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 $n \geqslant 0$.

Solution.

(a) For starters, we observe that $111^{333}+333^{111} \equiv (-1)^{333}+4^{111} = -1+4^{111} \pmod 7$. Next, since 7 is a prime, Fermat's little theorem predicts that $4^6 \equiv 1 \pmod 7$. This means that we can reduce the exponent 111 modulo 6 ($111 \equiv 3 \pmod 6$). Indeed,

$$4^{111} = (4^6)^{18} \cdot 4^3 \equiv 4^3 = 64 \equiv 1 \pmod 7.$$

Combined, $111^{333}+333^{111} \equiv -1+4^{111} \equiv -1+1 = 0 \pmod 7$, which shows that $111^{333}+333^{111}$ is divisible by 7.

(b) We use binary exponentiation. Note that $48 = 32+16$. Modulo 97, we have

$$2^2 = 4, \quad 2^4 = 16, \quad 2^8 = 16^2 \equiv -35, \quad 2^{16} \equiv (-35)^2 \equiv -36, \quad 2^{32} \equiv (-36)^2 \equiv 35.$$

Hence,

$$2^{48} = 2^{32} \cdot 2^{16} \equiv 35 \cdot (-36) \equiv 1 \pmod{97}.$$

In other words, 97 divides $2^{48}-1$.

Comment. It may be tempting to apply Fermat's little theorem. Since 97 is a prime, it implies that $2^{96} \equiv 1 \pmod{97}$. So, if we write $x = 2^{48}$, then $x^2 \equiv 1 \pmod{97}$. By the last part of the next problem, this allows us to conclude that $x \equiv 1 \pmod{97}$ or $x \equiv -1 \pmod{97}$. However, without further work, we cannot decide which of these cases is true.

Tricky alternative. However, we can apply Fermat's little theorem if we realize (this is the tricky part) that $2 \equiv 14^2 \pmod{97}$. It then follows that $2^{48} \equiv 14^{96} \equiv 1 \pmod{97}$.

(c) $3^{n+2}+4^{2n+1} = 9 \cdot 3^n + 4 \cdot 16^n \equiv 9 \cdot 3^n + 4 \cdot 3^n = 13 \cdot 3^n \equiv 0 \pmod{13}$.

In other words, 13 divides $3^{n+2}+4^{2n+1}$.

(d) $6^{n+2}+7^{2n+1} = 36 \cdot 6^n + 7 \cdot 49^n \equiv 36 \cdot 6^n + 7 \cdot 6^n = 43 \cdot 6^n \equiv 0 \pmod{43}$.

In other words, 43 divides $6^{n+2}+7^{2n+1}$. □

Problem 2.

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

Armin Straub
straub@southalabama.edu

(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 $x = \pm 1$.

Solution.

(a) We compute all squares modulo 15: $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 9$, $4^2 \equiv 1$, $5^2 \equiv 10$, $6^2 \equiv 6$, $7^2 \equiv 4$, $8^2 \equiv 4$, $9^2 \equiv 6$, $10^2 \equiv 10$, $11^2 \equiv 1$, $12^2 \equiv 9$, $13^2 \equiv 4$, $14^2 \equiv 1$. Hence, $x^2 \equiv 1 \pmod{15}$ if and only if x is congruent to one of $1, 4, 11, 14$.

Important comments. Note that the values of the squares repeat themselves backwards. That's because instead of $\{0, 1, 2, ..., 14\}$ it would have been more natural to use the (equally complete) set of residues $\{0, \pm 1, \pm 2, ..., \pm 7\}$. Then, we only need to compute that, all modulo 15: $0^2 \equiv 0$, $(\pm 1)^2 \equiv 1$, $(\pm 2)^2 \equiv 4$, $(\pm 3)^2 \equiv -6$, $(\pm 4)^2 \equiv 1$, $(\pm 5)^2 \equiv -5$, $(\pm 6)^2 \equiv 6$, $(\pm 7)^2 \equiv 4$. Hence, $x^2 \equiv 1 \pmod{15}$ if and only if x is congruent to one of ± 1, ± 4. That's equivalent to our previous answer, but it highlights some more of the structure.

