Spring 2024

18.200 Homework 6

Instructions: Include a list of your **collaborators** or state that you worked on your own.

1. Consider Euclid's algorithm to compute the gcd of $x_0 = a$ and $x_1 = b$ (with $x_0 \geq x_1$). The algorithm starts by computing $x_2 = x_0 \pmod{x_1}$ and then $x_3 = x_1 \pmod{x_2}$ and so on. Prove that for all $k \geq 1$

$$x_{2k} + x_{2k+1} \leq \frac{1}{2^k}(a+b).$$

   Hence show that the algorithm stops after no more than $2\log_2(a+b)+1$ steps. (Very reasonable, isn't it!)

2. Does 375 have a multiplicative inverse modulo 1024? If so, find it. Does 628? If so, find it.

3. Find all integer solutions to

$$x \equiv 5 \pmod{15}$$
$$x \equiv 11 \pmod{26}$$
$$x \equiv 7 \pmod{77}$$

4. (a) Consider a prime p, and assume that k is such that $gcd(k, p-1) = 1$. Prove that the only solution to $x^k \equiv 1 \pmod{p}$ is $x \equiv 1 \pmod{p}$. (Think about Fermat's little theorem and what the gcd implies...)

   (b) Give one solution of

$$x^3 \equiv 1 \mod 3599,$$

   different than $x \equiv 1 \mod 3599$. (Notice that 3599 is a composite number...) (If you'd like to explore, you could look at the number of solutions of this modular equation.)

5. Prove that for a prime p,

$$(p-1)! \equiv -1 \pmod{p}.$$

MIT OpenCourseWare
https://ocw.mit.edu

18.200 Principles of Discrete Applied Mathematics
Spring 2024

For information about citing these materials or our Terms of Use, visit: https://ocw.mit.edu/terms.