Extra problem sheet - some solutions

(Sorry about the mess, this was supposed to be part of a video, so not stand-alone!)

1. Find solutions (if they exist!) to each of the following congruences.
   (a) $2x \equiv 1 \mod 3$.
   (b) $2x \equiv 5 \mod 7$.
   (c) $2x \equiv 5 \mod 8$.
   (d) $3x \equiv 4 \mod 8$.
   (e) $6x \equiv 3 \mod 15$.
   (f) $6x \equiv 7 \mod 15$.
   (g) $8x \equiv 7 \mod 18$.
   (h) $7x \equiv 4 \mod 54$.
   (i) $51x \equiv 3 \mod 128$.
   (j) $9x + 23 \equiv 28 \mod 25$.

1a) Sol'n I Trial and error.

$2x \equiv 1 \mod 3$ means $2x = 1 +$ some multiple of 3.

Try adding multiples of 3 until we find one that is divisible by 2 (even):

$1+0=1,\ 1+3=4,\ 1+6=7,\ 1+9=10, \dots$

so let $x = 4 \div 2 = 2$. Check: works ✓

Sol'n II Euclidean Algorithm:

$3 = 2\cdot 1 + 1$

$2 = 1 \cdot 2 + 0$

so GCF = 1 (we knew that!)

$1 = 3 - 2\cdot 1 = 1\cdot 3 + (-1)\cdot 2$

So $x = -1$ works. However, it is not a residue (not >0) so let's add 3 to it; $3 + -1 = 2$, so take $x = 2$.

1c) Try the same approach as Sol'n I in last example. Add multiples of 8 to 5 until we find one that is divisible by 2:

$5+0=5,\ 5+8=13,\ 5+16=21,\ 5+24=29,\ 5+32=37 \dots$ not working! Why not? Note $GCF(2,8)=2$, and $2 \nmid 5$, so no solution exists. (If we'd noticed that at the beginning, it would have made the problem easier!)

One more example, not from this list:

Solve $18x \equiv 4 \mod 26$

We could try adding multiples of 26 to 4 and see if we get a multiple of 18! $4, 30, 56, 82, \dots$ Can you recognize a multiple of 18? I can't...

Let's use the Euclidean Algorithm:

$26 = 18\cdot 1 + 8$

$18 = 8 \cdot 2 + 6$

$8 = 6\cdot 1 + 2$

$6 = 2 \cdot 3 + 0$

So $GCF(26,18) = 2$. Moreover,

$2 = 8 - 6\cdot 1$ (now get rid of 6)

$= 8 - (18 - 8\cdot 2)$ (regroup)

$= 3\cdot 8 - 18$ (get rid of 8)

$= 3\cdot(26 - 18\cdot 1) - 18$ (regroup)

$= \underbrace{3\cdot 26}_{\text{divisible by 26}} - 4\cdot 18$

so $18\cdot(-4) \equiv 2 \mod 26$

this isn't 4

this is negative

so add 26 to the -4, multiply by 2

$18\cdot(22) \equiv 2 \mod 26$

$18 \cdot 44 \equiv 4 \mod 26$

While $x = 44$ is an OK answer, better to have the residue mod 26, so take $x = 44 - 26 = 18$.

Let's check that it works:

$18 \cdot 18 \bmod 26 = 9 \cdot 36 \bmod 26 = 9 \cdot 10 \bmod 26 = 90 \bmod 26$
$= 18$ (since $90 - 26 \cdot 3 = 18$) ✓ whew!

2. $3^{302} \mod 5 =?$
3. $3^{302} \mod 7 =?$
4. $3^{302} \mod 11 =?$
5. What is the remainder after dividing 3^{50} by 7?
6. What is the remainder after dividing 2^{63} by 61?

Note these are just like #2-4 (why?)

7. Does $10|(101^{2015} - 1)$?
8. Suppose a is not divisible by 23. Find $a^{154} \mod 23$.
9. True or False:
   (a) For any integer $a, a^5 - a$ is divisible by 30.
   (b) For any integer $a, a^{11} - a$ is divisible by 66.

3

$\underbrace{3}_{a}^{302} \bmod \underbrace{7}_{p} = ?$ FLT tells us that $a^{p-1} \equiv 1 \bmod p$, or $3^6 \equiv 1 \bmod 7$.

Note $302 = 300 + 2 = 6 \cdot 50 + 2$, so

$3^{302} \bmod 7 \equiv 3^{300} \cdot 9 \bmod 7$
$\equiv (3^6)^{50} \cdot 9 \bmod 7 \equiv 1^{50} \cdot 9 \bmod 7$
$\equiv 9 \bmod 7 = 2$. done!

Let's do #7.

Is $101^{2015} - 1$ divisible by 10? One sol'n: If you start multiplying 101 by itself, every time (even after 2015 times!) it looks like $\boxed{\text{stuff}}1$, so $101^{2015} - 1 = \boxed{\text{stuff}}0$, which is divisible by 10!

Here's another sol'n:

Since $10 = 2 \cdot 5$, we'll check divisibility by 2 & 5.

$101^{2015} \bmod 2 \equiv 1^{2015} \bmod 2 \equiv 1 \bmod 2$ (since $101 \equiv 1 \bmod 2$)

so $101^{2015} - 1 \equiv 0 \bmod 2$, or $2 \mid 101^{2015} - 1$

$101^{2015} \bmod 5 \equiv 1^{2015} \bmod 5$ (since $101 \equiv 1 \bmod 5$)

$\equiv 1 \bmod 5$, so $5 \mid 101^{2015} - 1$

Since both $2 \mid 101^{2015} - 1$ and $5 \mid 101^{2015} - 1$, we must have $10 \mid 101^{2015} - 1$.