Solutions to HW07 Problems

BILL, RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

HW07, Problem 1

HW07, Problem 1

SOLUTION

What DAY and TIME are the TIMED FINAL?

HW07, Problem 1

SOLUTION
What DAY and TIME are the TIMED FINAL?
SOLUTION Friday Dec 17 at 8:00PM on Zoom.

HW07, Problem 1

SOLUTION
What DAY and TIME are the TIMED FINAL?
SOLUTION Friday Dec 17 at 8:00PM on Zoom.

If that DAY/TIME is not good for you then EMAIL ME.

HW07, Problem 1

SOLUTION
What DAY and TIME are the TIMED FINAL?
SOLUTION Friday Dec 17 at 8:00PM on Zoom.

If that DAY/TIME is not good for you then EMAIL ME.
SOLUTION If this applies to you, EMAIL ME.

HW07, Problem 1

SOLUTION
What DAY and TIME are the TIMED FINAL?
SOLUTION Friday Dec 17 at 8:00PM on Zoom.

If that DAY/TIME is not good for you then EMAIL ME.
SOLUTION If this applies to you, EMAIL ME.

We are NOT meeting the Tuesday of Thankgiving. When is the make-up lecture?

HW07, Problem 1

SOLUTION
What DAY and TIME are the TIMED FINAL?
SOLUTION Friday Dec 17 at 8:00PM on Zoom.

If that DAY/TIME is not good for you then EMAIL ME.
SOLUTION If this applies to you, EMAIL ME.

We are NOT meeting the Tuesday of Thankgiving. When is the make-up lecture?
SOLUTION Wed Nov 17 at 8:00PM on my zoom
`https://umd.zoom.us/my/gasarch`

HW07, Problem 2

Let a_1, a_2, a_3 be such that every pair a_i, a_j are relatively prime. Show that

$$\phi(a_1 a_2 a_3) = \phi(a_1)\phi(a_2)\phi(a_3).$$

You may use that if a, b are rel prime then $\phi(ab) = \phi(a)\phi(b)$.

HW07, Problem 2

Let a_1, a_2, a_3 be such that every pair a_i, a_j are relatively prime. Show that

$$\phi(a_1 a_2 a_3) = \phi(a_1)\phi(a_2)\phi(a_3).$$

You may use that if a, b are rel prime then $\phi(ab) = \phi(a)\phi(b)$.

SOLUTION

Since $a_1 a_2$ is rel prime to a_3 we know that

$$\phi(a_1(a_2 a_3)) = \phi(a_1)\phi(a_2 a_n).$$

HW07, Problem 2

Let a_1, a_2, a_3 be such that every pair a_i, a_j are relatively prime. Show that

$$\phi(a_1 a_2 a_3) = \phi(a_1)\phi(a_2)\phi(a_3).$$

You may use that if a, b are rel prime then $\phi(ab) = \phi(a)\phi(b)$.
SOLUTION
Since $a_1 a_2$ is rel prime to a_3 we know that

$$\phi(a_1(a_2 a_3)) = \phi(a_1)\phi(a_2 a_n).$$

We now use $\phi(a_2 a_3) = \phi(a_2)\phi(a_3)$ to get

$$\phi(a_1(a_2 a_3)) = \phi(a_1)\phi(a_2 a_3) = \phi(a_1)\phi(a_2)\phi(a_3).$$

HW07, Problem 3, EXTRA

If $a_1, \ldots, a_n$ are such that every pair is rel prime then

$$\phi(a_1 a_2 \cdots a_n) = \phi(a_1)\phi(a_2)\cdots\phi(a_n).$$

HW07, Problem 3, EXTRA

If $a_1, \ldots, a_n$ are such that every pair is rel prime then

$$\phi(a_1 a_2 \cdots a_n) = \phi(a_1)\phi(a_2)\cdots\phi(a_n).$$

How do you prove this?

