MAS114 Homework Solutions

Week 9 (hand in in week 10)

1. Solve the following simultaneous congruence equations:

   (a) $x \equiv 5 \pmod 7$, $\quad x \equiv 2 \pmod 6$;

   (b) $x \equiv 5 \pmod 8$, $\quad x \equiv 2 \pmod 6$;

   (c) $x \equiv 5 \pmod 9$, $\quad x \equiv 2 \pmod 6$;

   (d) $x \equiv 17 \pmod{41}$, $\quad x \equiv 36 \pmod{43}$.

   Solution

   (a) The Chinese Remainder Theorem says that it is the same as some class modulo 42. In fact $x \equiv 26 \pmod{42}$.

   (b) No solution exists: one equation says that x is even, and the other that x is odd.

   (c) It can be found (by experimentation, for example), that $x \equiv 14 \pmod{18}$ is the general solution.

   (d) We find that $x = 41m+17$ and $x = 43n+36$. Hence, by identifying these and simplifying, $41m-43n = 19$. The usual techniques solve this for us to get a solution $n = 12$, $m = 11$.

   Hence, by the Chinese Remainder Theorem, we have one solution mod $41 \times 43 = 1763$, and that's $x = 41 \times 12 + 17 = 509$: the solution is $x \equiv 509 \pmod{1763}$.

2. Show that $17 \mid (3^{32} - 2^{32})$ using Fermat's Little Theorem.

Solution Fermat's Little Theorem gives us that

$$3^{32} - 2^{32} = 3^{16}3^{16} - 2^{16}2^{16} \equiv 1 \cdot 1 - 1 \cdot 1 = 0 \pmod{17}.$$

3. **Challenge:**

   (i) Show that 561 is not prime.

   (ii) Show that, even though 561 is not prime, if $\gcd(a, 561) = 1$, then $a^{560} \equiv 1 \pmod{561}$.

   This shows that one possible converse of Fermat's Little Theorem is not true. Numbers with this property, of being composite but "apparently prime" from the point of view of Fermat's Little Theorem, are called Carmichael numbers*.*

   [*Please hand in attempts to the Challenge problem on a separate sheet of paper so they can make their way to Dr Cranch more easily.*]