

due-01-22

William Stein

1/13/2014

Contents

1 Homework 1 Due Jan 22, 2014	1
1.1 Instructions	1
1.2 Problems	1
1.2.1 Problem 1: a gcd by hand	1
1.2.2 Problem 2: a conjecture about primes	1
1.2.3 Problem 3: prove something about gcds.	2
1.2.4 Problem 4: prove something about squares	2
1.2.5 Problem 5: compute the first few digits of a huge Mersenne prime	2
1.2.6 Problem 6: extended Euclidean algorithm	2
1.2.7 Problem 7: your project	2

1 Homework 1 Due Jan 22, 2014

1.1 Instructions

- Put your solutions in the empty space below the problem.
- Create a new cell by clicking on the horizontal cell dividers.
- If you put
 - If you then press shift-enter youll see the rendered math.
 - If you double click on the output then you can edit the input again.
 - This uses Markdown format, which you can learn about here: <http://daringfireball.net/projects/markdown/>
- Put this worksheet in a folder called homework in your project.
- For this first assignment, when youre done, open the worksheet, and copy/paste the URL into an email to wstein@gmail.com with the subject math 480: homework 01-22. (Later Ill automate this.)

1.2 Problems

1.2.1 Problem 1: a gcd by hand

Compute the greatest common divisor $\gcd(455, 1235)$ by hand.

1.2.2 Problem 2: a conjecture about primes

Let $\pi(x)$ be the number of primes $\leq x$ and let $\psi(x)$ be the number of primes of the form $4k-1$ that are $\leq x$.

1. Make a conjectural guess based on data about $\lim_{x \rightarrow \infty} \psi(x)/\pi(x)$. State your guess precisely and give evidence.
2. Search around in books or the internet for theorems, and use any of them to either prove or disprove your guess.

1.2.3 Problem 3: prove something about gcds.

Let a, b, c, n be integers. Prove that

1. if $a \mid n$ and $b \mid n$ with $\gcd(a, b) = 1$, then $ab \mid n$.
2. if $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

1.2.4 Problem 4: prove something about squares

Prove that if a positive integer n is a perfect square, then n cannot be written in the form $4k+3$ for k an integer.

(Hint: Compute the remainder upon division by 4 of each of $(4m)^2$, $(4m+1)^2$, $(4m+2)^2$, and $(4m+3)^2$.)

1.2.5 Problem 5: compute the first few digits of a huge Mersenne prime

How can you efficiently compute the first few digits of $p = 2^{57885161} - 1$ efficiently (i.e., in less than a second)?
(HINT: do not use modular arithmetic.)

1.2.6 Problem 6: extended Euclidean algorithm

- Find integers x and y such that $2014x + 480y = 2$.
- Are there integers x and y such that $2014x + 480y = 3$?

1.2.7 Problem 7: your project

List three ideas for topics that you could do a project about. Look for inspiration in the following sources:

- the course textbook, and other number theory books
- past projects <http://wstein.org/courses/>
- search for number theory topics online
- any past experience you have in number theory.

Try to find topics that you are personally very curious about.