Assignment #2 – Solutions

Problem 1

$x \bmod 7 = \pm 1$ and $x \bmod 11 = \pm 1$

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

$11^{-1} \bmod 7 = 2$ $\quad\quad$ $7^{-1} \bmod 11 = 8$

<u>Four solutions</u>

$x = [(+1) \times 11 \times 2 \ + (+1) \times 7 \times 8] \bmod 77 = [+22 + 56] \bmod 77 = +78 \bmod 77 = 1$

$x = [(+1) \times 11 \times 2 \ + (-1) \times 7 \times 8] \bmod 77 = [+22 - 56] \bmod 77 = -34 \bmod 77 = 43$

$x = [(-1) \times 11 \times 2 \ + (+1) \times 7 \times 8] \bmod 77 = [-22 + 56] \bmod 77 = +34 \bmod 77 = 34$

$x = [(-1) \times 11 \times 2 \ + (-1) \times 7 \times 8] \bmod 77 = [-22 - 56] \bmod 77 = -78 \bmod 77 = 76$

Problem 2

- Given $N = pq$,
  select a random y,
  compute $z = y^2 \bmod N$,
  and input z and N to the black box to produce output x.
- If $x \pm y \bmod N = 0$, 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

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

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

Problem 3 (cont.)

By induction on k …

Base case $k = 0$:

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

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)

Problem 3 (cont.)

Inductive step:

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

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

Problem 3 (cont.)

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

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

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

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

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

$= x^{p} \bmod p$

$= x \bmod p$ (by Fermat's Little Theorem)

Problem 4

Show that for distinct primes p and q,

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

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

together imply that

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

Problem 4

$x \bmod p = y \bmod p$

$\Rightarrow (x \bmod p) - (y \bmod p) = 0$

$\Rightarrow (x - y)$ is a multiple of p.

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

$\Rightarrow (x - y)$ is a multiple of q.

Problem 4

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

$\Rightarrow (x - y) \bmod pq = 0$

$\Rightarrow (x \bmod pq) - (y \bmod pq) = 0$

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

Problem 5

Put problems 3 and 4 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.

Problem 5 (cont.)

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

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

and

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

By Problem #1, and then by Problem #2

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