Answers 7

Problem 1

According to Euler's generalization of Fermat's Little Theorem,

$a^{m\cdot(p-1)(q-1)+1} \bmod pq = a \bmod pq$ for all prime p and q.

For $q = 2$ and 1 $m = 1$,

$a^p \bmod p = a \bmod 2p$

compared with $a^p \bmod p = a \bmod p$ that we proved on p.4 of Lecture 7.

Problem 2

Assume that

$a^{m\cdot(p-1)(q-1)/2+1} \bmod pq = a \bmod pq$ for all prime p and q except 2.

For $q = 3$ and $m = 1$,

$a^p \bmod p = a \bmod 3p$

compared with $a^p \bmod p = a \bmod p$ that we proved on p.4 of Lecture 7.

Problem 3

For $p = 3$, $q = 5$, $a = 5$, and $m = 3$,

$n = m\cdot(p-1)(q-1)/2 + 1 = 13$, $pq = 15$.

$a^{n\cdot} = 1220703125$, $a^{n\cdot} \bmod 15 = 5 = a \bmod 15$.

For $p = 3$, $q = 5$, $a = 21$, and $m = 3$,

$n = m\cdot(p-1)(q-1)/2 + 1 = 13$, $pq = 15$.

$a^{n\cdot} = 154472377739119461$, $a^{n\cdot} \bmod 15 = 6 = a \bmod 15$.

For $p = 3$, $q = 5$, $a = 5$, and $m = 5$,

$n = m\cdot(p-1)(q-1)/2 + 1 = 21$, $pq = 15$.

$a^{n\cdot} = 476837158203125$, $a^{n\cdot} \bmod 15 = 5 = a \bmod 15$.

For $p = 3$, $q = 5$, $a = 8$, and $m = 7$,

$n = m\cdot(p-1)(q-1)/2 + 1 = 29$, $pq = 15$.

$a^{n\cdot} = 154742504910672534362390528$, $a^{n\cdot} \bmod 15 = 8 = a \bmod 15$.

Problem 4

For the case $p = 5$, $q = 13$, $a = 5$, and $m = 5$

$n = m\cdot(p-1)(q-1)/2 + 1 = 121$, $pq = 65$.

$a^{n\cdot} = 3.762 \times 10^{85}$.

$n = A \times B$, where $A = 11$ and $B = 11$.

$a^n \bmod 65 = a^{A\times B} \bmod 65 = [a^A \bmod 65]^B \bmod 65 = [5^{11} \bmod 65]^{11} \bmod 65$

$= [48828125 \bmod 65]^{11} \bmod 65 = 60^{11} \bmod 65$

$= 362797056000000000000 \bmod 65 = 5 = a \bmod 65$

Problem 5

For the case $p = 3$, $q = 5$, $a = 5$, and $m = 5$,

$n = m\cdot(p - 1)(q - 1)/2 + 1 = 21$, $pq = 15$.

$a^{n\cdot} = 476837158203125$, $a^{n\cdot} \bmod 15 = 5 = a \bmod 15$.

Or:

$n = A\times B$, where $A = 3$ and $B = 7$.

$a^n \bmod 15 = a^{A\times B} \bmod 15 = [a^A \bmod 15]^B \bmod 15 = [5^3 \bmod 15]^7 \bmod 15$

$= [125 \bmod 15]^7 \bmod 15 = 5^7 \bmod 15 = 78125 \bmod 15 = 5 = a \bmod 15$