Assignment #3 Solutions

January 24, 2006

Problem #1

Use Fermat's Little Theorem and induction on k to prove that

$$x^{k(p-1)+1} \bmod p = x \bmod p$$

for all primes p and $k \geq 0$.

Answer #1

By induction on k …

Base case $k = 0$:

$$x^{k(p-1)+1} \bmod p = x^{0+1} \bmod p = x \bmod p$$

Base case $k = 1$:

$$x^{k(p-1)+1} \bmod p = x^{(p-1)+1} \bmod p$$

$$= x^p \bmod p = x \bmod p$$

(by Fermat's Little Theorem)

Answer #1 (cont.)

Inductive step:

Assume that $x^{k(p-1)+1} \bmod p = x \bmod p$.

Prove that $x^{(k+1)(p-1)+1} \bmod p = x \bmod p$.

Answer #1 (cont.)

$$x^{(k+1)(p-1)+1} \bmod p$$

$$= x^{k(p-1)+(p-1)+1} \bmod p$$

$$= x^{k(p-1)+1+(p-1)} \bmod p$$

$$= x^{k(p-1)+1} x^{(p-1)} \bmod p$$

$$= x\, x^{(p-1)} \bmod p \text{ (by inductive hypothesis)}$$

$$= x^{p} \bmod p$$

$$= x^{p} \bmod p \text{ (by Fermat's Little Theorem)}$$

Problem #2

Show that for distinct primes p and q,

$$x \bmod p = y \bmod p$$

$$x \bmod q = y \bmod q$$

together imply that

$$x \bmod pq = y \bmod pq.$$

Answer #2

$x \bmod p = y \bmod p$

➔ $(x \bmod p) - (y \bmod p) = 0$

➔ $(x - y) \bmod p = 0$ (by first assignment)

➔ $(x - y)$ is a multiple of p.

Similarly $x \bmod q = y \bmod q$

➔ $(x - y)$ is a multiple of q.

Answer #2 (cont.)

Therefore, $(x - y)$ is a multiple of pq

- ➔ $(x - y) \bmod pq = 0$
- ➔ $(x \bmod pq) - (y \bmod pq) = 0$
- ➔ $x \bmod pq = y \bmod pq$.

Problem #3

Put everything together to prove that

$$x^{K(p-1)(q-1)+1} \bmod pq = x \bmod pq$$

For $K \geq 0$ and distinct primes p and q.

Answer #3

Let $k_1 = K(q-1)$ and $k_2 = K(p-1)$.

$$x^{K(p-1)(q-1)+1} \bmod p = x^{k_1(p-1)+1} \bmod p = x \bmod p$$

and

$$x^{K(p-1)(q-1)+1} \bmod q = x^{k_1(q-1)+1} \bmod q = x \bmod q$$

By Problem #1, and then by Problem #2

$$x^{K(p-1)(q-1)+1} \bmod pq = x \bmod pq.$$

Problem #4

$$E(x) = x^{43} \bmod 143$$

Find the inverse function

$$D(x) = x^{d} \bmod 143.$$

Answer #4

$$143 = 11 \times 13$$

We need to find d such that

$$43d \bmod (11-1)(13-1) = 1.$$

Use the Extended Euclidean Algorithm to find a solution to find x and y such that

$$120x + 43y = 1.$$

Extended Euclidean Algorithm

Given A,B > 0, set $x_1=1$, $x_2=0$, $y_1=0$, $y_2=1$,
$a_1=A$, $b_1=B$, $i=1$.

Repeat while $b_i>0$: {$i = i + 1$;
$q_i = a_{i-1}$ div b_{i-1}; $b_i = a_{i-1}-q_i b_{i-1}$; $a_i = b_{i-1}$;
$x_{i+1}=x_{i-1}-q_i x_i$; $y_{i+1}=y_{i-1}-q_i y_i$}.

For all i: $Ax_i + By_i = a_i$. Final $a_i = \gcd(A,B)$.

Answer #4 (cont.)

i	a_i	b_i	x_i	y_i	q_i
1	120	43	1	0	
			0	1	

Answer #4 (cont.)

i	a_i	b_i	x_i	y_i	q_i
1	120	43	1	0	
2	43	34	0	1	2
			1	-2	

Answer #4 (cont.)

i	a_i	b_i	x_i	y_i	q_i
1	120	43	1	0	
2	43	34	0	1	2
3	34	9	1	-2	
			-1	3	

Answer #4 (cont.)

i	a_i	b_i	x_i	y_i	q_i
1	120	43	1	0	
2	43	34	0	1	2
3	34	9	1	-2	1
4	9	7	-1	3	3
			4	-11	

Answer #4 (cont.)

i	a_i	b_i	x_i	y_i	q_i
1	120	43	1	0	
2	43	34	0	1	2
3	34	9	1	-2	1
4	9	7	-1	3	3
5	7	2	4	-11	1
			-5	14	

Answer #4 (cont.)

i	a_i	b_i	x_i	y_i	q_i
1	120	43	1	0	
2	43	34	0	1	2
3	34	9	1	-2	1
4	9	7	-1	3	3
5	7	2	4	-11	1
6	2	1	-5	14	3
			19	-53	

Answer #4 (cont.)

i	a_i	b_i	x_i	y_i	q_i
1	120	43	1	0	
2	43	34	0	1	2
3	34	9	1	-2	1
4	9	7	-1	3	3
5	7	2	4	-11	1
6	2	1	-5	14	3
7	1	0	19	-53	2
			-43	120	

Problem #5

Digital Signature Algorithm

Public parameters: $q = 11$, $p = 67$, $g = 9$, $y = 62$

Private secret: $x = 4$

Message to be signed: $M = 8$

Selected random parameter: $k = 2$

The Digital Signature Algorithm

To sign a 160-bit message M,

- Generate a random integer k with $0 < k < q$,
- Compute $r = (g^k \bmod p) \bmod q$,
- Compute $s = ((M+xr)/k) \bmod q$.

The pair (r,s) is the signature on M.

Answer #5

- $r = (g^k \bmod p) \bmod q$

  $= (9^2 \bmod 67) \bmod 11$

  $= (81 \bmod 67) \bmod 11 = 14 \bmod 11 = 3$
- $s = ((M+xr)/k) \bmod q$

  $= ((8+4\times3)/2) \bmod 11$

  $= (20/2) \bmod 11 = 10 \bmod 11 = 10$

The pair (3,10) is the signature on 8.

The Digital Signature Algorithm

A signature (r,s) on M is verified as follows:

- Compute $w = 1/s \bmod q$,
- Compute $a = w\mathrm{M} \bmod q$,
- Compute $b = wr \bmod q$,
- Compute $v = (g^a y^b \bmod p) \bmod q$.

Accept the signature only if $v = r$.

Answer #5 (cont.)

- $w = 1/s \bmod q = 1/10 \bmod 11 = 10$
- $a = w\mathrm{M} \bmod q = 10 \times 8 \bmod 11 = 3$
- $b = wr \bmod q = 10 \times 3 \bmod 11 = 8$
- $v = (9^3 \times 62^8 \bmod 67) \bmod 11$
  $= (59 \times 15 \bmod 67) \bmod 11$
  $= 14 \bmod 11 = 3$

$v = 3$ and $r = 3$ so the signature is validated.