ is the sum of a multiple of 13 and 1. Mathematically, this is equivalent to $7x = 13m + 1$ for some x and m.

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Solving modulus equation

Find all integers x such that $7x \bmod 13 = 1$.

Proof. The remainder is 1 means that $7x$ is the sum of a multiple of 13 and 1.
Mathematically, this is equivalent to $7x = 13m + 1$ for some x and m.
Rewrite it into $7x - 13m = 1$ and let $y = -m$.

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Solving modulus equation

Find all integers x such that $7x \bmod 13 = 1$.

Proof. The remainder is 1 means that $7x$ is the sum of a multiple of 13 and 1.

Mathematically, this is equivalent to $7x = 13m + 1$ for some x and m.

Rewrite it into $7x - 13m = 1$ and let $y = -m$.

It becomes $7x + 13y = 1$ and should have infinitely many solutions.

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Solving modulus equation

Find all integers x such that $7x \bmod 13 = 1$.

Proof. The remainder is 1 means that $7x$ is the sum of a multiple of 13 and 1.

Mathematically, this is equivalent to $7x = 13m + 1$ for some x and m.

Rewrite it into $7x - 13m = 1$ and let $y = -m$.

It becomes $7x + 13y = 1$ and should have infinitely many solutions.

Finally, using the euclidean algorithm,

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Solving modulus equation

Find all integers x such that $7x \bmod 13 = 1$.

Proof. The remainder is 1 means that $7x$ is the sum of a multiple of 13 and 1.

Mathematically, this is equivalent to $7x = 13m + 1$ for some x and m.

Rewrite it into $7x - 13m = 1$ and let $y = -m$.

It becomes $7x + 13y = 1$ and should have infinitely many solutions.

Finally, using the euclidean algorithm,

k	r_k	q_k	x_k	y_k	Formulae
0	13		1	0	
1	7		0	1	
2	6	1	1	-1	$13 = 7 \cdot 1 + 6$
3	1	1	-1	2	$7 = 6 \cdot 1 + 1$
4	0	6	7	-13	$6 = 1 \cdot 6 + 0$

we find $x = 2$ is one of the solution.

Euclidean algorithm
- Finding integer solutions
- Solving modulus equation

End

Solving modulus equation

Find all integers x such that $7x \bmod 13 = 1$.

Proof. The remainder is 1 means that $7x$ is the sum of a multiple of 13 and 1.
Mathematically, this is equivalent to $7x = 13m + 1$ for some x and m.
Rewrite it into $7x - 13m = 1$ and let $y = -m$.
It becomes $7x + 13y = 1$ and should have infinitely many solutions.
Finally, using the euclidean algorithm,

k	r_k	q_k	x_k	y_k	Formulae
0	13		1	0	
1	7		0	1	
2	6	1	1	-1	$13 = 7 \cdot 1 + 6$
3	1	1	-1	2	$7 = 6 \cdot 1 + 1$
4	0	6	7	-13	$6 = 1 \cdot 6 + 0$

we find $x = 2$ is one of the solution.

Hence, all the integers x are of the form $2 + 13k$ where k is any integers.

□

Euclidean algorithm
End

End