HW07, Problem 3, EXTRA

If $a_1, \ldots, a_n$ are such that every pair is rel prime then

$$\phi(a_1 a_2 \cdots a_n) = \phi(a_1)\phi(a_2)\cdots\phi(a_n).$$

How do you prove this?

By Induction!

HW07, Problem 3

Let p be a prime and $a \geq 1$. Find and prove a formula for $\phi(p^a)$.

HW07, Problem 3

Let p be a prime and $a \geq 1$. Find and prove a formula for $\phi(p^a)$.

SOLUTION

We need to know:

How many elements of $\{1, \ldots, p^a\}$ **are** rel prime to p^a?

HW07, Problem 3

Let p be a prime and $a \geq 1$. Find and prove a formula for $\phi(p^a)$.

SOLUTION

We need to know:

How many elements of $\{1, \ldots, p^a\}$ **are** rel prime to p^a?

It is easier to find

How many elements of $\{1, \ldots, p^a\}$ **are not** rel prime to p^a?

HW07, Problem 3

Let p be a prime and $a \geq 1$. Find and prove a formula for $\phi(p^a)$.
SOLUTION
We need to know:
How many elements of $\{1, \ldots, p^a\}$ **are** rel prime to p^a?

It is easier to find
How many elements of $\{1, \ldots, p^a\}$ **are not** rel prime to p^a?

Those elements are

$$\{p, 2p, 3p, \ldots, p^{a-1}p\}.$$

So there **are** p^{a-1} such elements.

HW07, Problem 3

Let p be a prime and $a \geq 1$. Find and prove a formula for $\phi(p^a)$.
SOLUTION
We need to know:
How many elements of $\{1, \ldots, p^a\}$ **are** rel prime to p^a?

It is easier to find
How many elements of $\{1, \ldots, p^a\}$ **are not** rel prime to p^a?

Those elements are

$$\{p, 2p, 3p, \ldots, p^{a-1}p\}.$$

So there **are** p^{a-1} such elements.

So the number that **are** rel prime to p^a is

$$p^a - p^{a-1}$$

HW07, Problem 4

Using the last two problems, compute by hand: $\phi(3528)$.

HW07, Problem 4

Using the last two problems, compute by hand: $\phi(3528)$.

SOLUTION

We first FACTOR 3528. Since the last digit is even, 2 divides it.
TRICK: since the last 2 digits, 28, is div by 4, its div by 4.

HW07, Problem 4

Using the last two problems, compute by hand: $\phi(3528)$.

SOLUTION

We first FACTOR 3528. Since the last digit is even, 2 divides it.
TRICK: since the last 2 digits, 28, is div by 4, its div by 4.

$3528 = 2^2 \times 882.$

HW07, Problem 4

Using the last two problems, compute by hand: $\phi(3528)$.

SOLUTION

We first FACTOR 3528. Since the last digit is even, 2 divides it.
TRICK: since the last 2 digits, 28, is div by 4, its div by 4.

$3528 = 2^2 \times 882$. 882 is div by 2 so we get

HW07, Problem 4

Using the last two problems, compute by hand: $\phi(3528)$.

SOLUTION

We first FACTOR 3528. Since the last digit is even, 2 divides it. TRICK: since the last 2 digits, 28, is div by 4, its div by 4.

$3528 = 2^2 \times 882$. 882 is div by 2 so we get

$3528 = 2^3 \times 441$.

HW07, Problem 4

Using the last two problems, compute by hand: $\phi(3528)$.

SOLUTION

We first FACTOR 3528. Since the last digit is even, 2 divides it.
TRICK: since the last 2 digits, 28, is div by 4, its div by 4.

$3528 = 2^2 \times 882$. 882 is div by 2 so we get

$3528 = 2^3 \times 441$. Sum of digits of 441 is 9, so $441 \equiv 0 \pmod{9}$.

