Problem 1. Find all solutions to the polynomial congruence $x^3 - 4x^2 - 2x - 83 \equiv 0 \pmod{1183}$. (Hint: you will need to use Hensel’s lemma on one of the smaller congruences that you get by breaking apart this big one. Once you solve the smaller congruences, you can crank on the Chinese remainder theorem in the usual way.)

Problem 2. Say how many solutions there are to the congruence $x^2 + x + 1 \equiv 0 \pmod{7^{100}13^{100}}$. Do not look for actual solutions. The point is that huge scary moduli are not necessarily scary.

Problem 3. This problem is about counting the number of integers in $1, \ldots, n$ that are coprime to some given integer $n$. This number is usually written $\phi(n)$. It doesn’t look at first like a CRT problem but really it is.

(a) If $n$ is a prime then you already know that $\phi(n) = n - 1$. Work out $\phi(n)$ when $n = p^e$ where $p$ is a prime and $e$ is an integer $> 1$.

(b) $\phi(n)$ is the number of elements of $\mathbb{Z}_n$ which have a multiplicative inverse.

(c) This is the same as the number of solutions $(x, y)$ to the polynomial equation $xy - 1 = 0$ where $x, y$ vary over the number system $\mathbb{Z}_n$.

(d) if $n’s$ prime factorization is $p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$ then $\phi(n) = \phi(p_1^{e_1})\phi(p_2^{e_2})\cdots \phi(p_k^{e_k})$.

(e) combine this with (a) to compute $\phi(10,000)$ and $\phi(196,560)$.

Problem 4. Sometimes one meets systems of congruences where the moduli are not pairwise coprime. Then there might or might not be a solution, and this problem is about how to recognize when there is. It is not the most general possible result, but is meaty enough to give a taste of the general result.

Suppose $p$ and $q$ are primes, $a, b, c, d$ are positive integers, and $Y, Z$ are integers, and consider the system of congruences

$$x \equiv Y \pmod{p^aq^b}$$
$$x \equiv Z \pmod{p^cq^d}$$

You can suppose $a \leq c$ and $b \geq d$, which is the meatiest case.

(a) give a specific example showing that there might not be a solution.

(b) rewrite the system of congruences as an equivalent system (means: having the same set of solutions) of four congruences, mod $p^a$, $q^b$, $p^c$ and $q^d$.

(c) find a condition of the following general form, which must be satisfied for a solution $x$ to exist: $Z$ satisfies a certain congruence and $Y$ satisfies a certain other congruence.

(d) show that if your congruences in (c) hold then a solution $x$ is guaranteed to exist, and is unique modulo $p^aq^b$. 