(b) We compute all squares modulo 13: $0^2 \equiv 0$, $(\pm 1)^2 \equiv 1$, $(\pm 2)^2 \equiv 4$, $(\pm 3)^2 \equiv 9$, $(\pm 4)^2 \equiv 3$, $(\pm 5)^2 \equiv -1$, $(\pm 6)^2 \equiv -3$. Hence, $x^2 \equiv 1 \pmod{15}$ if and only if x is congruent to ± 1.

(c) $x^2 \equiv 1 \pmod{p}$ is equivalent to $p|x^2 - 1$. That is, $p|(x-1)(x+1)$. Since p is a prime, $p|x-1$ or $p|x+1$. In other words, $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. □

Problem 3.

(a) Express 53 in base 2.

(b) Express 1234 in base 2.

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

Solution.

(a) $53 = 32 + 16 + 4 + 1 = 2^5 + 2^4 + 0 \cdot 2^3 + 2^2 + 0 \cdot 2^1 + 2^0$, so that $53 = (110101)_2$.

(b) $1234 = (10011010010)_2$ as the following calculation shows:

- $1234 = 617 \cdot 2 + 0$. Hence, $1234 = (...0)_2$ where ... are the digits for 617.
- $617 = 308 \cdot 2 + 1$. Hence, $1234 = (...10)_2$ where ... are the digits for 308.
- $308 = 154 \cdot 2 + 0$. Hence, $1234 = (...010)_2$ where ... are the digits for 154.
- $154 = 77 \cdot 2 + 0$. Hence, $1234 = (...0010)_2$ where ... are the digits for 77.
- $77 = 38 \cdot 2 + 1$. Hence, $1234 = (...10010)_2$ where ... are the digits for 38.
- $38 = 19 \cdot 2 + 0$. Hence, $1234 = (...010010)_2$ where ... are the digits for 19.
- $19 = 9 \cdot 2 + 1$. Hence, $1234 = (...1010010)_2$ where ... are the digits for 9.
- $9 = 4 \cdot 2 + 1$. Hence, $1234 = (...11010010)_2$ where ... are the digits for 4.
- $4 = 2 \cdot 2 + 0$. Hence, $1234 = (...011010010)_2$ where ... are the digits for 2.

- $2 = 1 \cdot 2 + 0$. Hence, $1234 = (10011010010)_2$.

(c) Modulo 503, we have

$$19^2 \equiv -142, \quad 19^4 \equiv (-142)^2 \equiv 44, \quad 19^8 \equiv 44^2 \equiv -76, \quad 19^{16} \equiv (-76)^2 \equiv 243, \quad 19^{32} \equiv 243^2 \equiv 198.$$

Hence,

$$19^{53} = 19^{32} \cdot 19^{16} \cdot 19^4 \cdot 19 \equiv 198 \cdot 243 \cdot 44 \cdot 19 \equiv -97 \pmod{503}.$$ □

Problem 4. The International Standard Book Number ISBN-10 consists of nine digits $a_1 a_2 ... a_9$ 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!

Solution.

(a) The check digit is

$$a_1 + 2a_2 + 3a_3 + ... + 9a_9 = 0 + 0 + 3 \cdot 7 + 4 \cdot 3 + 5 \cdot 3 + 6 \cdot 8 + 7 \cdot 3 + 8 \cdot 1 + 9 \cdot 4 = 161 \equiv 7 \pmod{11}.$$

The full ISBN is 007338314-7. (That's the one of the book we are using.)

(b) The ISBN we are trying to find is 05254788a_9-7. The condition it needs to satisfy is

$$0 + 2 \cdot 5 + 3 \cdot 2 + 4 \cdot 5 + 5 \cdot 4 + 6 \cdot 7 + 7 \cdot 8 + 8 \cdot 8 + 9 \cdot a_9 \equiv 7 \pmod{11}.$$

This simplifies to

$$-2 + 9 \cdot a_9 \equiv 7 \pmod{11},$$

which is satisfied if and only if $a_9 = 1$.

Hence, the ISBN 052547883-7 is incorrect, and the corrected ISBN is 052547881-7. □