Assignment #2 – Solutions
Problem 1

\[ x \mod 7 = \pm 1 \text{ and } x \mod 11 = \pm 1 \]

(Note: \( x \mod N = -1 \) is shorthand for \( x \mod N = N - 1 \).)

\[ 11^{-1} \mod 7 = 2 \quad 7^{-1} \mod 11 = 8 \]

Four solutions

\[ \begin{align*}
x &= [(+1) \times 11 \times 2 + (+1) \times 7 \times 8] \mod 77 = [+22 + 56] \mod 77 = +78 \mod 77 = 1 \\
x &= [(+1) \times 11 \times 2 + (-1) \times 7 \times 8] \mod 77 = [+22 - 56] \mod 77 = -34 \mod 77 = 43 \\
x &= [(-1) \times 11 \times 2 + (+1) \times 7 \times 8] \mod 77 = [-22 + 56] \mod 77 = +34 \mod 77 = 34 \\
x &= [(-1) \times 11 \times 2 + (-1) \times 7 \times 8] \mod 77 = [-22 - 56] \mod 77 = -78 \mod 77 = 76
\]
Problem 2

- Given $N = pq$,
  select a random $y$,
  compute $z = y^2 \mod N$,
  and input $z$ and $N$ to the black box to produce output $x$.
- If $x \pm y \mod N = 0$, repeat above.
- Otherwise, compute $\gcd(x - y, N)$ to produce a non-trivial factor of $N$. 
Problem 2 – Bonus

- Remove all powers of 2 from $N = 2^m N'$. 
- Repeatedly use black box to split $N'$ into prime powers $P = p^k$. 
- For each non-prime prime power, try each of $i = 2, 3, \ldots, \log_2 P$ until an $i$ is found such that the $i^{th}$ root of $P$ is prime.
Problem 3

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

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

for all primes $p$ and $k \geq 0$. 
Problem 3 (cont.)

By induction on $k$ ...

Base case $k = 0$:

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

Base case $k = 1$:

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

$$= x^p \mod p = x \mod p$$

(by Fermat’s Little Theorem)
Problem 3 (cont.)

Inductive step:

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

Prove that $x^{(k+1)(p-1)+1} \mod p = x \mod p$. 
Problem 3 (cont.)

\[ x^{(k+1)(p-1)+1} \mod p \]

\[ = x^{k(p-1)+(p-1)+1} \mod p \]

\[ = x^{k(p-1)+1+(p-1)} \mod p \]

\[ = x^{k(p-1)+1} x^{(p-1)} \mod p \]

\[ = x \cdot x^{(p-1)} \mod p \quad \text{(by inductive hypothesis)} \]

\[ = x^p \mod p \]

\[ = x \mod p \quad \text{(by Fermat’s Little Theorem)} \]
Problem 4

Show that for distinct primes $p$ and $q$,

$$x \mod p = y \mod p$$

$$x \mod q = y \mod q$$

together imply that

$$x \mod pq = y \mod pq.$$
Problem 4

\[ x \mod p = y \mod p \]
\[ \Rightarrow (x \mod p) - (y \mod p) = 0 \]
\[ \Rightarrow (x - y) \text{ is a multiple of } p. \]

Similarly \[ x \mod q = y \mod q \]
\[ \Rightarrow (x - y) \text{ is a multiple of } q. \]
Problem 4

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

\[\Rightarrow (x - y) \mod pq = 0\]

\[\Rightarrow (x \mod pq) - (y \mod pq) = 0\]

\[\Rightarrow x \mod pq = y \mod pq.\]
Problem 5

Put problems 3 and 4 together to prove that

\[ x^{K(p-1)(q-1)+1} \mod pq = x \mod pq \]

For \( K \geq 0 \) and distinct primes \( p \) and \( q \).
Problem 5 (cont.)

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

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

and

$x^{K(p-1)(q-1)+1} \mod q = x^{k_2(q-1)} \mod q = x \mod q$

By Problem #1, and then by Problem #2

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

\[\frac{1}{20/2011}\]