Homework #4

MATH 311 — Intro to Number Theory
due in class on Tuesday, Oct 11

Please print your name:

These problems are not suited to be done last minute!
Also, if you start early, you can consult with me if you should get stuck.

Problem 1.

(a) Show that $111^{333}+333^{111}$ is divisible by 7.

(b) Show that $2^{48}-1$ is divisible by 97.

(c) Show that $13|3^{n+2}+4^{2n+1}$, for all integers $n \geqslant 0$.

(d) Show that $43|6^{n+2}+7^{2n+1}$, for all integers $n \geqslant 0$.

Problem 2.

(a) Determine all x modulo 15 such that $x^2 \equiv 1 \pmod{15}$. [There should be four values in $\{0,1,2,...,14\}$.]

(b) Determine all x modulo 13 such that $x^2 \equiv 1 \pmod{13}$. [There should be two values in $\{0,1,2,...,12\}$.]

(c) Let p be a prime, and let x be an integer such that $x^2 \equiv 1 \pmod{p}$. Show that $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.

Hint. Note that $x^2 \equiv 1 \pmod{p}$ is equivalent to $p|x^2-1$. Factor x^2-1. Then, ...

Moral. Working with real numbers, we know that the equation $x^2=1$ has exactly two solutions (namely, $x=1$ and $x=-1$). When working with congruences modulo n, there can be additional solutions! (As the example modulo 15 shows.) However, when working with congruences modulo primes, we are back in the situation that there exist precisely the solutions $x=\pm 1$.

Problem 3.

(a) Express 53 in base 2.

(b) Express 1234 in base 2.

(c) Using binary exponentiation, compute $19^{53} \pmod{503}$.

Problem 4. The International Standard Book Number ISBN-10 consists of nine digits $a_1a_2...a_9$ followed by a tenth check digit a_{10} (the symbol X is used if the digit equals 10), which satisfies

$$a_{10} \equiv \sum_{k=1}^{9} k a_k \pmod{11}.$$

(a) The ISBN 007338314-? is missing the check digit (printed as "?"). Compute it!

(b) Confirm that the ISBN 052547883-7 is incorrect. You believe that the error lies in the ninth digit, the "3". Assuming this is true, what should the ninth digit be changed to to get a correct ISBN?

Advertisement. The ISBN scheme allows everyone to test the correctness of an ISBN. However, as you noticed in the second part, everyone can also create a (possibly fake) ISBN. For some applications, it is necessary that everyone can verify the correctness (with much more certainty than the single check digit provides) but only one authority can issue such numbers (in other words, you would not be able to correct an incorrect number, or fake a new one). Principles of cryptography make that possible!

Armin Straub
straub@southalabama.edu