HW07, Problem 4

Using the last two problems, compute by hand: $\phi(3528)$.

SOLUTION

We first FACTOR 3528. Since the last digit is even, 2 divides it. TRICK: since the last 2 digits, 28, is div by 4, its div by 4.

$3528 = 2^2 \times 882$. 882 is div by 2 so we get

$3528 = 2^3 \times 441$. Sum of digits of 441 is 9, so $441 \equiv 0 \pmod 9$.

$3528 = 2^3 \times 3^2 \times 49 = 2^3 \times 3^2 \times 7^2$.

HW07, Problem 4

Using the last two problems, compute by hand: $\phi(3528)$.

SOLUTION

We first FACTOR 3528. Since the last digit is even, 2 divides it. TRICK: since the last 2 digits, 28, is div by 4, its div by 4.

$3528 = 2^2 \times 882$. 882 is div by 2 so we get

$3528 = 2^3 \times 441$. Sum of digits of 441 is 9, so $441 \equiv 0 \pmod 9$.

$3528 = 2^3 \times 3^2 \times 49 = 2^3 \times 3^2 \times 7^2$.

$$\phi(2^3 3^2 7^2) = \phi(2^3)\phi(3^2)\phi(7^2) = (2^3 - 2^2)(3^2 - 3^1)(7^2 - 7^1)$$

$$= 4 \times 6 \times 42 = 1008$$

Point of the Problem

Its often said (correctly)

If Factoring is easy than RSA can be cracked.

Point of the Problem

Its often said (correctly)

If Factoring is easy than RSA can be cracked.

Recall that in RSA

$N = pq$ is public.

p, q are private.

$R = \phi(N) = (p-1)(q-1)$ is private.

e is public and rel prime to R.

d is private. Recall that $ed \equiv 1 \pmod{R}$.

Point of the Problem

Its often said (correctly)

If Factoring is easy than RSA can be cracked.

Recall that in RSA

$N = pq$ is public.

p, q are private.

$R = \phi(N) = (p-1)(q-1)$ is private.

e is public and rel prime to R.

d is private. Recall that $ed \equiv 1 \pmod{R}$.

If Eve knows d she can crack RSA.

Point of the Problem

Its often said (correctly)

If Factoring is easy than RSA can be cracked.

Recall that in RSA
$N = pq$ is public.
p, q are private.
$R = \phi(N) = (p-1)(q-1)$ is private.
e is public and rel prime to R.
d is private. Recall that $ed \equiv 1 \pmod{R}$.

If Eve knows d she can crack RSA.

We just showed that
Factoring easy $\Rightarrow \phi$ easy.

Point of the Problem

Its often said (correctly)

If Factoring is easy than RSA can be cracked.

Recall that in RSA

$N = pq$ is public.

p, q are private.

$R = \phi(N) = (p-1)(q-1)$ is private.

e is public and rel prime to R.

d is private. Recall that $ed \equiv 1 \pmod{R}$.

If Eve knows d she can crack RSA.

We just showed that

Factoring easy $\Rightarrow \phi$ easy.

Putting it all together we get

Factoring easy $\Rightarrow \phi$ easy $\Rightarrow$ inv mod R easy $\Rightarrow$ RSA cracked.

Point of the Problem

Its often said (correctly)

If Factoring is easy than RSA can be cracked.

Recall that in RSA
$N = pq$ is public.
p, q are private.
$R = \phi(N) = (p-1)(q-1)$ is private.
e is public and rel prime to R.
d is private. Recall that $ed \equiv 1 \pmod{R}$.

If Eve knows d she can crack RSA.

We just showed that
Factoring easy $\Rightarrow \phi$ easy.

Putting it all together we get
Factoring easy $\Rightarrow \phi$ easy $\Rightarrow$ inv mod R easy $\Rightarrow$ RSA cracked.

Proving converses of any of the above would be interesting.

Point of the Problem

Its often said (correctly)

If Factoring is easy than RSA can be cracked.

