Midterm #3: practice

MATH 311 — Intro to Number Theory
midterm: Thursday, Nov 17

Please print your name:

Calculators will not be permitted on the exam. The numbers on the exam will be suitable for calculating by hand.

Problem 1. For unknown reasons, the high priest of number theory has banned usage of the Euclidean algorithm. With the help of the Chinese remainder theorem, determine the modular inverse of 149 modulo 666.

Problem 2. Compute $7^{111} \pmod{90}$ in the following three different ways:

(a) Directly, using binary exponentiation.

(b) With the help of Euler's theorem.

(c) With the help of the Chinese remainder theorem (as well as Euler's theorem).

Problem 3. Note that $323 = 17 \cdot 19$.

(a) Modulo 323, what do we learn from Euler's theorem?

(b) Using the Chinese remainder theorem, show that $x^{144} \equiv 1 \pmod{323}$ for all x coprime to 323.

(c) Compare the two results!

Bonus: Can you come up with a strengthening of Euler's theorem?

Problem 4. Let a, b be positive integers.

(a) Suppose that $x^a \equiv 1 \pmod{n}$ and $x^b \equiv 1 \pmod{n}$. Show that $x^{\gcd(a,b)} \equiv 1 \pmod{n}$.

(b) Use the previous result to find all solutions to $x^{10} \equiv 1 \pmod{2017}$.

(c) On the other hand, there are 16 solutions to $x^{10} \equiv 1 \pmod{2016}$. What is different in this case?

Problem 5.

(a) You wonder whether 33, 660, 239 is a prime. A (comparatively) quick computation shows that $2^{33660238} \equiv 20364778 \pmod{33660239}$. What do you conclude?

(b) You wonder whether 39, 916, 801 is a prime. A quick computation shows that $2^{39916800} \equiv 1 \pmod{39916801}$. What do you conclude?

Armin Straub
straub@southalabama.edu

Problem 6.

(a) Using Fermat's little theorem and base 3, show that 341 is not a prime.

(b) Is 341 a pseudoprime to the base 2?

These computations are tedious to do by hand. Do make sure though that the idea and the procedure are clear.

Problem 7.

(a) Among the numbers $1, 2, ..., 2016$, how many are coprime to 2016?

(b) Carefully state Euler's theorem.

(c) If the prime factorization of n is $n = p_1^{k_1} \cdots p_r^{k_r}$, what does $\phi(n)$ evaluate to?

(d) Carefully state Wilson's theorem.

Problem 8.

(a) What does it mean for n to be a pseudoprime to base a?

(b) What does it mean for n to be an absolute pseudoprime?

(c) Outline the Fermat primality test. What makes this a heuristic test?

Problem 9.

(a) Using the Chinese remainder theorem, determine all solutions to $x^2 \equiv 1 \pmod{105}$.

(b) Can you predict how many solutions the congruence $x^2 \equiv 1 \pmod{210}$ is going to have?

Problem 10.

(a) Which number is represented by the continued fraction $[1; 2, 1, 2, 1, 2]$?

(b) Determine all convergents of $[1; 2, 1, 2, 1, 2]$.

(c) Which number is represented by the infinite continued fraction $[1; 2, 1, 2, 1, 2, 1, 2, ...]$?

(d) Compare, numerically, the first six convergents (computed above) to the value of the infinite continued fraction.

Problem 11.

(a) Express the numbers $\frac{252}{193}$ and $-\frac{337}{221}$ as a simple continued fraction.

(b) Is this the unique simple continued fraction representing $\frac{252}{193}$? Explain!

— It is also a very good idea to review the problems from Homework 5 as well as the previous practice problems. —

Armin Straub
straub@southalabama.edu