Midterm #2: practice

MATH 311 — Intro to Number Theory
Midterm: Tuesday, Nov 12

Please print your name:

Bonus challenge. Let me know about any typos you spot in the posted solutions (or lecture sketches). Any typo, that is not yet fixed by the time you send it to me, is worth a bonus point.

Problem 1.

(a) Determine the number of invertible residues modulo 116.

(b) Determine the (multiplicative) order of 2 modulo 11.

(c) Is 2 a primitive root modulo 11?

(d) For which a is 2^a a primitive root modulo 11?

(e) List all primitive roots modulo 11.

(f) Suppose $x \pmod n$ has (multiplicative) order k. What is the order of x^a?

(g) What is the number of primitive roots modulo 101?

Problem 2.

(a) Find the smallest positive integer x simultaneously solving the four congruences:
$x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 4$, $x \equiv 3 \pmod 5$, $x \equiv 4 \pmod{11}$.

(b) What is the next largest solution x to the above congruences?

(c) Solve $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 4$, $2x \equiv 3 \pmod 5$, $3x \equiv 4 \pmod{11}$.

(d) Find the smallest integer $a > 2$ such that $2|a$, $3|(a+1)$, $4|(a+2)$ and $5|(a+3)$.

Problem 3.

(a) Using the Chinese remainder theorem, determine all solutions to $x^2 \equiv 4 \pmod{55}$.

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

(c) How many solutions does the congruence $x^2 \equiv 1 \pmod N$ have for $N = 210$? Modulo $N = 1995$?

Problem 4.

(a) What are the last two (decimal) digits of 3^{4488}?

(b) Determine $137^{738} \pmod{63}$.

Armin Straub
straub@southalabama.edu

Problem 5. 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 6. 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 7. 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. (Compare!)

Problem 8. 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) Use the previous result to find all solutions to $x^{10} \equiv 1 \pmod{2018}$.

(d) On the other hand, there are 16 solutions to $x^{10} \equiv 1 \pmod{2016}$. Explain!

Problem 9.

(a) Among the numbers $1, 2, ..., 2019$, how many are coprime to 2019? (673 is a prime.)

(b) Carefully state Euler's theorem.

(c) Carefully state the Chinese remainder theorem.

(d) Carefully state Euler's criterion for quadratic residues.

(e) Use Euler's criterion for quadratic residues to determine whether 3 is a quadratic residue modulo 19.

(f) Use Euler's criterion for quadratic residues to determine whether 3 is a quadratic residue modulo 23.

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

Armin Straub
straub@southalabama.edu

Problem 10.

(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?

(c) What does it mean for a to be a Fermat liar modulo n?

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

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

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

(g) Is 2 a Fermat liar modulo 341?

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

Problem 11.

(a) State Wilson's theorem.

(b) List all quadratic residues modulo 21.

(c) What is the number of invertible quadratic residues modulo 91? Modulo 101? Modulo 165?

Armin Straub
straub@southalabama.edu