Recall that in RSA
$N = pq$ is public.
p, q are private.
$R = \phi(N) = (p-1)(q-1)$ is private.
e is public and rel prime to R.
d is private. Recall that $ed \equiv 1 \pmod{R}$.

If Eve knows d she can crack RSA.

We just showed that
Factoring easy $\Rightarrow \phi$ easy.

Putting it all together we get
Factoring easy $\Rightarrow \phi$ easy $\Rightarrow$ inv mod R easy $\Rightarrow$ RSA cracked.

Proving converses of any of the above would be interesting.

Next Slide has some possible futures!

RSA Might be Cracked Without Factoring

Possible futures:

RSA Might be Cracked Without Factoring

Possible futures:

1. Factoring easy! RSA is cracked!

RSA Might be Cracked Without Factoring

Possible futures:

1. Factoring easy! RSA is cracked!
2. Factoring hard; ϕ easy! RSA is cracked!

RSA Might be Cracked Without Factoring

Possible futures:

1. Factoring easy! RSA is cracked!
2. Factoring hard; ϕ easy! RSA is cracked!
3. Factoring hard; ϕ hard; The following easy:
   Given $N = pq$ (but not p, q) and e rel prime to
   $R = (p-1)(q-1)$ can find d such that $ed \equiv 1 \pmod{R}$.

RSA Might be Cracked Without Factoring

Possible futures:

1. Factoring easy! RSA is cracked!
2. Factoring hard; ϕ easy! RSA is cracked!
3. Factoring hard; ϕ hard; The following easy:
   Given $N = pq$ (but not p, q) and e rel prime to
   $R = (p-1)(q-1)$ can find d such that $ed \equiv 1 \pmod{R}$.
4. RSA remains uncracked.

HW07, Problem 5

For $(x, y) =$
$(0, 1), (1, 0), (0, 2), (1, 1), (2, 0), (0, 3), (1, 2), (2, 1), (3, 0), \ldots$

HW07, Problem 5

For $(x, y) =$
$(0,1),(1,0),(0,2),(1,1),(2,0),(0,3),(1,2),(2,1),(3,0),\ldots$

1. Compute $M = 2^x 3^y$.

HW07, Problem 5

For $(x, y) =$
$(0,1),(1,0),(0,2),(1,1),(2,0),(0,3),(1,2),(2,1),(3,0),\ldots$

1. Compute $M = 2^x 3^y$.
2. Compute $d = GCD(2^M - 1 \text{ mod } 143, 143)$. (The $\pmod{143}$ keeps the numbers small.)

HW07, Problem 5

For $(x, y) =$
$(0,1),(1,0),(0,2),(1,1),(2,0),(0,3),(1,2),(2,1),(3,0),\ldots$

1. Compute $M = 2^x 3^y$.
2. Compute $d = GCD(2^M - 1 \bmod 143, 143)$. (The $\pmod{143}$ keeps the numbers small.)
3. If $d \neq 1$ and $d \neq 143$ then output d (it will divide 143) and BREAK OUT of the for loop.

HW07, Problem 5, Solution

$(x, y) = (0, 1)$: $M = 2^0 \times 3^1 = 3$.
$d = GCD(2^3 - 1 \pmod{143}, 143) = GCD(7, 143) = 1$. Darn!

HW07, Problem 5, Solution

$(x, y) = (0, 1)$: $M = 2^0 \times 3^1 = 3$.
$d = GCD(2^3 - 1 \pmod{143}, 143) = GCD(7, 143) = 1$. Darn!

$(x, y) = (1, 0)$: $M = 2^1 \times 3^0 = 2$.
$d = GCD(2^2 - 1 \pmod{143}, 143) = GCD(3, 143) = 1$. Darn!

