Appendix 3
Modular arithmetic for Cryptography Masterclass

A. G. Curnock

April 2009

We have already noticed that "$7 = 2 \mod 5$" means that we may subtract integer multiples of 5 from 7 and arrive at an integer between 0 and 5. So if we divide 7 by 5, 2 is the remainder. This gives us a general definition.

Definition 0.1. We write $a \equiv b \mod n$ to mean b is the remainder after dividing a by n. We say $a \equiv b \mod n$ means"a is congruent to b mod n." In effect this means $b - a$ is divisible by n, or $\frac{b-a}{n}$ is an integer.

Understanding how to solve equations using modular arithmetic will be important in cryptography.

Now if we consider $7 \equiv 2 \mod 5$ and $25 \equiv 0 \mod 5$. Now we can add these two types of equations and arrive at $32 = 2 \mod 5$. This is true but we should prove it so that we know this works for all values.

Proposition 0.2. *If* $a_1 \equiv b_1 \mod n$ *and* $a_2 \equiv b_2 \mod n$ *then we have the following*

- $(a_1 \pm a_2) \equiv (b_1 \pm b_2) \mod n$;
- $(a_1 a_2 \equiv (b_1 b_2) \mod n$.

Proof. Firstly let's write each modular expression in our hypothesis as an equation using the definition. Thus

$$\begin{aligned} a_1 &\equiv b_1 \mod n \quad \text{is the same as} \quad b_1 - a_1 = jn \\ a_2 &\equiv b_2 \mod n \quad \text{is the same as} \quad b_2 - a_2 = kn, \end{aligned} \tag{0.1}$$

where j, k are integers.

We may add these two equations which results in

$$b_1 - a_1 + b_2 - a_2 = \ell n$$

with ℓ an integer. Re-arranging this gives us $(b_1 + b_2) - (a_1 + a_2) = \ell n$ which our definition tells us can be written as $(a_1 + a_2) \equiv (b_1 + b_2) \mod n$. Similarly subtracting the two equations in 0.1 we will have proved $(a_1 - a_2) \equiv (b_1 - b_2) \mod n$. Thus if our hypothesis is true, we've proved the first conclusion is true. The second result is easily proved as follows, but it's worth writing out once. We need to arrive at $b_2 b_1 - a_1 a_2 = k' n$ where k' is an integer. Reading the definitions of the two modular equations in our hypothesis, let's multiply these : $(b_1 - a_1)(b_2 - a_2) = k'' n$ where k'' is an integer. (Write out exactly what k'' is if you think this is false, noting that any term with an n in it is a multiple of n, so these can be combined.) Simplifying this we have $b_1 b_2 + a_1 a_2 - a_1 b_2 - b_1 a_2 = k'' n$.

We don't want to affect the first two terms as we know we need these in our answer. Let's try and remove the third and fourth terms. Substitute $b_2 = a_2 + kn$ and $b_1 = a_1 + jn$ in the third and fourth terms. Thus

$$b_1 b_2 + a_1 a_2 - a_1(a_2 + kn) - (a_1 + jn)a_2 = k'' n,$$

which simplifies to

$$b_1 b_2 - a_1 a_2 = n(a_1 k + a_2 j)$$

which is our required result

$$b_1 b_2 - a_1 a_2 + k' n,$$

where k' is some integer. □

Numerous computational examples e.g. finding multiplicative inverses were also discussed.