Assignment 29

Alex Clemmer
Student number: u0458675

1

Transforming $x^p \equiv x (\text{mod } p)$ into a more familiar format is really simple. We start with prime identity given by the book, $x^{p-1} \equiv 1 (\text{mod } p)$. Multiplying both sides by x, we get $x^p \equiv x (\text{mod } p)$. We know that we can do this because x is obviously relatively prime to x.

2

Transforming some $x^{k(p-1)+1} \equiv x (\text{mod } p)$ also begins with the familiar identity that $x^{p-1} \equiv 1 (\text{mod } p)$. By raising both sides to the power of k we get $x^{k(p-1)} \equiv 1 (\text{mod } p)$. Remember that this is intuitively satisfying because we mod intuitively at every point we multiply a number by itself when raising it to some power. So if a number is congruent mod p, it should be congruent for all powers k that it is raised to.

There's no black magic in the last step: we simply multiply both sides by x. This gives us our final solution, $x^{k(p-1)+1} \equiv x (\text{mod } p)$.

3

e and $p-1$ are relatively prime, so we can use Extended Euclid's algorithm to give $fe+b(p-1) = 1$. Mod-ing both sides by $p-1$ gives us $fe \equiv 1 (\text{mod } p-1)$.

4

For some message y in $y \equiv x^e (\text{mod } p)$: we've found f in the previous part, so our equivalence relation becomes $y^f \equiv x^{ef} (\text{mod } p)$. The totient function $\phi(p) = p-1$, so by Euler's we can $y^f \equiv x^{ef (\text{mod } p-1)} (\text{mod } p)$, which is then $y^f \equiv x (\text{mod } p)$.

Decrypting is simple: find f then use $x \equiv y^f (\text{mod } p)$.