HW07, Problem 5, Solution

$(x, y) = (0, 1)$: $M = 2^0 \times 3^1 = 3$.
$d = GCD(2^3 - 1 \pmod{143}, 143) = GCD(7, 143) = 1$. Darn!

$(x, y) = (1, 0)$: $M = 2^1 \times 3^0 = 2$.
$d = GCD(2^2 - 1 \pmod{143}, 143) = GCD(3, 143) = 1$. Darn!

$(x, y) = (0, 2)$: $M = 2^0 \times 3^2 = 9$.
$d = GCD(2^9 - 1 \pmod{143}, 143) = GCD(83, 143) = 1$. Darn!

HW07, Problem 5, Solution

$(x, y) = (0, 1)$: $M = 2^0 \times 3^1 = 3$.
$d = GCD(2^3 - 1 \pmod{143}, 143) = GCD(7, 143) = 1$. Darn!

$(x, y) = (1, 0)$: $M = 2^1 \times 3^0 = 2$.
$d = GCD(2^2 - 1 \pmod{143}, 143) = GCD(3, 143) = 1$. Darn!

$(x, y) = (0, 2)$: $M = 2^0 \times 3^2 = 9$.
$d = GCD(2^9 - 1 \pmod{143}, 143) = GCD(83, 143) = 1$. Darn!

$(x, y) = (1, 1)$: $M = 2^1 \times 3^1 = 6$.
$d = GCD(2^6 - 1 \pmod{143}, 143) = GCD(63, 143) = 1$. Darn!

HW07, Problem 5, Solution

$(x, y) = (0, 1)$: $M = 2^0 \times 3^1 = 3$.
$d = GCD(2^3 - 1 \pmod{143}, 143) = GCD(7, 143) = 1$. Darn!

$(x, y) = (1, 0)$: $M = 2^1 \times 3^0 = 2$.
$d = GCD(2^2 - 1 \pmod{143}, 143) = GCD(3, 143) = 1$. Darn!

$(x, y) = (0, 2)$: $M = 2^0 \times 3^2 = 9$.
$d = GCD(2^9 - 1 \pmod{143}, 143) = GCD(83, 143) = 1$. Darn!

$(x, y) = (1, 1)$: $M = 2^1 \times 3^1 = 6$.
$d = GCD(2^6 - 1 \pmod{143}, 143) = GCD(63, 143) = 1$. Darn!

$(x, y) = (2, 0)$: $M = 2^2 \times 3^0 = 4$.
$d = GCD(2^4 - 1 \pmod{143}, 143) = GCD(15, 143) = 1$. Darn!

HW07, Problem 5, Solution. Cont

$(x, y) = (0, 3)$: $M = 2^0 \times 3^3 = 27$.
$d = GCD(2^{27} - 1 \pmod{143}, 143) = GCD(72, 143) = 1$. Darn!

HW07, Problem 5, Solution. Cont

$(x, y) = (0, 3)$: $M = 2^0 \times 3^3 = 27$.
$d = GCD(2^{27} - 1 \pmod{143}, 143) = GCD(72, 143) = 1$. Darn!

$(x, y) = (1, 2)$: $M = 2^1 \times 3^2 = 18$.
$d = GCD(2^{18} - 1 \pmod{143}, 143) = GCD(24, 143) = 1$. Darn!

HW07, Problem 5, Solution. Cont

$(x, y) = (0, 3)$: $M = 2^0 \times 3^3 = 27$.
$d = GCD(2^{27} - 1 \pmod{143}, 143) = GCD(72, 143) = 1$. Darn!

$(x, y) = (1, 2)$: $M = 2^1 \times 3^2 = 18$.
$d = GCD(2^{18} - 1 \pmod{143}, 143) = GCD(24, 143) = 1$. Darn!

$(x, y) = (2, 1)$: $M = 2^2 \times 3^1 = 12$.
$d = GCD(2^{12} - 1 \pmod{143}, 143) = GCD(91, 143) = 13$. Yeah!