

Some extra problems: Solving ‘modulo’ equations and using Fermat’s Little Theorem

These are extra problems. Some require the Euclidean Algorithm, the others use Fermat’s Little Theorem. You will probably want to review the lecture notes on RSA before doing them, as well as the posted notes/video on solving $ex \equiv b \pmod{m}$. (Recall that Fermat’s Little Theorem says that if p is a prime and a is not divisible by p then $a^p \equiv a \pmod{p}$, which is the same thing as saying $a^{p-1} \equiv 1 \pmod{p}$.)

These are NOT to be turned in. I will post answers to *some* of these in a day or two. *Some* of the others will be on a MML-based homework assignment. A few homework problems like these WILL be in the next exam; you should try all of them!

1. Find solutions (if they exist!) to each of the following congruences.

- (a) $2x \equiv 1 \pmod{3}$.
- (b) $2x \equiv 5 \pmod{7}$.
- (c) $2x \equiv 5 \pmod{8}$.
- (d) $3x \equiv 4 \pmod{8}$.
- (e) $6x \equiv 3 \pmod{15}$.
- (f) $6x \equiv 7 \pmod{15}$.
- (g) $8x \equiv 7 \pmod{18}$.
- (h) $7x \equiv 4 \pmod{54}$.
- (i) $51x \equiv 3 \pmod{128}$.
- (j) $9x + 23 \equiv 28 \pmod{25}$.

2. $3^{302} \pmod{5} = ?$

3. $3^{302} \pmod{7} = ?$

4. $3^{302} \pmod{11} = ?$

5. What is the remainder after dividing 3^{50} by 7?

6. What is the remainder after dividing 2^{63} by 61?

7. Does $10 \mid (101^{2015} - 1)$?

8. Suppose a is not divisible by 23. Find $a^{154} \pmod{23}$.

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.